



INTERNATIONAL LEGAL RESEARCH GROUP ON HUMAN RIGHTS & TECHNOLOGY VOL I

elsa

The European Law Students' Association
ALBANIA

elsa

The European Law Students' Association
AZERBAIJAN

elsa

The European Law Students' Association
HUNGARY

elsa

The European Law Students' Association
ITALY

elsa

The European Law Students' Association
MALTA

elsa

The European Law Students' Association
LITHUANIA

elsa

The European Law Students' Association
PORTUGAL

elsa

The European Law Students' Association
ROMANIA

elsa

The European Law Students' Association
SERBIA

International Legal Research Group on Human Rights and Technology

Vol. I

Reporting Countries:

ELSA Albania

ELSA Azerbaijan

ELSA Hungary

ELSA Italy

ELSA Lithuania

ELSA Malta

ELSA Portugal

ELSA Romania

ELSA Serbia

International Legal Research Group on Human Rights and Technology

ELSA International

Website: <https://legalresearch.elsa.org/>

Published by:

ELSA International, 2025

E-Mail: academicactivities@elsa.org

Website: <https://elsa.org/>

Editor in Chief

Maja Rajić

International Board of ELSA 2020/2021

Deputy Editor in Chief

Bernadetta Semczuk

Director for Legal Writing

ELSA International 2020/2021

International Coordinator

Alexandra-Daniela Stoica

International Coordinator for ILRG

ELSA International 2020/2021

International Linguistic Editor

Maisie Beavan

ELSA International 2020/2021

International Technical Editor

Antonette Persechino

ELSA International 2020/2021

International Editors

Velina Stoyanova & Francisco Amaral

ELSA International 2024/2025

Publishing Coordination

Niko Anzulović Mirošević

International Board of ELSA 2024/2025

Academic Board

Gavin Sutter

Professor at Queen Mary University of London

Guido Westkamp

Professor at Queen Mary University of London

William Echikson

Associate Senior Fellow at the Centre for European Policy Studies

Katerina Iliadou

Professor at Athens School of Law

Snjezana Vasiljevic

Associate Professor at the University of Zagreb

CONTRIBUTORS

National Coordinators

Glen Mebelli

Shabnam Guliyeva

Kamilla Bodori

Andela Bakula

Francesca Mulliri

Nina Blakeway

Aušra Abraitė

Emma de Gabriele

Matthew Camilleri

Ivan Chopyk

Iulia Mitache

National Academic Supervisors

Ažuolas Čekanavičius

Glen Mebelli

Elvin Balajanov

Turkhan Ismayilzada

Zsolt Gáspár

Enrica Priolo

Jackie Mallia

Miglė Petkevičienė

Paula Ribeiro Alves

Linguistic Editors

Amil Jafarguliyev

Enrica Bertoldi

Brândușa Enișor

Giulia Piccioni

Inês Alves	Raminta Matulytė
Karen Scerri	Skaidrė Dudėnaitė
Maila Cimino	Tariyel Aliyev
Maria Duminică	

Technical Editors

Andreea Iordache	Luke Bonanno
Diogo Gambini Neves	Marika Francescapia Casula
Federico Quagliarini	Martynas Matusevičius
Fidan Namazova	Raluca Elena Irimia
Inês Henriques Fraga da Costa	Zsófia Márta Tengőlics
Kamilla Bodori	

Researchers and Authors

Alexandra Grieb	Danielė Giedraitytė	Francisco Lima
Alexandra Török	Denis Knežević	Gianluca Vella
Algirdas Gedminas	Diogo Gambini Neves	Giulia Piccioni
Amil Jafarguliyev	Dóra Horváth	Ibrahim Mammadzade
Ana Memeti	Elisa Micallef Peplow	Inês Alves
Andreea Iordache	Enikő Takács	Inês Henriques Fraga da Costa
Antonia Pîslariu	Enrica Bertoldi	Jelena Branković
Arianna Crosera	Ersona Cakaj	Kamil Demirli
Bálint Imre Bodó	Esmeralda Dida	Kamilla Bodori
Bárbara da Rosa Lazarotto	Eugenio Ciliberti	Karen Scerri
Beatriz Assunção Ribeiro	Federica Paolucci	Katarina Bakula
Bence Tumoró	Federico Quagliarini	Kinga Kálmán
Cătălin Panțiru	Fidan Namazova	Kirsty Ellul

Kotryna Seliutaitė	Michaela Pia Camilleri	Sama Mammadli
Leila Kentache	Miglė Petkevičienė	Sevil Hasanli
Luisa Matos	Milica Cvetković	Shovkat Rasulova
Luke Bonanno	Natacha Alves	Skaidrė Dudėnaitė
Maila Cimino	Nesrine Kraiem	Taleh Abbasli
Maria Carolina Nicolini	Olena Barda	Tariyel Aliyev
Maria Duminică	Oleksandr Melnyk	Tatjana Kovačević
Maria Vittoria Voi	Paula Ribeiro Alves	Tea Mladenov
Mariam Atakishieva	Pierfrancesco De Felice	Teisa Kurti
Marika Francescapia Casula	Raluca Crețu	Turkhan Ismayilzada
Martina Caslini	Raluca Elena Irimia	Valeria Argento
Martynas Matusevičius	Raminta Matulytė	Veronica Gallo
Matthew Mifsud	Rebekah Cilia	Vytautas Pasvenskas
Megı Reçi	Sama Jafarli	Zsófia Márta Tengölics

FOREWORD

What is ELSA?

The European Law Students' Association (ELSA) is a non-political, non-governmental, non-profit making, independent organisation which is run by and for students. ELSA has 43 Member and Observer countries with more than 375 Local Groups and 60 000 students. The Association was founded in 1981 by five law students. Since then, ELSA has aimed to unite students from all around Europe, provide a channel for the exchange of ideas and opportunities for law students and young lawyers to become internationally minded and professionally skilled. The purpose of the Association is to contribute to legal education, to foster mutual understanding and to promote social responsibility of law students and young lawyers. Our focus is to encourage individuals to act for the good of society in order to realise our vision: 'A just world in which there is respect for human dignity and cultural diversity'.

What is a Legal Research Group?

A Legal Research Group (LRG) is an academic, legal writing project that provides law students and young lawyers with the opportunity to develop various legal skills, such as legal English, legal research and writing skills, as well as soft skills. The LRG involves a group of law students and young lawyers conducting research on a specified topic of law with the aim to make their work publicly accessible. The project can work at local, national, or international level. The first working LRG was formed by ELSA International in 1996 on aspects of 'International Criminal Law'. Since the publication of that first research in 1997, ELSA International has launched LRGs on different topics of law, making the project more appealing and popular to its National Groups.

What is the International Legal Research Group on Human Rights and Technology?

While the thesis of the report is 'The Right to Privacy and Data Protection in the Age of Advanced Digital Technologies', the International Legal Research Group on Human Rights and Technology focuses on human rights issues caused by artificial intelligence and analyses how proper protection may be ensured. Researchers from over 20 countries have examined aspects such as data privacy, discrimination and the implications of AI on fundamental rights in order to offer recommendations on how legislation can strike a balance between enabling technological developments and ensuring sufficient protection of human rights. The report emphasizes the need for adaptive legal frameworks that safeguard individual privacy while allowing innovation to thrive. It stresses the importance of ongoing research and dialogue to address emerging challenges, advocating for a forward-thinking approach to privacy and data protection in an increasingly digital world.

Contents

ACADEMIC FRAMEWORK	17
ELSA ALBANIA	20
Introduction	21
1. Which human rights issues do Advanced Digital Technologies pose in your country?	21
2. How is personal information protected in your national legislation?	22
3. To which extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?	25
4. What is the process of judicial review of cases of data protection breaches?	27
5. Does the review constitute effective protection of data privacy?	31
6. What is the process of judicial review of anti-discrimination cases?	32
7. Does your country have any specific regulations on Advanced Digital Technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?	35
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	37
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	40
10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the upcoming five years?	41
Conclusion	42
Table of legislation	44
Bibliography	55
ELSA AZERBAIJAN	59
Introduction	61
1. Which human rights issues does Advanced Digital Technologies (ADT) pose in your country?	61
2. How is personal information protected in your national legislation?	65
3. To what extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?	70
4. What is the process of judicial review of cases data protection breaches?	74
5. Does the review constitute effective protection of data privacy?	78
6. What is the process of judicial review of anti-discrimination cases?	82
7. Does Azerbaijan have any specific regulations on advanced digital technologies, such as big data, Artificial Intelligence, Internet of Things?	86
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	87
9. Has your country reached an adequate balance between allowing digital	

advancements and protecting human rights online?	90
10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the coming 5 years?	92
Conclusion	93
Table of legislation	95
Bibliography	97
ELSA HUNGARY	101
1. Which human rights issues do Advanced Digital Technologies pose in your country?	102
2. How is personal information protected in your national legislation?	106
3. To which extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?	108
4. What is the process of judicial review of cases data protection breaches?	110
5. Does the review constitute effective protection of data privacy?	115
6. What is the process of judicial review of anti-discrimination cases?	120
7. Does your country have any specific regulations on Advanced Digital Technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?	125
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	129
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	132
10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the upcoming five years?	135
Table of legislation	140
Bibliography	182
ELSA ITALY	189
Introduction	191
1. Which human rights issues do Advanced Digital Technologies pose in your country?	191
2. How is personal information protected in your national legislation?	194
3. To which extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?	196
4. What is the process of judicial review of cases data protection breaches?	199
5. Does the review constitute effective protection of data privacy?	202
6. What is the process of judicial review of anti-discrimination cases?	204
7. Does your country have any specific regulations on Advanced Digital Technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?	207

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	210
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	213
10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the upcoming five years?	216
Conclusion	219
Table of legislation	222
Bibliography	242
ELSA LITHUANIA	272
Introduction	273
1. Which human rights issues do Advanced Digital Technologies pose in your country?	273
2. How is personal information protected in your national legislation?	275
3. To which extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?	277
4. What is the process of judicial review of cases of data protection breaches?	279
5. Does the review constitute effective protection of data privacy?	285
6. What is the process of judicial review of anti-discrimination cases?	287
7. Does your country have any specific regulations on Advanced Digital Technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?	289
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	291
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	294
10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the upcoming five years?	295
Conclusion	296
Table of legislation	298
Bibliography	316
ELSA MALTA	325
Introduction	327
1. Which human rights issues does Advanced Digital Technologies (ADT) pose in your country?	327
2. How is personal information protected in your national legislation?	330
3. To what extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?	335
4. What is the process of judicial review of cases data protection breaches?	335

5. Does the review constitute effective protection of data privacy?	340
6. What is the process of judicial review of anti-discrimination cases?	346
7. Does your country have any specific regulations on advanced digital technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?	347
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	350
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	353
10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the coming 5 years? Incorporate the answers, you have given to the previous questions, and the main results of your research.	355
Conclusion	357
Table of Legislation	359
Bibliography	361
ELSA PORTUGAL	364
Introduction	366
1. Which human rights issues do Advanced Digital Technologies pose in your country?	367
2. How is personal information protected in your national legislation?	371
3. To which extent is the data protection self-regulated by the private sector in your country?	373
4. What is the process of judicial review of cases of data protection breaches?	375
5. Does the review constitute effective protection of data privacy?	380
6. What is the process of judicial review of anti-discrimination cases?	382
7. Does your country have any specific regulations on advanced digital technologies, such as big data, Artificial Intelligence (AI), Internet of Things (IoT) and/or encryption?	387
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	390
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online? If applicable, specify how the situation in your country is perceived externally (by other countries/ members of the economic/political bloc, international organizations, etc).	395
10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the coming 5 years? Incorporate the answers you have given to the previous questions, and the main results of your research.	396
Conclusions	399

Table of legislation	403
Bibliography	405
ELSA ROMANIA	407
Introduction	408
2. How is personal information protected in your national legislation?	411
3. To which extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?	416
4. What is the process of judicial review in cases of data protection breaches?	417
5. Does the review constitute effective protection of data privacy?	420
6. What is the process of judicial review of anti-discrimination cases?	422
7. Does your country have any specific regulations on advanced digital technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?	425
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	429
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	430
10. Based on your analysis, how do you believe the legislation regarding on the area of protecting human rights online will develop in the coming 5 years?	434
Conclusion	436
Table of legislation	437
Bibliography	455
ELSA SERBIA	458
Introduction	459
1. Which human rights issues do Advanced Digital Technologies pose in your country?	459
2. How is personal information protected in your national legislation?	463
3. To which extent is the data protection self-regulated by the private sector in your country? How do the public and private sectors cooperate in this regard?	465
4. What is the process of judicial review of cases of data protection breaches?	468
5. Does the review constitute effective protection of data privacy?	470
6. What is the process of judicial review of anti-discrimination cases?	475
7. Does your country have any specific regulations on Advanced Digital Technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?	476
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	478
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	481

10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the upcoming five years?	484
Conclusion	484
Table of legislation	486
Bibliography	488

ACADEMIC FRAMEWORK

1. Which human rights issues does Advanced Digital Technologies pose in your country?
 - 1.1. Is there or what is a legal framework that provides for procedure on human rights impact assessments? What are other instruments used for identifying human rights issues posed by ADT?
 - 1.2. What national and international standards of human rights protection are at risk due to the ADT development and implementation?
2. How is personal information protected in your national legislation?
 - 2.1. How is personal information defined by your national legislation (or by a legal framework that affects your national legislation, e.g. GDPR)?
 - 2.2. If your country is a Member State of the European Union, please provide a concise analysis of the extent to which your country's laws regarding protection of personal information are compatible with EU law, particularly the General Data Protection Regulation (GDPR).
 - 2.3. How do external instruments (such as the abovementioned GDPR) influence the data protection in your country (N.B. can be applicable to non-EU countries as well).
3. To which extent is the data protection self-regulated by the private sector in your country?
How do public and private sectors cooperate in this regard?
4. What is the process of judicial review of cases data protection breaches?
 - 4.1. Is the right to data privacy defined in your legal system? If not, is it a part of another right protected the national law?
 - 4.2. Can the data subject restrict or object the data processing? What are the circumstances and exceptions to this option?
 - 4.3. In case of data protection breaches, what is the process to notify the data subject? Are there any exceptional grounds not to notify the data subject? If such grounds exist, what would be the ideal or optimal balance for necessity and proportionality?
5. Does the review constitute effective protection of data privacy?
 - 5.1. Which bodies conduct such review?

- 5.2. What is the process of judicial review for cases of data protection breaches?
 - 5.3. Does the review provide effective remedies to the data protection breaches? If so, please specify. For example, what kind of sanctions are imposed as penalties or what remedies are available?
6. What is the process of judicial review of anti-discrimination cases?
 - 6.1. Which bodies conduct such review? What are the elements that are taken into consideration when such review is conducted?
 - 6.2. Does the review constitute effective protection against discrimination?
 - 6.3. What is a considered role of the technical aspects that result in discrimination (such as algorithmic bias)? How are these problems tackled?
7. Does your country have any specific regulations on advanced digital technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?
 - 7.1. Please specify any existing or proposed legislation. If none is in place, are there any initiatives introduced by private actors or NGOs?
 - 7.2. To what extent are the external legislative developments influential on your country's regulation of this area?
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?
 - 8.1. Specify the circumstances in which such decryption may be conducted? What are the potential or real consequences of such requirement?
 - 8.2. Does this requirement (in general or in practice) provide the authorised body with too much power? Clarify your answer.
 - 8.3. What level of protection does your country's legislation provide to the individuals in the circumstances mentioned above?
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?
 - 9.1. If applicable, specify how the situation in your country is perceived externally (by other countries/ members of the economic/political bloc, international organizations, etc).

10. Based on your analysis, how do you believe that legislation regarding on the area of protecting human rights online will develop in the coming 5 years?

10.1. Incorporate the answers, you have given to the previous questions, and the main results of your research.

Conclusion

ELSA ALBANIA

Contributors

National Coordinator

Glen Mebelli

National Academic Coordinator

Glen Mebelli

National Researchers

Esmeralda Dida

Ersona Cakaj

Megi Reçi

Teisa Kurti

National Academic Supervisor

Dr. Desara Dushi

Introduction

The growth of information technologies role in our society and the widespread of data on online networks present some substantial challenges and potential risks for the personal data protection, privacy and cybersecurity. The Republic of Albania has made moderate steps toward approximation of the national legislation with that of the EU and developed countries on the AI, however prompt actions must be taken to further progress.

In this report we will provide a detailed information on issues such as data protection and privacy as well as other legal challenges in Albania, imposed by the current digital era.

1. Which human rights issues do Advanced Digital Technologies pose in your country?

1.1. Is there or what is a legal framework that provides for procedure on human rights impact assessments? What are other instruments used for identifying human rights issues posed by ADT?

The assessment of the impact of Advanced Digital Technologies on human rights is not provided for or regulated under the applicable legal framework in Albania. Furthermore, there is no specific legislation currently into effect in Albania on Advanced Digital Technologies, such as big data, artificial intelligence, Internet of Things and/or encryption. Other issues such as algorithmic bias are neither regulated in the law nor discussed enough in the research and human rights community. Nevertheless, the right to private life, protection of personal data, secrecy of electronic communication, and privacy of correspondence are guaranteed under the Constitution and the relevant national laws. Having these basic rights guaranteed by law, does not suffice. In order to identify and address the contemporary challenges arising from advanced digital technologies, laws, case law and research need to advance quickly to respond to the speed in which digital technologies advance, and to be able to tackle the new societal realities and challenges posed to human rights.

1.2. What national and international standards of human rights protection are at risk due to the ADT development and implementation?

Some fundamental rights are put at risk due to ADT development including freedom of expression, right to information, protection from hate speech and discrimination, right to private life, protection of personal data and privacy of communication, protection from sexual harassment etc. On the other hand, security and intelligence agencies have to face increased challenges in countering serious crime, in the form of cyber terrorism, organized crime and online extremism. Artificial intelligence obscures and attenuates responsibility for harms in ways that undermine traditional mechanisms for holding wrongdoers accountable¹. Further,

¹ Molly K. Land., Jay D. (2020) Aronson *Human Rights and Technology: New Challenges to Justice and Accountability*.

technologies that scholars and practitioners once thought would democratize human rights fact finding have been weaponized by state and non-state actors. They are now used to surveil and track citizens and spread disinformation that undermines public trust in knowledge. Addressing these challenges requires efforts to ensure that the development and implementation of new technologies respects and promotes human rights.² Advanced digital technologies pose numerous threats to human rights and lawmakers, policy makers, law enforcement agencies, judges, prosecutors, NHRIs, must be prepared to respond to that in their daily work and must be trained to a continuous learning process about human rights issues to be able to embrace arising contemporary perspectives. As the UN High Commissioner for Human Rights Michelle Bachelet said in 2019: “The digital revolution is a major global human rights issue. Its unquestionable benefits do not cancel out its unmistakable risks. Neither can we afford to see cyberspace and artificial intelligence as an ungoverned or ungovernable space – a human rights black hole. The same rights exist online and offline.”³

2. How is personal information protected in your national legislation?

2.1. How is personal information defined by your national legislation (or by a legal framework that affects your national legislation, e.g. GDPR)?

Law No. 9887, dated 10.3.2008 ‘On Personal Data Protection’⁴, as amended, is the cornerstone with regard to personal data/information within the territory of the Republic of Albania. According to Article 3(1) of this law, personal data refers to any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity etc. In addition, sensitive data is defined as any piece of information related to the natural person in referring to his racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal prosecution, as well as with data concerning his health and sexual life.

2.2. If your country is a Member State of the European Union, please provide a concise analysis of the extent to which your country’s laws regarding protection of personal information are compatible with EU law, particularly the General Data Protection Regulation (GDPR).

² *ibid.*

³ OHCHR “Human rights in the digital age” (17 October 2019). <<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E>> accessed 8 May 2021.

⁴ Law No. 9887, dated 10.3.2008 ‘On Personal Data Protection amended with Law No. 120/2014 “On Some amendments and additions to Law No. 9887, dated 10.3.2008 On Personal Data Protection’ (Personal Data Protection Law). <<https://qbz.gov.al/eli/ligj/2008/03/10/9887/41ed4e3c-3dde-4028-9755-11887c48b7f6;q=LIGJ%20Nr.9887,%20dat%C3%AB%2010.3.2008%20P%C3%8BR%20MBROJTJEN%20E%20T%C3%8B%20DH%C3%8BNAVE%20PERSONALE%20>> accessed 17 May 2021.

The Republic of Albania is not an EU Member State, nevertheless our country is engaged in protecting personal information and has undertaken significant steps toward enhancement of the national legislation in compliance with the European standards to protect personal information. In the framework of aspiration to EU integration, Albania has concluded the Stabilization and Association Agreement ('SAA') with the EU and according to Article 70 of the SAA⁵ 'the Parties recognise the importance of the approximation of Albania's existing legislation to that of the Community and of its effective implementation. Albania shall endeavour to ensure that its existing laws and future legislation shall be gradually made compatible with the Community acquis. Albania shall ensure that existing and future legislation shall be properly implemented and enforced'. With the adoption of the new GDPR and under the SAA, the Albanian Commissioner on the Right to Information and Personal Data ('ACRIPD') has incorporated into the strategy⁶ 'On Information and Personal Data Protection 2018-2020' the harmonization of current law on protection of personal data with the GDPR 697/2016. In a nutshell, one of the objectives of the ACRIPD is to analyse and identify gaps in the current Albanian legislation, propose and adopt a new law on protection of personal data which addresses the novelties of the GDPR, precisely: the right to be forgotten, data transferability right, strengthening of accountability in relation to data processors, transparency, protection of the data of children, strengthening the independence of the authority for the protection of personal data, appointment of data protection officers, and certification of data controllers/data processors. The above mentioned strategy was foreseen to be completed by the end of 2020, but up to date there has been no amendments to the Law No. 9887, dated 10.3.2008 'On Personal Data Protection'.

2.3. How do external instruments (such as the abovementioned GDPR) influence the data protection in your country?

As mentioned above, our national legislation on data protection has not incorporated the GDPR yet, nevertheless, the extraterritorial scope of the Regulation affects not only EU Member States but also non-Member States such as Albania.

Article 3 of the GDPR uses two key criteria to determine territorial scope: the 'establishment' criterion and the 'targeting' criterion. In a nutshell, either a data controller or processor is established in the European Union or they are established outside the European Union but

⁵ Stabilization and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Albania, of the other part [2009] (OJ L107/166)
<[https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02009A0428\(02\)-20170201&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02009A0428(02)-20170201&from=EN)> accessed 17 May 2021.

⁶ Strategy 2018-2020 on the Right to Information and Protection of Personal Data, 18
<https://www.idp.al/wp-content/uploads/2018/02/Strategjia_per_te_Drejten_e_Informimit_dhe_Mbrojtjen_e_te_Dhenave_Personale.pdf> accessed 12 May 2021.

target the EU market.⁷ In this sense, the territorial scope of the GDPR affects non-EU member states.

Firstly, as per Article 3(1),⁸ the European Data Protection Board confirms that it is the presence, through an establishment, of a data controller or processor in the EU and the fact that a processing takes place in the context of the activities of this establishment that trigger the application of the GDPR to its processing activities. The place of processing is therefore not relevant in determining whether or not the processing, carried out in the context of the activities of an EU establishment, falls within the scope of the GDPR.⁹ This implies that if companies have branches or cooperate with companies located outside EU Member States, i.e in Albania and they process or collect personal data, then the application of the GDPR is triggered.¹⁰

Secondly, the GDPR goes further and extends its territorial scope to non-EU companies if two conditions are met: the organization offers goods or services to people in the EU; or the organization monitors their online behaviour.¹¹ Thus, Albanian companies whose data processing activity relate to the above mentioned activities/criteria are subject to the rules set out in the GDPR. Put simply, if Albanian companies cater to EU customers, then they should strive to be GDPR compliant and if Albanian companies use web tools that allow tracking cookies or the IP addresses of people who visit the website from EU countries, then they fall under the scope of the GDPR.¹² However, as both criteria are broad and sketchy on the edges, it remains to be seen how these will be interpreted and applied by national data privacy authorities and the CJEU.

In toto, the Albanian organizations offering goods or services to EU citizens as well as monitoring their behaviour potentially fall under the application of the GDPR. In addition,

⁷ Eversheds Sutherland, 'Data Protection across all borders? GDPR's territorial scope' (Lexology 2020) <<https://www.lexology.com/library/detail.aspx?g=2e9ac1a4-ffa3-4c25-99e7-3f9665fd815a>> accessed 17 May 2021.

⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L119/1) art.3 '1. *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.* 2. *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.* 3. *This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*

⁹ 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', 9 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf> accessed 12 May 2021.

¹⁰ Megi Kurti, 'The Impact of GDPR On Private Law: Challenges Of Business Liability And Personal Data Protection In Albania' (2019) bogalawjournal <<http://bogalawjournal.com/the-impact-of-gdpr-on-private-law/>> accessed 12 May 2021.

¹¹ Does the GDPR apply to companies outside the EU? <<https://gdpr.eu/companies-outside-of-europe/#:~:text=The%20GDPR%20does%20apply%20outside,%E2%80%9CExtra%2Dterritorial%20effect.%E2%80%9D>> accessed 12 May 2021.

¹² Kurti (n 10).

cooperation between Albanian companies and EU based companies/foreign business investments in Albania influence the application of the GDPR, therefore harmonization of the legislation with regard to personal data protection will consequently offer a more secure legal environment for foreign investments to collaborate with the Albanian enterprises.¹³

3. To which extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?

It is important to note that the legal framework does not postulate any restrictions nor interdiction to whether private companies can adopt policies for data protection, therefore any company may set up an internal instrument, on the condition that such self-regulating instrument provides no less than the minimum of protection guaranteed by the Law No 9887, dated 10.3.2008 'On Personal Data Protection'.

Nonetheless, large economic operators such as banks or telecommunications companies draft regulations on the privacy of customers and the processing of data, referring to the legal framework applicable in the territory of the Republic of Albania.

More precisely, ProCredit Bank in its 'Privacy Policy' states that 'Data shall be collected, processed and stored in full compliance with the Law No. 9887, dated 10.3.2008 and in accordance to the purpose of processing; international transfer of data to ProCredit Bank Kosovo shall be completed in compliance with the law and bylaws; the consumer confirms his consent for further processing of data by completing a Declaration as issued by the bank'.¹⁴ Similarly, Tirana Bank in its 'Policy on Privacy'¹⁵ details the use, collection and processing of data when consumers navigate in the website of Tirana Bank for the purpose of improving the service (*such data shall be processed in accordance with the Law*), the right of consumers/users to request information regarding the processing of data or to request the annulment or blocking of any information processed in non-compliance with the Law.

Telecommunications companies, such as Vodafone Albania set up Privacy Policies¹⁶ which are constructed according to the Law No. 9918, dated 19.05.2008 'On Electronic Communications

¹³ *ibid.*

¹⁴ Privacy Policy, ProCredit Bank (2018)

<https://www.procreditbank.com.al/Uploads/Data/Files/157/PolitikaeprivatesisePCBALB_rVfqVARNtU.pdf?fbclid=IwAR20Qbpl_U7ROeSwsqbyHh9psvBpEqucDEZ41XsA7VZ0lRxZnDMpRHiE0M> accessed 17 May 2021.

¹⁵ Policy on Privacy, Tirana Bank

<<https://www.tiranabank.al/media/15469460285c3485ecb4bde.pdf?fbclid=IwAR3oi1hwQeAa4cyq333fp6Ucsixfm3oTx0THf4JUq7uI87JDKnkwupCDdA4>> accessed 17 May 2021.

¹⁶ Privacy Policy, Vodafone Albania

<<https://www.vodafone.al/en/informacion-ligior/informacion-i-pergijthshem-ligior/rregullore-e-privatesise/>> accessed 17 May 2021.

in the Republic of Albania' and Law No. 9887, dated 10.03.2008 'On Personal Data Protection' as well as in compliance with the regulatory framework as updated from time to time by the Commissioner for the Right of Information and Protection of Personal Data. The only additional safeguard (compared to other private entities) that Vodafone Albania provides for in case of international transfer of data, is a contract setting out the obligations between the parties during the transfer of data to ensure the protection of personal data (*international transfer of data is however conducted in accordance with the requirements of the law on data protection*).

In conclusion, companies operating within the territory of Albania have not adopted pure self-regulated instruments but it seems that they compile policies that do not go far beyond the regulations and protection guaranteed by the relevant laws on data protection or electronic communications, or any other law affecting the data of consumers/users. However, with the rapid technological advances it is necessary for companies to offer a high level of protection for costumers and to guarantee a standard of protection that surpasses the protection provided by the current applicable laws in Albania.

Cooperation under the Law No. 9887, dated 10.3.2008 'On Personal Data Protection', as amended.

According to Article 32 of the Law on Personal Data Protection, public and private institutions cooperate with the Commissioner, by delivering to him all the information upon its request. The Commissioner is entitled to have access to the computers system, achieve systems, conduct processing of personal data and in any other document related to processing and transferring of the data.

Moreover, in the framework of ensuring protection of personal data, the Albanian Commissioner is responsible to supervise and monitor the protection of personal data¹⁷ therefore the Commissioner undertakes the necessary steps to ensure that private as well as public entities comply with the relevant law(s) on protection of personal data and any other legal act. For this purpose, one of the safeguards is the legal requirement for controllers to notify the Commissioner's Office on any processing of personal data during their activity. Such notice must be delivered prior to commencement of personal data processing (if the processing is concluded for the first time) or when alterations to the purpose of processing of personal data is sought to be completed¹⁸ (*the law and other legal acts provide for exemptions from this rule*).

Prior approval by the Commissioner is required for the processing of sensitive data for an important public interest under adequate safeguards. Additionally, authorization is required for international data transfers to countries without an adequate level of protection of personal data.

¹⁷ Personal Data Protection Law 2008, art 29.

¹⁸ Policy on Privacy, Tirana Bank (n 15) art 21.

In such cases, after an evaluation by the Commissioner, the latter issues an authorization along with conditions and obligations.¹⁹

Subsequently, cooperation between private / public processors or controllers is of utmost importance to generate a set of best practices with regard to the protection of personal data, as well as to guarantee the fulfilment of rights and obligations assigned by law to the Commissioner. Failure to cooperate with the Commissioner leads to administrative contraventions punishable by a fine (varying from ALL 10 000 – 500 000 or approximately EUR 80 - 4000).

4. What is the process of judicial review of cases of data protection breaches?

4.1. Is the right to data privacy defined in your legal system? If not, is it a part of another right protected by the national law?

The right to data privacy is defined in the Albanian legal system in the Constitution and it is regulated by the Law on the Protection of Personal Data. Other relevant laws, such as the Law on Electronic Communications as well as the Criminal Code, regulate specific aspects of data privacy protection.

The Constitution of Albania²⁰ establishes that no one may be obliged, except for when the law requires it, to make public data related to his person. The Constitution also requires the consent of the person when collecting, using and publishing the data, except for cases provided by law. According to the Constitution, everyone has the right to become acquainted with data collected about him, except for the cases provided by law and everyone has the right to request the correction or deletion of untrue or incomplete data or data collected in violation of the law. Furthermore, freedom and secrecy of correspondence or any other means of communication are guaranteed.²¹

The Law on Protection of Personal Data regulates in detail the means for the protection of personal data, the criteria for lawful data processing, and the available remedies.

The Law on Electronic Communications²² establishes the obligation of the service-providers and relevant stakeholders to ensure the secrecy of electronic communications and the protection of personal data as well as to not allow unauthorized access in electronic communications and data processing.

¹⁹ *ibid*, art 9.

²⁰ The Constitution of Albania, art. 35.

²¹ *ibid* art. 36.

²² On Electronic Communications Law 2008, art. 121.

The Criminal Code of Albania²³ prescribes intruding into someone's privacy, spreading of personal secrets, and obstruction or violation of the privacy of correspondence as criminal violations punishable by law.

Albania is a member of the Council of Europe and the European Convention on Human Rights is directly applicable. Furthermore, Albania is a ratifying state of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol

4.2. Can the data subject restrict or object the data processing? What are the circumstances and exceptions to this option?

According to the Law on Protection of Personal Data, the data subject can restrict the data processing, by refusing to give consent, which is the first criteria required for lawful data processing.²⁴ The data subject has the right to object the processing²⁵ of data related to him/her, the right to demand the controller not to start processing, or if processing has started, to stop the processing of personal data related to him as well as the right to object the data processing by requesting blocking, rectification, and erasure²⁶ in the cases when data relating to him/her are irregular, untrue, and incomplete or have been processed and collected in contradiction with the law.

The Law on Protection of Personal Data, stipulates that the data can be lawfully processed only in the following circumstances:

*'1. The personal data subject has given his/her consent; 2. The processing is necessary for the performance of a contract to which the data subject is a party or in order to negotiate or amend a draft/contract at the request of the data subject; 3. In order to protect the vital interests of the data subject; 4. To comply with a legal obligation of the controller; 5. For the performance of a legal task of public interest or in the exercise of powers of the controller or of a third party to whom the data are disclosed; 6. Processing is necessary for the protection of the legitimate rights and interests of the controller, the recipient, or any other interested party'.*²⁷

However, in any case, the processing of personal data cannot be in clear contradiction with the data subject's right to protection of personal life and privacy.²⁸ Processing of personal data in the framework of crime prevention and prosecution activities, in cases of a criminal offence against the public order and other violations in the field of criminal law, defence and national security, are performed by official authorities as stipulated in the law.²⁹ In the event the controller or

²³ Criminal Code of Albania, art. 121-123.

²⁴ On Protection of Personal Data Law 2008, art. 6.

²⁵ *ibid* art 15.

²⁶ *ibid* art 13.

²⁷ *ibid* art 6.

²⁸ *ibid* art (dh).

²⁹ *ibid* art 6/2.

processor carries out personal data processing for the purpose of offering business opportunities or services provided that the data were taken from a public list of data.³⁰ The controller or processor cannot process further the data specified in this paragraph if the data subject has expressed his disagreement or has objected to their further processing.³¹ No additional personal data is attached to the data specified above without the consent of the data subject.³²

Furthermore, the data subject can object the processing of sensitive data³³. The Law on Protection of Personal Data prohibits the processing of sensitive data, except for the following circumstances³⁴:

'1. The data subject has given his/her consent, which may be revoked at any given moment making illegal any further processing of data; 2. It is in the vital interest of the data subject or another person and the data subject is physically or mentally incapable of giving his/her consent; 3. It is authorized by the responsible authority for an important public interest, under adequate safeguards; 4. It is related to data that are manifestly made public by the data subject or is necessary for the exercise or defence of legal rights; 5. Data are processed for historic, scientific, or statistical research, under adequate safeguards; 6. Data are required for preventive medicine, medical diagnosis, the provision of health care, treatment or management of health care services, and data are used by medical personnel or other persons with the obligation to preserve confidentiality; 7. Data are processed by non-profit political, philosophical, or religious organisations and trade unions for purposes of their legitimate activity, only for members, sponsors, or other persons related to their activity, while these data shall not be disclosed to a third party without the consent of the data subject unless otherwise stipulated by law; 8. The data processing is necessary for the purpose of accomplishing a legal obligation and specific rights of the controller in the field of employment in compliance with the Labour Code.'

4.3. In case of data protection breaches, what is the process to notify the data subject? Are there any exceptional grounds not to notify the data subject? If such grounds exist, what would be the ideal or optimal balance for necessity and proportionality?

The Law on Protection of Personal Data³⁵ does not prescribe the process of notification for data protection breaches but it stipulates that the data subject shall be notified by the controller³⁶ when their personal data is being processed. The data subject has the right to be informed on the

³⁰ *ibid* art 6/3.

³¹ *ibid*.

³² *ibid* art 6/4.

³³ According to art 3/4 of the Law No. 9887, 10.3.2008 On Protection of Personal Data: '*Sensitive data*' includes any piece of information related to the natural person in referring to his racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal prosecution, as well as with data concerning his health and sexual life.

³⁴ On Protection of Personal Data Law 2008, art 7.

³⁵ *ibid* art 18.

³⁶ According to art 3/5 of the Law No. 9887, dated 10.3.2008 On Protection of Personal Data: '*Controller*' shall mean the natural or legal person, public authority, agency or any other body, which alone or jointly with others determines the purposes and means of the processing of personal data, in compliance with the laws and secondary legal acts applicable, and who is responsible for the fulfillment of obligations defined by this law.

scope and purpose for which personal data are being processed, the person who is going to process the data, on the mean of processing, on the right to access, and the right to rectify the data concerning him/her, on the fact whether the provision of the personal data is obligatory or optional and on the consequences of refusal to provide personal data in the case that obligation derives from a legal or secondary act. In cases when controllers fail to inform the data subject on personal data processing the Law on Protection of Personal Data prescribes for administrative sanctions. In such cases, the applicable fines amount between 10 000 ALL to 300 000 ALL.³⁷

Exceptions to this obligation of the controller to inform are allowed when the data subject is already aware of the processing of the data; when the data subject has given consent; when the personal data is processed exclusively for the purpose of historical, statistical, and scientific research and if informing the data subject is not possible or demands disproportionate efforts; in cases when the controller must process personal data on grounds of a legal provision; when the data being processed are already made public.³⁸

Additionally, every controller shall notify the Commissioner for the Right to Information and Data Protection (The Commissioner)³⁹ about the processing of personal data for which they are responsible. The notification shall be made before the controller processes the data for the first time, or when a change of the processing notification status is required. The exceptions to the obligation to notify the Commissioner on data processing concern cases when the data is being processed for the sole purpose of keeping a record, which under the law or sub-legal acts provides information for the public in general or when data are being processed for the purpose of protection of the constitutional institutions, interests of national security, foreign policy, economic or financial interests of the state, prevention or prosecution of the criminal offences. The Commissioner can issue decisions to indicate other cases of exceptions. The Law on Protection of Personal Data prescribes the content this notification should have, the procedure of examination from the Commissioner, the cases in which the authorisation of the Commissioner is required, as well as administrative sanctions in cases when controllers fail to notify the Commissioner. The applicable fines, in this case, amount between 10 000 ALL to 500 000 ALL.⁴⁰

For the ideal balance of necessity and proportionality in the exceptions made to the right of the data subject to be informed when their data is being processed or breached, consisting in an interference with the rights, freedoms, and legitimate interests of the data subject, the principle of proportionality according to the ECtHR case-law⁴¹ should be applied. According to this

³⁷ On Protection of Personal Data Law 2008, art 39 (b).

³⁸ *ibid* art 18.

³⁹ *ibid* art 21.

⁴⁰ *ibid* art 39/d.

⁴¹ European Union Agency for Fundamental Rights and Council of Europe, 2018 “Handbook on European data protection law” (2018) <https://www.echr.coe.int/Documents/Handbook_data_protection_Eng.pdf> accessed 24 May 2021.

principle, the processing of personal data constitutes lawful interference with the right to respect for private life and can only be carried out if it is in accordance with the law, pursues a legitimate aim, respects the essence of the fundamental rights and freedoms, is necessary and proportionate in a democratic society to achieve a legitimate purpose.

5. Does the review constitute effective protection of data privacy?

The Commissioner for the Protection of Personal Data is the independent authority in charge of supervising and monitoring the protection of personal data by respecting and guaranteeing fundamental human rights and freedoms in compliance with the law. The Commissioner enjoys the right to conduct administrative investigations, to have access to the processing of personal data, and to collect all information necessary to carry out his/her supervisory duties and also to order the blocking, deletion, destruction, or suspension of the illegal processing of personal data. The Commissioner can start the administrative investigation *ex officio*, or after the complaint of the data subject or controller. In case a breach of personal data is found, the Commissioner can decide to impose administrative sanctions. The Commissioner is an intermediate remedy and the data subject cannot file a lawsuit in court without exhausting it. When the data subject files a complaint, the data controller may not change the personal data until a final decision.⁴²

After exhausting the complaint mechanism at the Commissioner, the data subject has the right to file a lawsuit in the civil courts and claim non-pecuniary damage for violations to their private life, violations of their honor, personality, reputation, and for damages to their mental health.⁴³ The civil court determines the civil liability and the extent of non-pecuniary damage.

Additionally, if the breach consists of one of the criminal offences prescribed in the Criminal Code such as the intrusion into someone's privacy, spreading of personal secrets, and obstruction or violation of the privacy of correspondence, the data subject can file a lawsuit in the criminal courts. According to the Code of Criminal Procedure,⁴⁴ a person who has been caused damage from a criminal offense may file a civil lawsuit in the criminal proceedings against the defendant or civil defendant, to seek redress and compensation for the damage. The court may decide to separate the civil lawsuit and send it to the civil court if this makes the trial difficult or prolongs it.

With regards to the effects that final decisions of the civil and criminal courts have on one another, the final criminal court decision is binding on the civil court which examines the civil consequences of the offense only with regards to the fact of whether the criminal offense was committed and if it was committed by the defendant⁴⁵. Furthermore, in case a verdict of

⁴² On Protection of Personal Data Law 2008, art 16/2.

⁴³ Civil Code, art 625.

⁴⁴ Code of Criminal Procedure, art 61.

⁴⁵ *ibid* art 70.

innocence is given because the act is not prescribed as a criminal offense or when the termination of the trial is decided by the criminal court, the civil lawsuit is left unreviewed.⁴⁶ If the civil case cannot proceed without a final verdict of the criminal court, the civil court decides to suspend the case.⁴⁷ On the other hand, the final civil decision is binding on the criminal court only as to whether the offense occurred or not, but not with regards to the guilt of the defendant.⁴⁸

With regards to administrative offences, when the cases of data processing do not constitute any criminal offence the Commissioner can impose fines amounting between 10 000 to 1 000 000 ALL depending on the offence. The applicable fines are doubled in some specific cases such as when the offence is committed by a legal person; when the controller makes changes to the personal data after a complaint has been filed; or when the data are processed without the authorization of the Commissioner when this is required.

With regards to the criminal procedure, intrusion into someone's privacy is punishable by a fine or up to 2 years of prison. The spreading of personal secrets is punishable by a fine or up to 1 year of prison. If the same act is committed with the intent of embezzlement or of damaging another person is punishable by a fine or up to two years of prison. An intentional commitment of acts such as destruction, non-delivery, opening and reading of letters or any other correspondence, as well as the interruption, placement under control or tapping of telephones, telegraphs, or any other means of communication is punishable by a fine or up to two years of prison.

With regards to the civil procedure, the court determines the amount of damage and compensation depending on the case and taking into account facts such as the way, form or time of distribution of the statements or commission of actions; forms and degree of guilt; the fact whether the statements pertain to the privacy issues of the impaired person and their relationship to the public interest, etc.⁴⁹

The administrative procedure at the Commissioner and the judicial review in the civil and criminal courts altogether provide for effective remedies to the data protection breaches

6. What is the process of judicial review of anti-discrimination cases?

The judicial review is an extraordinary and exceptional form of appeal against a final decision of the court, which cannot be appealed by the usual means of appeal (appeal and recours)⁵⁰.

⁴⁶ *ibid* art 68.

⁴⁷ Code of Civil Procedure, art 297.

⁴⁸ Code of Criminal Procedure, art 71.

⁴⁹ Civil Code, art 647/a.

⁵⁰ [2013] Unifying Decision No.3/08, point 24 (Supreme Court Joint Panels).

6.1. Which bodies conduct such review? What are the elements that are taken into consideration when such review is conducted?

Based on Law No. 10221 of 4.2.2010 'On the protection against discrimination', the Commissioner on the Protection Against Discrimination is the body that ensures effective protection and any kind of conduct that encourages discrimination. The People's Advocate (Ombudsman) is another body which plays an important role in the defense of human rights and the fight against discrimination. Referring to the 6th Report of the European Commission against Racism and Intolerance for Albania⁵¹, this two bodies interact, developing a successful partnership in the fight against discrimination.

If there is a parallelism between the period before 2017 and the period after that year, there are changes to legislation concerning the competent body for the judicial review. Before 2017, the Supreme Court was liable for the case review. Meanwhile, after 2017, it is envisaged that the Supreme Court has just the functional competence to review its final judgments and the request for review falls within the jurisdiction of the court of first instance which issues the decision, but in the case that the decision is appealed to the highest courts, competent is the highest which has reviewed the case on the merit⁵².

However, all these institutions should not be confused with each other since they are distinct and perform different functions.

6.1.1. Competences of the Commissioner on the Protection Against Discrimination

The anti-discrimination legislation determines the competences of the Commissioner. Among the tasks performed by the Commissioner on the Protection against Discrimination is his duty to report once a year to the committees of the Assembly, providing a summary and interpretation of the implementation of the legislation in question, and including also the achievements throughout this period.

The commissioner analyzes complaints from individuals or groups of persons who have been discriminated against and the law also grants organizations the right to appeal on behalf of and with the written consent of individuals or groups of individuals who have been discriminated against, providing that they have a valid interest.

Among the most important competencies is the promotion of the principle of equality and non-discrimination through awareness-raising in the society, through engagement and dialogue

⁵¹ECRI Report on Albania (sixth monitoring cycle, 2020) 9.

<<https://rm.coe.int/report-on-albania-6th-monitoring-cycle-/16809e8241>> accessed 24 May 2021.

⁵²Florjan Kalaja, Dr. Arjana Fullani, *Civil Trial in the Supreme Court* (Fondacioni Shoqëria e Hapur për Shqipërinë, 2019) 172. <<https://www.magjistratura.edu.al/komentari/resources/kreu-II.html>> accessed 24 May 2021.

with social groups, including non-governmental organizations, and through the creation of educational programs.

The Commissioner also tracks the enforcement of this law as well as the law ‘On gender equality in society’, it provides information on the right to protection against discrimination and the legal means available for this protection, conducts surveys, makes recommendations to the relevant authorities and publishes reports on current legislation as well as on issues related to discrimination. It may also sue and protect concerns related to common interests.

With the amendments that have been made to the law, the Commissioner may bring an action before the Constitutional Court if he finds that the law or the normative act infringes the fundamental rights and freedoms of individuals.⁵³

6.2. Does the review constitute effective protection against discrimination?

In 2020 according to law no. 10221, dated 4.2.2010 ‘On the protection against discrimination’ some amendments have been made, such as the definition of the terms ‘discrimination’ and ‘hate speech’.

Article 1 of the aforementioned law, regulates the implementation and the monitoring of the principle of equality and non-discrimination relating to race, ethnicity, colour, language, nationality, political, religious or philosophical beliefs, economic, educational or social status, gender, gender identity, sexual orientation, sex characteristics, living with HIV / AIDS, pregnancy, parenthood, parental responsibility, age, marital status, residence, health status, genetic predispositions, appearance, ability of limited, belonging to a particular group, or for any other reason. The phrase ‘*for any other reason*’ leaves room for interpretation that discrimination can also occur through the use of technology.

Discrimination as provided in law is any difference, exception, restriction or preference, based on any cause referred in its Article 1, that has as its purpose or consequence the obstruction or impossibility, in the same way with others, of exercising the fundamental rights and freedoms recognized by the Constitution of the Republic of Albania, international acts ratified by the Republic of Albania, as well as by the laws in force.

Whereas the definition of hate speech based on the law defines any form of public expression through any means of promotion, incitement to denigration, hatred or slander, any harassment, insult, negative stereotypes, stigmatization or threat to a person or a group of persons, as well as any justification for any form of expression based on a non-exhaustive list of causes defined as ‘hate speech’.

⁵³On Protection Against Discrimination Law 124/2020 (amendment), art 32 (i/1)
<<http://www.parlament.al/Files/ProjektLigje/20201020143441ligj%20nr.%20124%20dt.%2015.10.2020.pdf>>
accessed 24 May 2021.

The meaning referred to above suggests that hate speech is governed by this law when committed '*by any means or method*', so it can be assumed that it covers hate speech happening by technological means as well as social networking sites, etc. Although this law does not directly express or regulate the discrimination by technological means, this case and Article 1 of the law make us understand that if we find hate speech on social networking sites we have the right to report it to the competent authorities responsible for the defense against discrimination.

Any action or inaction by public authorities or any person involved in the public or private sector which gives rise to the denial of equality to an individual or group of persons or which exposes them to unfair and unequal treatment constitutes discrimination. Public bodies have a duty to promote equality and to avoid discrimination in the exercise of their duties. The Constitution provides for the elimination of all privileges and unfair discrimination.⁵⁴

6.3. What is a considered role of the technical aspects that result in discrimination (such as algorithmic bias)? How are these problems tackled?

Albanian legislation does not regulate technical aspects that result in discrimination. These problems are currently not tackled at all.

7. Does your country have any specific regulations on Advanced Digital Technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?

There is currently no specific legislation in Albania on Advanced Digital Technologies, such as big data, Artificial Intelligence (AI), Internet of Things (IoT) and/or encryption. Nevertheless, between 2008-2014 timeframe a series of laws were drafted and approved which aimed to regulate the environment of business communication, create and maintain infrastructure for electronic communication for the public administration and e-governance, build broadband infrastructure, and offer e-services for the enterprises and citizens.⁵⁵

A number of sub-legal acts mainly related to e-governance have also been adopted, such as:

- Decision of Council of Ministers (DCM) No. 248, dated 27.4.20075, as amended, for the establishment and functioning of The National Agency for Information Society (NAIS);
- DCM No. 945, dated 2.11.2012, 'On the Adoption of Regulation 'Administration of the database of State Data';

⁵⁴ On the Protection Against Discrimination Law 10221/2010, art 7 <https://www.uart.edu.al/media/150329-Ligi%2010221_%202010%20per%20mbrojtjen%20nga%20%20diskrimi.pdf> accessed 24 May 2021.

⁵⁵ 'Albania Digital Agenda Observatory, Country Report and Roadmap' (2020) <<https://www.mjft.org/sites/default/files/Digital%20Agenda%20Observatory%20Albania%20June%20%2720.pdf>> accessed 19 May 2021.

- DCM No. 961, dated 24.11.2010, 'On the Establishment of the Regulatory Coordination Authority of the database of state data';
- DCM No. 357, dated 24.2.2013, 'On the Adoption of Regulation for the Management of Electronic Documents in the Republic of Albania';
- DCM No. 303, dated 31.3.2011, 'On the Establishment of Information and Communication Technological Units at the line ministry and subordinate institutions'.

Nowadays many of the government institutions in Albania digitized their systems and framework, but unfortunately in many cases, these systems have been developed without a communication strategy among them. The current innovative changes and the requirements for quick, precise, transparent and up-to-date information for citizens and businesses, necessitate that these frameworks associate with one another sharing enormous volumes of data.

Database processing and public use of information is at an early stage of development and is still considered as a future potential expectation for better governance.⁵⁶

One of these systems is e-government, an instrument, in the form of governing principles, strategies, systems and tools. The e-government development and main statistics in the e-services is described as an input for the potential of using *big data* as no current national initiatives exist in this field, renewing their administrative structure and processes.

Big data management challenges include data processing challenges, managing data across organizations and an absence of the technologies and expertise required to manage large amounts of data.⁵⁷

Also, e-government refers to the utilization of current innovation assets, and to the improvement of e-services that especially provide to the citizens, businesses, and organizations the use of modern technology.

Mostly, this platform aims at providing governmental information and services online for fast delivery and cost effectiveness. Moreover, there is a conflict between demands for privacy and those for more openness and transparency. As an example, the e-Albania portal serves as a single contact point for government services, helping to improve the overall accessibility of information to the public. Services such as access to personal data, business data, and online declaration of personal income will soon be added as e-services offered by the portal.⁵⁸

⁵⁶ Imelda Sejdini, *E-Government Implementation in Albania, as a Tool to Increase Citizens' participation and Benefits* (2010) <https://www.sobiad.org/eJOURNALS/journal_IJEBEG/archives/2010/02imelda_sejdini.pdf> accessed 19 May 2021.

⁵⁷ Ogerta Elezaj, *Big Data in e-Government Environments: Albania as a Case Study* (2018) <<https://www.mcser.org/journal/index.php/ajis/article/view/10285/9916>> accessed 19 May 2021.

⁵⁸ e-Albania (AL0040) <<https://www.opengovpartnership.org/members/albania/commitments/AL0040/>> accessed 19 May 2021.

As an initial legal basis Law No. 10 325, of 23 September 2010 On State Databases has created the primary basis for data transfer between different Government agencies.

Regarding the topic also some regulations can be found spread over several kinds of sources, laws or normative acts.

Considering here:

- Law no. 9918 dated 19.5.2008, The Electronic and Postal Communications Authority (AKEP) has approved Regulation no. 37, dated 29.10.2015 ‘On Technical and Organizational Measures to Guarantee the Security and Integrity of Electronic Networks and / or Services’⁵⁹.
- Law No 9887 date 10.03.2008, ‘On Protection of Personal Data’, as amended;
- Law No 119/2014 ‘On the right to information’;
- Law No. 9918, date 19.05.2008, ‘On electronic communications in the Republic of Albania’ as amended;

Based on the analysis of technological developments mentioned above, there are no initiatives for the regulation of Big Data and no technology is being developed to respond to these huge data capacities.⁶⁰

8. Does your country’s legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?

The Constitution of the Republic of Albania guarantees the confidentiality of communications or of any means of communication⁶¹, but also allows the restriction of rights and freedoms by statute, for the benefit of the public or for the preservation of the rights of others. These limitations do not go beyond the provisions of the European Convention on Human Rights⁶².

Albanian's legislation does not explicitly regulate encryption, but in order to facilitate the continuation of a criminal investigation, the competent authorities can, listen to or tap the telephone communications of the suspect or of the individual under investigation for the commission of a specific offense.

8.1. Specify the circumstances in which such decryption may be conducted. What are the potential or real consequences of such a requirement?

In order to provide the requisite facts to prove whether or not a criminal offence has been committed, the Criminal Procedure Code of the Republic of Albania provides that eavesdropping is one of the ways of providing evidence by which information of communication

⁵⁹ Regulation No. 37, dated 29.10.2015 ‘On Technical and Organizational Measures to Guarantee the Security and Integrity of Electronic Networks and / or \Services’
<http://www.akdie.org/sites/default/files/ligji_per_komunikimet_elektronike.pdf> accessed 20 May 2021.

⁶⁰ Elezaj (n 57).

⁶¹ Constitution of the Republic of Albania, art 36.

⁶² Criminal Procedure Code of the Republic of Albania, art 17.

of any kind, type or manner, between two or more individuals, is collected or obtained secretly, without the knowledge of the individual being eavesdropped.⁶³

Communication means the sharing or transmission of information between a small number of users, without including the transmission of information that is part of radio and television broadcasting by electronic communications networks, except where the information may apply to the subscriber or well-known user who receives the information.⁶⁴

8.1.1. Limits and circumstances allowing wiretaps by the competent bodies

Pursuant to letters a, b and c, paragraph 1 of Article 221 of the Code of Criminal Procedure, wiretaps on private places are allowed only for offenses for which a sentencing of minimum seven years is imposed; for any intentional criminal offense committed by means of telecommunications or the use of information or telematics technology; for criminal offences referred to in paragraph 1 of Article 75/a, letter 'a' of the Criminal Procedure Code.

In the same Article, the second paragraph stipulates that wiretapping can also be carried out in public areas, but only on one condition, for offences for which a sentence of imprisonment of not less than three years is imposed.

Referred to Article 37 of the Constitution of the Republic of Albania (as this Code does not include a description of what is considered as 'private place'), the 'residence' may be a private place in a narrow sense and, by reference to the Supreme Court's jurisprudence 'private place' may be a house or office where a person who enters is 'under the control of his owner'.

There is also no specification of the concept 'public place' in the Code of Criminal Procedure. The Venice Commission describes it as an area that anyone can easily access, theoretically, without prejudice, in any case, at any time.⁶⁵

As regards the fact to which subjects the interception may be ordered, Article 221(3) of the Criminal Procedure Code defines the categories of subjects which may be: suspected of committing a criminal offence, suspected of receiving or transmitting communications from the suspect and the person involved in transactions with the suspect or person whose observation may lead to the discovery of a crime.

8.1.2. Transmission of the stored data

⁶³ D Lara, Commentary on Criminal Procedure (Morava Publications 2019) 715.

⁶⁴ On Electronic Communications Law 2008, art 3, para 1

<https://www.idp.al/wp-content/uploads/2020/12/Ligj_9918_dt.19.05.2008_Per_komunikimet_elektronike_i_ndr_yshuar_2020.pdf> accessed 24 May 2021.

⁶⁵ Opinion of the Venice Commission on video surveillance in public places by public authorities and the Defense of Human Rights, adopted by the Venice Commission at its 70th Plenary Session (16-17 March 2007) 4 <[https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2007\)014-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)014-e)> accessed 24 May 2021

Through criminal proceedings in the field of technology, the court may, at the request of the prosecutor or the accused victim, order the holder or controller to transmit the stored data to a database server or other storage device. It can also order the contractor to provide customers with all the basic features of the services offered by the service provider.⁶⁶

8.1.3. Seizure of computer data

In the case of information technology offences, the court can determine the right to view, request and obtain computer data on the computer system.

The prosecution or judicial police officer, delegated by the prosecutor, can take measures such as stopping further action or securing the computer system and for this procedure the Prosecutor may order the summoning of an expert who is aware of the functioning of computer systems.⁶⁷

8.2. Does this requirement (in general or in practice) provide the authorized body with too much power? Clarify your answer.

An important notion in article 221 of Criminal Procedure Code is '*secret interception*' of communications in private areas by technical means. Interception of communications is confidential because the legislation empowers the authorities to perform a discreet interception of communications between citizens in private places, without requiring the authorities to alert them of any action taken against them⁶⁸.

Wiretapping in public places or the use of location monitoring devices can be decided upon by the prosecutor without the intervention of the court and without the need for authorisation/validation of wiretapping. Since wiretapping in a public place constitutes a minor interference with the constitutional rights of privacy, family and correspondence, the legislature requires for wiretapping action to be approved only by the prosecutor without a request for a court decision.⁶⁹

Article 222, paragraph 6, of the Criminal Procedure Code sets out the particular case of a judicial police officer or a competent expert who must secretly access a private premise for interception of communications or taking photos or filming. As this constitutes a particular interference with the constitutional right to privacy and family life, paragraph 6 sets out the requirement of a court authorisation in such a case. This means that the prosecutor must indicate and justify the need in the request for authorisation, confirmation or extension of the interception, and the court must then expressly allow the access to these sites in secret⁷⁰.

⁶⁶ Criminal Procedure Code (n 62), art 191/a, paras (1) (2)

<http://www.pp.gov.al/web/kodi_i_procedures_penale_date_30_gusht_2017_1201.pdf> accessed 24 May 2021.

⁶⁷ *ibid* art 208/a, paras (3) (4).

⁶⁸ Electronic Commentary of the Magistrature, comments on different issues of the provision (which provision), para 4 <<http://komentarielektronik.magiistratura.edu.al/sq/eli/fz/2017/7905/221>> accessed 24 May 2021.

⁶⁹ *ibid*.

⁷⁰ *ibid*.

The dissemination or use of the data obtained during the interception procedures without any prior permission from the competent body is categorically prohibited for persons participating in the interception process. Any activity outside the provisions of the law is prohibited, as the wiretapping procedure is a state secret, the breach of which is punishable by applicable criminal law.⁷¹ In *Antovic and Mirkovic v. Montenegro* case the European Court of Human Rights held that *‘video surveillance of an employee in the workplace, be it covert or not, must be considered as a considerable intrusion into the employee’s private life and hence it considers that it constitutes an interference within the meaning of Article 8.’*⁷²

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?

The Internet has fundamentally changed the way we access information, creating new opportunities for strengthening and fortifying democracy. Unfortunately, it can likewise be utilized to restrict human rights and to commit crimes.

Albania, as well as other countries, is facing the issues of protecting human rights online. With these new forms of technology which have come in our way, new legal challenges are presented in every state to revise the legal framework with respect to human rights.

As a field of law, human rights are constantly affected by new changes; the more the technology evolves the bigger the need to protect human rights in every legal system. The development of these technologies brings up significant issues about whether our current policies, legal framework, and advocacy strategies are adequate to mitigate the human rights risks that may result, many of which are yet unclear.

During the years, one of the challenges on human rights in our country has been the protection of personal data. In this direction, on 14 February 2004 Albania has ratified the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data and Law no. 9887, dated 10.03.2008 ‘On the protection of personal data’ has been amended accordingly by the law no. 48/2012.

The Law is equally applicable for each of the following subjects:

- data controllers established in the Republic of Albania;
- diplomatic missions or consular offices in Albania;
- data controllers who are not established in the Republic of Albania, but make use of any equipment located in the Republic of Albania;

⁷¹ On the Interception of Electronic Communications Law 2003, art 16
<<https://www.shish.gov.al/files/Ligjet/Ligji%20nr.9157,%20dat%C3%AB%204.12.2003.pdf>> accessed 24 May 2021.

⁷² *Antovic and Mirkovic v. Montenegro* [2018], para 55 <[CASE OF ANTOVIC AND MIRKOVIC v. MONTENEGRO.pdf](#)> accessed 24 May 2021.

- public authorities processing data in the framework of crime prevention and prosecution activities, in cases of criminal offences against public order and other violations in the field of criminal law, and national security.

To achieve the objectives of the Convention, the directive requires the establishment of an independent national authority responsible for the protection of personal data for each Member State. For the implementation of this Convention in Albania an independent institution was set up, the Commissioner for Personal Data Protection.⁷³

Albanian data protection legislation is further undergoing a process of approximation with the EU *acquis communautaire* and seems to follow the guidelines of the European Commission.

10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the upcoming five years?

Taking into consideration the analysis in our contribution, we conclude that our country does not provide adequate protection of human rights in the online environment. However, we believe that despite these legislative gaps the Republic of Albania will establish effective and model legislation in order to address these rapidly evolving challenges in the digital era.

In order to identify and address the contemporary challenges arising from advanced digital technologies, laws, case law and research need to advance quickly to respond to the speed in which digital technologies advance, and to be able to tackle the new societal realities and challenges posed to human rights.

Putting aside our expectations as citizens from the legislator to progress and develop the area of protecting human rights online, the upcoming year will most probably determine the level of protection of human rights and international standards in Albania. Up to date, uncertainty whether institutions aim at respecting and protecting human rights remains. To explain why, we will give a short reflection of how personal data of Albanian citizens are alleged to have been *violated*⁷⁴ recently. On 11 April, an Albanian media portal published a database containing personal data and private information of 910,000 individuals, allegedly maintained by the country's ruling Socialist Party. It was revealed – and since then confirmed – that 'patrons' were assigned to voters who tracked their political preferences (who they were likely to vote – note

⁷³ Paulina Hoti and Florian Bjanku, *The Data Protection in Albania and the Enhancing of The Respective Commissioner in The Framework Of Last Legal Reforms*

<<http://dspace.epoka.edu.al/bitstream/handle/1/1002/THE%20DATA%20PROTECTION%20IN%20ALBANIA%20AND%20THE%20ENHANCING%20OF%20THE%20RESPECTIVE%20COMMISSIONER%20IN%20THE%20FRAMEWORK%20OF%20LAST%20LEGAL%20REFORMS%20Paulina%20Hoti%20and%20Florian%20Bjanku.pdf?sequence=1&isAllowed=y>> accessed 20 May 2021.

⁷⁴ Investigations are being carried out by the Special Anti-Corruption Structure, therefore it is still not determined if there has been a breach of personal data protection or if the incumbent party abused state resources (obtaining personal data from state institutions) for securing a win in parliamentary elections.

added).⁷⁵ Further data such as name, surname, birthday, personal identification number, place of work, voting center, place of birth, residence code, phone number etc. were recorded by the ‘patrons’. The Prime Minister confirmed the existence of the ‘patron’ system but claimed that citizens’ data was collected through door-to-door meetings.

Competent authorities have commenced an investigation and the process is still undergoing, however as Mr. Eriksson, Chief Executive Officer of Transparency International Secretariat said ‘The failure to adequately investigate and sanction wrongdoing will cast a shadow over the fairness of the upcoming election’. Not only of the upcoming elections but if allegations proven, it would constitute a breach of personal data and public trust. Having said that, since institutions are still struggling to protect personal and sensitive data in spite of the existence of a Data Protection Law that stipulates procedures and steps to collect and use personal information, an immediate intervention to ensure that the right to privacy and personal data will not be sold or misused.

The results of the above mentioned case will most probably serve as the foundation for the way forward to the protection of human rights in the digital era in Albania. As mentioned in previous sections, human rights such as freedom of expression, right to information, protection from hate speech and discrimination, right to private life, protection of personal data and privacy of communication, protection from sexual harassment etc. as well as delivery of accurate information to the public is at risk, therefore it is of utmost importance to address these issues by proposing, adopting and implementing relevant laws on Artificial Intelligence and protection of personal data. In this sense, we strongly believe that public and private actors will engage to establish or develop regulatory frameworks on Advanced Digital Technologies, such as big data, artificial intelligence, Internet of Things and/or encryption, with special aim at approximating the national legislation to the EU standards as well as to protecting and respecting human rights online in the same extent as offline. Lastly, international human rights law and universal principles have to guide the legislator and the government therefore the legislation regarding the area of protecting human rights online shall certainly develop and provide safeguards to prevent any breach of human rights.

Conclusion

As lined out in this report, Albania is facing the issues of protecting human rights online. With these new forms of technology which have come in our way, new legal challenges are presented in every state to revise the legal framework with respect to human rights.

⁷⁵ Transparency International, *Albania: Alarm over indications of personal data breach, election campaign violations*. <<https://www.transparency.org/en/press/albania-alarm-over-indications-of-personal-data-breach-election-campaign-violations#>> accessed 1 June 2021.

To start with, it is important to highlight the main issues and gaps with regard to protecting human rights online: (i) currently there is no specific legislation into effect in Albania on Advanced Digital Technologies (ii) although the Commissioner on Data Protection adopted a strategy aiming at harmonizing the Law No. 9887, dated 10.3.2008 'On Personal Data Protection' with the GDPR, there has been no practical endeavours to tackle this issue; (iii) Public and private sector need to strengthen their cooperation and work closely towards generating a set of best practises with regard to the protection of digital human rights.

Mechanisms to build a better online environment, monitor and enforce digital human rights, develop legal models underpinning the updated concept of human rights are crucial for the protection and consolidation of human rights online. Therefore, the government and relevant institutions hold the responsibility to act accordingly and in line with the rapid technological developments.

Table of legislation

Provision in Albanian	Corresponding translation in English
Kushtetuta e Republikës së Shqipërisë, <i>e ndryshuar</i> .	Constitution of the Republic of Albania, <i>as amended</i> .
Neni 35: 1. Askush nuk mund të detyrohet, përveçse kur e kërkon ligji, të bëjë publike të dhëna që lidhen me personin e tij. 2. Mbledhja, përdorimi dhe bërja publike e të dhënave rreth personit bëhet me pëlqimin e tij, me përjashtim të rasteve të parashikuara me ligj. 3. Kushdo ka të drejtë të njihet me të dhënat e mbledhura rreth tij, me përjashtim të rasteve të parashikuara me ligj. 4. Kushdo ka të drejtë të kërkojë ndreqjen ose fshirjen e të dhënave të pavërteta ose të paplota ose të mbledhura në kundërshtim me ligjin.	Article 35: 1. No one may be obliged, except when required by law, to make public information relating to his person. 2. The collection, use and publication of data about the person is done with his consent, except in cases provided by law. 3. Everyone has the right to be acquainted with the data collected about him, except in cases provided by law. 4. Everyone has the right to request the correction or deletion of untrue or incomplete data or collected in violation of the law.
Neni 36: Liria dhe fshehtësia e korrespondencës ose e çdo mjeti tjetër të komunikimit janë të garantuara.	Article 36: Freedom and confidentiality of correspondence or any other means of communication shall be guaranteed.

Provision in Albanian	Corresponding translation in English

Ligji Nr. 9887, datë 10.3.2008 “Për mbrojtjen e të dhënave personale”, ndryshuar me Ligjin Nr. 120/2014 ‘Për disa ndryshime dhe shtesa në Ligjin Nr. 9887, datë 10.3.2008 Për mbrojtjen e të dhënave personale”	Law No. 9887, dated 10.3.2008 ‘On Personal Data Protection’, amended with Law No. 120/2014 ‘On Some amendments and additions to Law No. 9887, dated 10.3.2008 On Personal Data Protection’
Neni 3 (1) (4): “<i>Të dhëna personale</i>” është çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm, direkt ose indirekt, në veçanti duke iu referuar një numri identifikimi ose një a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social. “<i>Të dhëna sensitive</i>” është çdo informacion për personin fizik, që ka të bëjë me origjinën e tij, racore ose etnike, mendimet politike, anëtarësimin në sindikata, besimin, fetar apo filozofik, dënimin penal, si dhe të dhëna për shëndetin dhe jetën seksuale.	Article 3 (1) (4): ‘<i>Personal data</i>’ refers to any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. ‘<i>Sensitive data</i>’ includes any piece of information related to the natural person in referring to his racial or ethnic origin, political opinions, trade union memberships, religious or philosophical beliefs, criminal prosecution, as well as with data concerning his health and sexual life.
Neni 3/5: “Kontrollues” është çdo person fizik ose juridik, autoritet publik, agjenci apo njësi tjetër, të cilët, vetëm apo në bashkëpunim me të tjerë, mbajnë, përpunojnë, administrojnë, arkivojnë dhe për këtë shkak kontrollojnë të dhëna personale.	Article 3/5: ‘Controller’ shall mean the natural or legal person, public authority, agency or any other body, which alone or jointly with others determines the purposes and means of the processing of personal data, in compliance with the laws and secondary legal acts applicable, and who is responsible for the fulfilment of obligations defined by this law.
Nen 9:	Article 9: 1. International transfer of personal data to a state that does not have a sufficient level of

1. Transferimi ndërkombëtar i të dhënave personale me një shtet, që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave, në raste të tjera nga ato të parashikuara në nenin 8 të këtij ligji, bëhet me autorizim të komisionerit. 2. Komisioneri, pasi bën vlerësimin, mund të japë autorizimin për transferimin e të dhënave personale në shtetin marrës, duke përcaktuar kushte dhe detyrime. 3. Komisioneri nxjerr udhëzime për lejimin e disa kategorive të transferimeve ndërkombëtare të të dhënave personale në një shtet që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave personale. Në këto raste, kontrolluesi përjashtohet nga kërkesa për autorizim. 4. Kontrolluesi, përpara transferimit të të dhënave, bën kërkesë për autorizim te komisioneri. Në kërkesë kontrolluesi duhet të garantojë respektimin e interesave për ruajtjen e sekretit të subjektit të të dhënave jashtë Republikës së Shqipërisë.	data protection, in cases other than those provided in Article 8 of this law, is completed by an authorization of the commissioner. 2. The commissioner, after an assessment, may authorize the transfer of personal data to the receiving state, setting conditions and obligations. 3. The Commissioner issues instructions for allowing certain categories of international transfers of personal data to a country that does not have a sufficient level of personal data protection. In these cases, the controller is exempted from the request for authorization. 4. The controller, prior to transferring the data, requests authorization from the commissioner. In the request the controller must guarantee the observance of the interests for the protection of the confidentiality of the data subject outside the Republic of Albania.
Neni 21 1.Çdo kontrollues duhet të njoftojë komisionerin për përpunimin e të dhënave personale, për të cilat është përgjegjës. Njoftimi duhet të bëhet para se kontrolluesi të përpunojë të dhënat për herë të parë ose kur kërkohet ndryshimi i qëllimit të përpunimit, të njoftuar më parë. 2. Përjashtohet nga detyrimi për të njoftuar përpunimi i të dhënave personale, me qëllim	Article 21: 1. Each controller must notify the commissioner about the processing of personal data, for which he is responsible. The notification must be made before the controller processes the data for the first time or when a change of the purpose of processing is sought, which is notified in advance.

mbajtjen e një registri, i cili, në përputhje me ligjin ose aktet nënligjore, siguron informacion për publikun në përgjithësi. 3. Përjashtohen nga detyrimi për të njoftuar të dhënat personale që përpunohen, me qëllim mbrojtjen e institucioneve kushtetuese, të interesave të sigurisë kombëtare, politikës së jashtme, interesave ekonomikë ose financiarë të shtetit, apo për parandalimin e ndjekjen e veprave penale. 4. Rastet e tjera, për të cilat njoftimi nuk është i nevojshëm, përcaktohen me vendim të Këshillit të Ministrave.	2. It is exempted from the obligation to notify the processing of personal data, in order to maintain a register, which, in accordance with the law or bylaws, provides information to the general public. 3. They are exempted from the obligation to notify the processing of personal data, in order to protect constitutional institutions, national security interests, foreign policy, economic or financial affairs of the state, or for the prevention and prosecution of criminal offenses. 4. Other cases, for which notification is not necessary, are determined by a decision of the Council of Ministers.
Neni 6/1 (dh) 1. Të dhënat personale përpunohen vetëm: dh) për ndjekjen e interesave legjitimë të kontrolluesit ose të një pale të tretë, së cilës i janë përhapur të dhënat, përveç kur këta interesa mbizotërojnë mbi interesat për mbrojtjen e të drejtave dhe të lirive themelore të subjektit të të dhënave.	Article 6/1 (dh): 1. Personal data shall be processed only: dh) for the pursuit of the legitimate interests of the controller or of a third party to whom the data have been disseminated, except where those interests prevail over the interests of the protection of the fundamental rights and freedoms of the data subject.
Neni 39/1/b/d: 1. Rastet e përpunimit të të dhënave në kundërshtim me dispozitat e këtij ligji përbëjnë kundërvajtje administrative dhe dënohen me gjobë, si më poshtë: b) kontrolluesit, që nuk përmbushin detyrimin për të informuar, të përcaktuar në nenin 18 të këtij ligji, dënohen me 10 000 deri në 30 000 lekë;	Article 39/1 /b / d: 1. Cases of data processing in contradiction with the provisions of this law constitute administrative contraventions and are punished with a fine, as follows: b) controllers, who do not fulfill the obligation to inform, defined in article 18 of this law, shall be punished by a fine of ALL 10 000 to 30 000;

d) kontrolluesit, që nuk përmbushin detyrimin për të njoftuar, sipas përcaktimit në nenin 21 të këtij ligji, dënohen me 10 000 deri në 50 000 lekë;	d) controllers, who do not fulfill the obligation to notify, according to the definition in article 21 of this law, shall be punished by a fine of ALL 10 000 to 50 000;
Neni 16/2: Në rast se subjekti i të dhënave ka bërë ankim, kontrolluesi nuk ka të drejtë të ndryshojë të dhënat personale deri në dhënien e vendimit përfundimtar.	Article 16/2: If the data subject has appealed, the controller has no right to change the personal data until the final decision is given.

Provision in Albanian	Corresponding translation in English
Kodi Civil	Civil Code
Neni 625: Personi që pëson një dëm jopasuror ka të drejtë të shpërblehet kur: a) ka pësuar një dëmtim të shëndetit, të integritetit fizik ose psikik të tij; b) është cenuar nderi, personaliteti ose reputacioni i tij; c) është cenuar e drejta e emrit; ç) është cenuar respektimi i jetës private; d) është cenuar kujtimi i një të vdekuri. Në këtë rast bashkëshorti i personit të vdekur ose të afërmit e tij deri në shkallë të dytë mund të kërkojnë shpërblimin e dëmit jopasuror.	Neni 625: A person who suffers a non-pecuniary damage is entitled to be compensated when: a) has suffered damage to his health, physical or mental integrity; b) his honor, personality or reputation has been violated; c) the right to a name has been violated; ç) respect for private life has been violated; d) the memory of a deceased person is violated. In this case the spouse of the deceased person or his relatives up to the second degree can claim compensation for non-pecuniary damage.

Provision in Albanian	Corresponding translation in English
Kodi I Procedurës Penale	Code of Criminal Procedure
Neni 61: Ai që ka pësuar dëm nga vepra penale ose trashëgimtarët e tij mund të ngrejë padi civile në procesin penal kundër të pandehurit ose të paditurit civil, për të kërkuar kthimin e pasurisë dhe shpërblimin e dëmit.	Article 61: A person who has incurred damage from a criminal offense or his heirs may file civil lawsuits in criminal proceedings against the defendant or civil defendant, seeking the return of property and compensation for damage.
Neni 68: 1. Gjykata, sipas rastit, pranon tërësisht ose pjesërisht padinë civile ose e rrëzon atë. 2. Kur jepet vendim pafajësie, për shkak se fakti nuk parashikohet si vepër penale ose kur vendoset pushimi i çështjes penale, padia civile lihet e pashqyrtuar. 3. Kur rrëzohet padia civile në procesin penal, nuk lejohet ngritja e saj përsëri në gjykatën civile.	Article 68: 1. The court, as the case may be, accepts in whole or in part the civil suit or dismisses it. 2. When a verdict of not guilty is rendered, because the fact is not provided as a criminal offense or when the dismissal of the criminal case is decided, the civil lawsuit is left unreviewed. 3. When the civil lawsuit is dismissed in the criminal process, it is not allowed to file it again in the civil court.

Provision in Albanian	Corresponding translation in English
Kodi I Procedurës Civile:	Code of Civil Procedure:
Neni 297: Gjykata vendos pezullimin e gjykimit kur:	Article 297: The court decides to suspend the trial when:

a) çështja nuk mund të zgjidhet para se të zgjidhet një çështje tjetër penale, civile ose administrative; b) kërkohet nga të dyja palët; c) njëra nga palët vdes ose mbaron personi juridik; ç) njëra nga palët nuk ka ose më vonë ka humbur zotësinë juridike për të vepruar si palë dhe shihet e nevojshme t'i emërohet një përfaqësues ligjor; d) parashikohet shprehimisht në ligj. dh) njëra nga palët paraqet kërkesën për zgjidhje të çështjes me ndërmjetësim dhe gjykata e vlerëson të arsyeshme. Gjatë pezullimit nuk mund të kryhen veprime procedurale.	a) the case cannot be resolved before another criminal, civil or administrative case is resolved; b) required by both parties; c) one of the parties dies or the legal person dies; ç) one of the parties has not or later lost the legal capacity to act as a party and it is deemed necessary to appoint a legal representative; d) is expressly provided by law. dh) one of the parties submits the request for resolution of the case through mediation and the court deems it reasonable. No procedural actions can be performed during the suspension.

Provision in Albanian	Corresponding translation in English
Ligj Nr. 10 221, datë 4.2.2010 ‘Për Mbrojtjen nga Diskriminimi’:	Law No. 10221, dated 4 February 2010 ‘On the Protection against Discrimination’:
Neni 7: 1. Çdo veprim ose mosveprim i autoriteteve publike ose i personave fizikë a juridikë që marrin pjesë në jetën dhe sektorët publikë ose privatë, që krijojnë baza për mohimin e barazisë ndaj një personi apo grupi personash, ose që i ekspozon ata ndaj një trajtimi të padrejtë dhe jo të barabartë, kur ata ndodhen në rrethana të njëjta ose të ngjashme, në krahasim me persona të tjerë	Article 7: 1. Any action or inaction of public authorities or of natural or legal persons participating in the life and public or private sectors, which creates grounds for denial of equality to a person or group of persons, or which exposes them to unfair treatment and unequal, when they are in the same or similar circumstances, compared to

ose grupe të tjera personash, përbën diskriminim.	other persons or other groups of persons, constitutes discrimination.
2. Eliminimi i të gjitha privilegjeve dhe i diskriminimit të padrejtë, garantohet për cilindo, në bazë të të drejtave vetjake, politike, ekonomike, shoqërore dhe kulturore të siguruara nga Kushtetuta e Republikës së Shqipërisë dhe aktet ndërkombëtare të ratifikuara nga Republika e Shqipërisë, si dhe nga ligjet në fuqi.	2. The elimination of all privileges and unfair discrimination is guaranteed to anyone, based on personal, political, economic, social and cultural rights provided by the Constitution of the Republic of Albania and international acts ratified by the Republic of Albania, as and by applicable laws.

Provision in [native] language	Corresponding translation in English
Ligj Nr. 124/2020 Për disa shtesa dhe ndryshime në Ligjin Nr. 10 221, datë 4.2.2010 “Për Mbrojtjen nga Diskriminimi”:	Law No. 124/2020 On Some Additions and Amendments to the Law No. 10221, dated 4 February 2010 “On the Protection against Discrimination”:
Neni 32, paragrafi i/1: “të vërë në lëvizje Gjykatën Kushtetuese, kur gjatë veprimtarisë së tij konstaton se ligji ose akti normativ cenon të drejtat dhe liritë themelore të individëve.”	Article 32, paragraph i / 1: ‘to set in motion the Constitutional Court, when during its activity finds out that the law or normative act violates the fundamental rights and freedoms of individuals’.

Provision in [native] language	Corresponding translation in English
Kodi Penal	Criminal Code
Neni 121: Vendosja e aparaturave që shërbejnë për dëgjim apo regjistrim të fjalëve ose të	Article: 121: Installation of devices for listening or recording words or pictures, listening or recording words,

figurave, dëgjimi ose regjistrimi i fjalëve, fiksimi ose regjistrimi figurave, si dhe ruajtja për publikim i të dhënave që ekspozojnë një aspekt të jetës private të personit, pa pëlqimin e tij, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim deri në dy vjet. Shpërndarja, ofrimi për publikim apo publikimi me çdo mjet ose formë të komunikimit publik apo mënyrë tjetër i të dhënave të marra në mënyrën e përcaktuar në paragrafin e parë të këtij neni, dënohet me burgim deri në tre vjet. Po kjo vepër, kur kryhet ndaj personave të mitur, dënohet me burgim nga një deri në tre vjet. Kur vepra penale kryhet nëpërmjet shfrytëzimit të funksionit shtetëror ose shërbimit publik apo nga personi që disponon këto të dhëna për shkak të detyrës shtetërore apo shërbimit publik, dënohet me burgim nga një deri në tre vjet.	fixing or recording pictures, as well as storing for publication data that expose an aspect of a person's private life, without his consent, constitutes criminal offense and punishable by a fine or by imprisonment of up to two years. Dissemination, offering for publication or publication by any means or form of public communication or other means of data obtained in the manner specified in the first paragraph of this article, is punishable by imprisonment of up to three years. The same offense, when committed against minors, is punishable by imprisonment of one to three years. When the criminal offense is committed through the use of state function or public service or by the person who possesses this data due to state duty or public service, it is punished with imprisonment of one to three years.
Neni 122: Përhapja e një sekreti që i përket jetës private të një personi nga ai që e siguron atë për shkak të detyrës ose të profesionit, kur detyrohet të mos e përhapë pa qenë i autorizuar, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në një vit. Po kjo vepër, e kryer me qëllim fitimi ose për të dëmtuar një person tjetër, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në dy vjet.	Article 122: Dissemination of a secret relating to the private life of a person by the one who secures it due to duty or profession, when he is forced not to disclose it without being authorized, constitutes a criminal offense and is punishable by a fine or imprisonment of up to one vit. The same offense, committed for profit or to harm another person, constitutes a criminal offense and is punishable by a fine or imprisonment of up to two years.

Neni 123:	Article 123:
Kryerja me dashje e veprimeve të tilla si asgjësimi, mosdorëzimi, hapja dhe leximi i letrave apo çdo korrespondencë tjetër, si dhe ndërprerja ose vënia nën kontroll, dëgjimi i bisedave telefonike, telegrafike ose i çdo mjeti tjetër telekomunikimi, përbën kundërvajtje penale dhe dënohet me gjobë ose burgim gjer në dy vjet.	Intentionally committing acts such as destruction, non-delivery, opening and reading of letters or any other correspondence, as well as interruption or controlling, listening to telephone conversations, telegraphs or any other means of telecommunication, constitutes a criminal offense and is punishable by a fine or imprisonment for up to two years.

Provision in Albanian	Corresponding translation in English
Ligj Nr. 9918, datë 19.5.2008 “Për Komunikimet Elektronike”:	Law nr.9918, 19.5.2008 “On Electronic Communications”:
Neni 121:	Article 121:
1. Sipërmarrësit duhet të marrin masa ndaj sistemeve të komunikimeve elektronike dhe të përpunimit të të dhënave, për të mbrojtur sekretin e komunikimeve elektronike dhe të të dhënave vetjake, si dhe për të ndaluar aksesin e paautorizuar në sistemet e komunikimeve elektronike dhe të përpunimit të të dhënave. 2. Sipërmarrësi, të autorizuarit dhe punonjësit e tij detyrohen të ruajnë e të mbrojnë të dhënat dhe fshehtësinë e komunikimeve, që kryhen nëpërmjet rrjetit e shërbimeve të tij gjatë gjithë periudhës së kryerjes së veprimtarisë, por dhe pas përfundimit të saj. 3. Sipërmarrësi mund të marrë dijeni për mesazhe ose të dhëna të transmetuara nëpërmjet rrjetit të tij, vetëm në masën që i	1. Entrepreneurs should take measures against electronic communications and data processing systems, to protect the secrecy of electronic communications and personal data, as well as to prevent unauthorized access to electronic communications and data processing systems. data. 2. The entrepreneur, the authorized person and his employees are obliged to preserve and protect the data and the secrecy of the communications, which are performed through the network of his services during the whole period of the activity, but also after its completion. 3. The entrepreneur may become aware of messages or data transmitted through his network, only to the extent that he needs to perform the task in providing electronic communications services.

nevojitet për të kryer detyrën në sigurimin e shërbimeve të komunikimeve elektronike. 4. Ndalohen marrja, regjistrimi, publikimi dhe përdorimi i të dhënave dhe i mesazheve të transmetuara nga rrjeti i komunikimeve elektronike dhe që nuk janë për publikun, si dhe dhënia e tyre personave të paautorizuar, për sa kohë që nuk përcaktohet ndryshe në legjislacionin në fuqi.	4. It is prohibited to receive, record, publish and use data and messages transmitted by the electronic communications network and which are not for the public, as well as the provision of to unauthorized persons, unless otherwise provided by applicable law.

Bibliography

English titles

Legislation

The Constitution of the Republic of Albania.

Law No. 7850, dated 29 July 1994 ‘On the Civil Code of the Republic of Albania’, *as amended*.

Law No. 8116, dated 29 March 1996 ‘Civil Procedure Code of the Republic of Albania’, *as amended*.

Law No. 7895, dated 27 January 1995 ‘Criminal Code of the Republic of Albania’, *as amended*.

Law No. 7905, dated 21 March 1995 ‘Criminal Procedure Code of the Republic of Albania’, *as amended*.

Law No. 9887, dated 10.3.2008 ‘On Personal Data Protection amended with Law No. 20/2014 “On Some amendments and additions to Law No. 9887, dated 10.3.2008 On Personal Data Protection” (Personal Data Protection Law).

Stabilization and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Albania, of the other part [2009] (OJ L107/166).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L119/1).

Law No. 124/2020 “On Some Additions and Amendments to the law no.10221, dated 4 February 2010 ‘On the Protection against discrimination’.

Law No. 9918, dated 19 May 2008 ‘On Electronic Communications’.

Law No. 10 325, dated 23 September 2010 ‘On State Databases’.

Regulation No. 37, dated 29 Tetor 2015 ‘On Technical and Organizational Measures to Guarantee the Security and Integrity of Electronic Networks and / or Services’.

Articles

Eversheds Sutherland, ‘Data Protection across all borders? GDPR’s territorial scope’ (Lexology 2020)

<<https://www.lexology.com/library/detail.aspx?g=2e9ac1a4-ffa3-4c25-99e7-3f9665fd815a>> accessed 31 May 2021.

Hoti P, Bjanku F, *The Data Protection in Albania and the enhancing of the respective Commissioner in the Framework of last Legal Reforms*

<<http://dspace.epoka.edu.al/bitstream/handle/1/1002/THE%20DATA%20PROTECTION%20IN%20ALBANIA%20AND%20THE%20ENHANCING%20OF%20THE%20RESPECTIVE%20COMMISSIONER%20IN%20THE%20FRAMEWORK%20OF%20LAST%20LEGAL%20REFORMS%20Paulina%20Hoti%20and%20Florian%20Bjanku.pdf?sequence=1&isAllowed=y>> accessed 22 May 2021.

Kurti M, 'The Impact of GDPR On Private Law: Challenges Of Business Liability And Personal Data Protection In Albania' (2019) bogalawjournal <<http://bogalawjournal.com/the-impact-of-gdpr-on-private-law/>> accessed 12 May 2021.

Kalaja F, Dr. Fullani A, *Civil Trial in the Supreme Court* (Fondacioni Shoqëria e Hapur për Shqipërinë, 2019) 172.

<<https://www.magjistratura.edu.al/komentari/resources/kreu-II.html>> accessed 24 May 2021

Land K. Molly, D. Jay (2020) Aronson *Human Rights and Technology: New Challenges to Justice and Accountability*.

Ogerta E. *Big Data in e-Government Environments: Albania as a Case Study* (2018) 123 <<https://www.mcser.org/journal/index.php/ajis/article/view/10285/9916>> accessed 22 May 2021.

Research Division, 'Internet: case-law of the European Court of Human Rights' (2015)

<https://www.echr.coe.int/documents/research_report_internet_eng.pdf> accessed 24 May 2021.

Digital resources (Reports and Manuals)

Does the GDPR apply to companies outside the EU? <<https://gdpr.eu/companies-outside-of-europe/#:~:text=The%20GDPR%20does%20apply%20outside,%E2%80%9Cextra%2Dterritorial%20effect.%E2%80%9D>> accessed 12 May 2021.

'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf> accessed 12 May 2021.

Handbook on European data protection law 2018 edition

<https://www.echr.coe.int/Documents/Handbook_data_protection_Eng.pdf> accessed 22 May 2021.

Human rights in the digital age

<<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E> > accessed 22 May 2021.

ProCredit Bank, Privacy Policy (2018)
<https://www.procreditbank.com.al/Uploads/Data/Files/157/PolitikaeprivatesisePCBALB_rVfqVARNtU.pdf?fbclid=IwAR20Qbpl_U7ROeSwsgbyHh9psvBpEqucDFZ41XsA7VZ0lRxZZnDMpRHiE0M > accessed 17 May 2021.

Strategy 2018-2020 on the Right to Information and Protection of Personal Data, 18
<https://www.idp.al/wp-content/uploads/2018/02/Strategjia_per_te_Drejten_e_Informimit_dhe_Mbrojtjen_e_te_Dhenave_Personale.pdf > accessed 12 May 2021.

Tirana Bank, Policy on Privacy,
<<https://www.tiranabank.al/media/15469460285c3485ecb4bde.pdf?fbclid=IwAR3oi1hwQeAa4cyq333fp6Ucsixfm3oTx0THf4JUq7uI87JDKnkwupCDdA4> > accessed 17 May 2021.

Vodafone Albania, Privacy Policy
<<https://www.vodafone.al/en/informacion-ligjor/informacion-i-pergjithshem-ligjor/rregullore-e-privatesise/>> accessed 17 May 2021.

Case-law

Antovic and Mirkovic v. Montenegro [2018], para 55 <[CASE OF ANTOVIC AND MIRKOVIC v. MONTENEGRO.pdf](#)> accessed 24 May 2021.

Unifying Decision of the Supreme Court Joint Panels No.3/08 July 2013.

Albanian titles

Legislation

Kushtetuta e Republikës së Shqipërisë.

Ligj Nr.7850, datë 29 Korrik 1994 “Për Kodin Civil të Republikës së Shqipërisë”, i ndryshuar.

Ligj Nr. 8116, datë 29 Mars 1996 “Kodi i Procedurës Civile i Republikës së Shqipërisë”, i ndryshuar.

Ligj Nr. 7895, datë 27 Janar 1995 “Kodi Penal i Republikës së Shqipërisë”, i ndryshuar.

Ligj Nr.7905, datë 21 Mars 1995 “Kodi i Procedurës Penale i Republikës së Shqipërisë”, i ndryshuar.

Ligji Nr. 9887, datë 10 Mars 2008 "Për Mbrojtjen e të Dhënave Personale i ndryshuar me Ligjin Nr. 20/2014" Për disa ndryshime dhe shtesa në Ligjin Nr. 9887, datë 10.3.2008 Për Mbrojtjen e të Dhënave Personale".

Marrëveshja Stabilizim-Asocimit ndërmjet Komuniteteve Evropiane dhe Shteteve të tyre Anëtare, në njërën anë, dhe Republikës së Shqipërisë, në anën tjetër [2009] (OJ L107/166).

Rregullorja (BE) 2016/679 e Parlamentit Evropian dhe e Këshillit e 27 Prillit 2016 mbi mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale dhe lëvizjen e lirë të të dhënave të tilla, dhe shfuqizimin e Direktivës 95/46 / EC (Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave) (OJ L119 / 1).

Ligj Nr. 124/2020 "Për disa shtesa dhe ndryshime në ligjin Nr. 10221, datë 4 Shkurt 2010 "Për mbrojtjen nga diskriminimi".

Ligji Nr. 9918, datë 19 Maj 2008 "Për komunikimet elektronike".

Ligj Nr. 10 325, datë 23 Shtator 2010 "Për bazat e të dhënave shtetërore".

Digital Source (Raporte dhe Manuale)

ProCredit Bank, Politikat e Privatësisë (2018)
<https://www.procreditbank.com.al/Uploads/Data/Files/157/PolitikaepriatesisePCBALB_rVfqVARNtU.pdf?fbclid=IwAR20Qbpl_U7ROeSwsgbyHh9psvBpEqcDFZ41XsA7VZ0lRxZZnDMpRHiE0M> aksesuar 17 Maj 2021.

Strategjia për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale 2018-2020
<https://www.idp.al/wp-content/uploads/2018/02/Strategjia_per_te_Drejte_n_e_Informimit_dhe_Mbrojtjen_e_te_Dhenave_Personale.pdf> aksesuar 12 Maj 2021.

Tirana Bank, Politikat e Privatësisë
<<https://www.tiranabank.al/media/15469460285c3485ecb4bde.pdf?fbclid=IwAR3oi1hwQeAa4cyq333fp6Ucsixfm3o7Tx0THf4JUq7uI87JDKnkwupCDdA4>> aksesuar 17 Maj 2021.

Vodafone Albania, Rregullore e Privatësisë
<<https://www.vodafone.al/en/informacion-ligjor/informacion-i-pergjithshem-ligjor/rregullore-e-priatesise/>> aksesuar 17 Maj 2021.

Case-law

Cështja e Antovic dhe Mirkovic v. Montenegro [2018] paragrafi 55.
<[CASE OF ANTOVIC AND MIRKOVIC v. MONTENEGRO.pdf](#)> aksesuar 24 Maj 2021
Vendim Unifikues i Kolegjeve të Bashkuara të Gjykatës së Lartë Nr. 3/ 08 Korrik 2013.

ELSA AZERBAIJAN

Contributors

National Coordinator

Shabnam Guliyeva

National Researchers

Ibrahim Mammadzade

Taleh Abbasli

Kamil Demirli

Sevil Hasanli

Sama Mammadli

Shovkat Rasulova

Sama Jafarli

Mariam Atakishieva

National Linguistic Editor

Amil Jafarguliyev

Tariyel Aliyev

National Technical Editor

Fidan Namazova

National Academic Supervisor

Elvin Balajanov

Turkhan Ismayilzada, LLM

Introduction

With the spread of digital technologies, new ethical questions arise about the implementation of fundamental human rights - the rights to respect for private life (privacy), freedom of speech, the prohibition of discrimination, and the protection of vulnerable groups. There is still no comprehensive explanation of how to fully protect these rights in the digital environment.

Currently, international organizations are actively explaining by publishing recommendations, guidelines and declarations on how traditional norms in the field of human rights should be enforced in the digital world. International organizations are preparing for the adoption of normative legal acts enforceable at the supranational level. First of all, this refers to documents on the protection of privacy in connection with the collection, storage and transfer of personal data.

It is not yet clear to what extent existing legal concepts and institutions in the field of human rights are capable of answering the ethical and legal questions that arise in connection with the development of advanced digital technologies. Therefore, the current state of international human rights law requires continued discussion on how to protect human rights values in a rapidly changing and digitalized world.

Given the threats posed by technological development, it is useful to consider to what extent are the right to respect for private life, freedom of expression, and the prohibition of discrimination respected and how vulnerable groups are protected are respected.

1. Which human rights issues does Advanced Digital Technologies (ADT) pose in your country?

The Republic of Azerbaijan (hereinafter Azerbaijan) is a party to several international agreements on human rights, including the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950),⁷⁶ International Covenant on Civil and Political Rights (1966), and its facultative protocols.⁷⁷ Also, section II, chapter 3 of the Constitution of the Republic of Azerbaijan, provides a wide range of human rights, including the right to privacy, freedom of expression, right to a fair trial, non-discrimination. Article 12 of the Constitution declares that ensuring the rights and liberties of individuals is the highest goal of the state.

However, the rapid development of advanced digital technologies and their impact on human rights might present challenges ensuring these rights. Although no statistical data in Azerbaijan is

⁷⁶ Law of the Republic of Azerbaijan on 'Ratification of the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols 1, 4, 6 and 7.' № 236-IIQ 2001.

⁷⁷ Law of the Republic of Azerbaijan on 'Accession to the Second Facultative Protocol of the International Covenant on Civil and Political Rights aimed at the abolition of the death penalty.' № 582-IQ 1998.

illustrating the specific human rights violations caused by advanced digital technologies, their global impact on human rights should be considered. In this context, Azerbaijan is not an exception, as the development concept of Azerbaijan titled ‘Azerbaijan 2020: Outlook to the Future’⁷⁸ sets the full digitalization of the government services and the ensuring of transition to an information society as priorities.⁷⁹ Digitalization of the justice system also is considered,⁸⁰ but it has its own challenges. To give an example, international experience of AI application in the criminal justice system has been the source of controversy, as the research shows that AI-powered systems, such as COMPAS recidivism scoring software used by US courts, are biased against black individuals and therefore discriminatory.⁸¹ Therefore, probably Azerbaijan, as well, will have to face the challenges of AI application in the justice system.

Furthermore, the overall application of ADTs such as big data and AI requires a proper legislative basis because these technologies and their access to personal data present an imminent challenge to human rights, including the right to privacy, freedom of expression, and non-discrimination.⁸² In addition, these technologies are susceptible to be weaponized and used for political purposes and manipulation of public opinion.⁸³ Furthermore, AI-powered social media algorithms facilitate the spread of disinformation, fake news, and information bubbles. These, in turn, cause deep polarization of the society, thus distorting the individuals’ perception and understanding of the ongoing public discourse.⁸⁴ As it is known from the Cambridge Analytica case, Facebook gave third-party companies access to its 87 million users and their friends’ data, which in turn was used for influencing more than 100 elections in 30 countries, including the 2016 US presidential elections and Brexit.⁸⁵

Azerbaijan is not insured from the above-mentioned threats. Growing distrust of the population to traditional media and the ever-increasing popularity of big social media platforms such as Facebook, YouTube, Instagram, etc. in the country makes them the number one ADT threat to human rights in Azerbaijan. Statistical data for January 2021 shows that 4.30 million of the overall 10 million population is active social media users in the country, a 16% increase compared

⁷⁸ Approved by the Decree of the President of the Republic of Azerbaijan, 29 December 2012.

⁷⁹ ‘Azerbaijan 2020: Look Into The Future’ Concept of Development (2021)

<https://president.az/files/future_en.pdf> accessed 14 March 2021, 10.

⁸⁰ ‘Süni İntellekt və İnsan Hüquqları’ Mövzusunda Beynəlxalq Konfrans Keçirilib’ (Apa.az, 2019)

<https://apa.az/az/sosial_xeberler/suni-intellekt-ve-insan-huquqlari-movzusunda-beynelxalq-konfrans-kecirilib-559148> accessed 14 March 2021.

⁸¹ Julia Angwin and others, ‘Machine Bias’ (*ProPublica*, 2016)

<<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>> accessed 20 February 2021.

⁸² Ingrid Schneider, ‘Democratic Governance of Digital Platforms and Artificial Intelligence?’ (2020) 12(1) *JeDEM - eJournal of eDemocracy and Open Government* 1, 4.

⁸³ *ibid.*

⁸⁴ Access Now, ‘human rights in the age of artificial intelligence’ (accessnow.org 2018)

<<https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>> accessed 14 March 2021

⁸⁵ Schneider (n 82) 4.

to January 2020.⁸⁶ The Second Karabakh War⁸⁷ between Azerbaijan and Armenia from September 27 to November 10, 2020 is of great importance, highlighting the influence and momentum these platforms have in the country's socio-political sphere. During the war, almost all social media and internet platforms became the field of information warfare between the two countries as both sides tried to turn the international public opinion in their favour. The spike in the creation of Twitter accounts during the war was noted by the International Cyber Policy Centre (ICPC), and these accounts were using the hashtags linked to the conflict.⁸⁸

Although the country has data protection laws and international human rights agreements demanding the data protection mechanisms in place, a proper data protection regime is far from GDPR standards. Furthermore, existing laws governing the different aspects of the management of personal data and its protection are fragmented. The Law on personal data⁸⁹ is composed of 19 articles and has serious gaps. For example, the Law does not establish independent supervisory authority to monitor the application of this Law. Instead, the decision of the cabinet of ministers attributes this authority to six different governmental bodies, namely the Ministry of Internal Affairs, Ministry of Justice, State Security Service, Foreign Intelligence Service, Special State Protection Service and Chamber of Control over Financial Markets.⁹⁰ In addition, the Law does not contain any specific sanctions for those who fail to comply with the requirements of personal data processing.

Besides, some of the laws, such as the Law on "Telecommunication"⁹¹ contain certain provisions which might facilitate privacy intrusions without strict scrutiny of courts. This can be illustrated briefly by Article 39 of the Law on 'Telecommunications' which states that operators and providers shall create conditions for conducting search, reconnaissance, and counterintelligence activities under the Law. Furthermore, they are obliged to keep the methods of these interference activities secret.⁹² Without establishing strict scrutiny over such privacy interference the Law makes it very easy to intrude the right to privacy of individuals.

1.1 What national and international standards of human rights protection are at risk due to the ADT development and implementation?

⁸⁶ Simon Kemp, 'DIGITAL 2021: AZERBAIJAN' (DataReportal – Global Digital Insights, 2021) <<https://datareportal.com/reports/digital-2021-azerbaijan>> accessed 14 March 2021.

⁸⁷ 'The Nagorno-Karabakh Conflict: A Visual Explainer' (Crisis Group, 2021) <<https://www.crisisgroup.org/content/nagorno-karabakh-conflict-visual-explainer>> accessed 29 May 2021.

⁸⁸ Christopher Giles and Upasana Bhat, 'Nagorno-Karabakh: The Armenian-Azeri Information Wars' (BBC News, 2020) <<https://www.bbc.com/news/world-europe-54614392>> accessed 14 March 2021.

⁸⁹ Law of the Republic of Azerbaijan, № 998-IIIQ, Dated on 11.05.2010, 'On Personal Data', <http://www.e-qanun.az/framework/19675> > accessed 14 March 2021.

⁹⁰ Decision of the Cabinet of Ministers No 161, dated 6 September 2011, on Approval of 'Requirements for the Protection of Personal Data', art 1.

⁹¹ Law of the Republic of Azerbaijan No 927-IIQ, dated 14 June 2005, 'On Telecommunication' <<http://www.e-qanun.az/framework/10663>> accessed 14 March 2021.

⁹² *ibid* 26.

Azerbaijan, a member of the United Nations since March 2, 1992 and the Council of Europe since January 25, 2001, is a party to more than 220 international treaties, about half of which are directly or indirectly related to human rights and freedoms.⁹³ Azerbaijan has ratified the International Covenant on Economic, Social and Cultural Rights (1966), the International Covenant on Civil and Political Rights (1966), and the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) (hereinafter ECHR).⁹⁴

The first national Constitution, adopted on November 12 1995, fully and comprehensively embraces the human rights and freedoms enshrined in international human rights treaties. Protection of human rights and freedoms in Azerbaijan has been declared as the highest goal of the state in accordance with Article 12 of the Constitution of the country. Thus, section II of the III Chapter III of the Constitution, titled 'Fundamental human and civil rights and freedoms', enshrines civil, political, economic, social, cultural, procedural, and other rights.

The threats posed by ADTs to human rights might lead to a breach of state obligations to ensure the above-mentioned international and national standards. For example, the failure of a state to protect and maintain its citizens' right to privacy could result in an international lawsuit against that state. In this regard, the European Court of Human Rights (hereinafter - ECtHR) is of great importance, as its jurisdiction covers Azerbaijan as well. ECtHR, when examining the cases related to Article 8-11 of ECHR, applies its famous three-part test to determine the existence of a violation. According to that test, the interference with the rights enshrined in articles 8-11 should be prescribed by law, have a legitimate aim, and be 'necessary in a democratic society'.⁹⁵ These tests are an indication of ECtHR's strict scrutiny over interference with articles 8-11 which include the right to private life, freedom of thought, conscience and religion, freedom of expression, and freedom of assembly. The major problem with the regulatory responses to ADT threats is these regulatory measures have the potential to harm the above-mentioned rights as collateral damage. For example, regulatory responses such as content removing, blocking, or criminal sanctions against fake news and disinformation campaigns might have a chilling effect on free expression.⁹⁶ To prevent such risks, states should tailor their ADT regulations with maximum caution.

1.2. Is there or what is a legal framework that provides for procedure on human rights impact assessments? What are other instruments used for identifying human rights issues posed by ADT?

⁹³ Azərbaycan Respublikasının İnsan Hüquqları Üzrə Müvəkkili (Ombudsman). Azərbaycan Respublikasının İştirakçisi Olduğu Beynəlxalq Konvensiyaların Milli Qanunvericilikdə Təsbiti (Qanun 2003) 4.

⁹⁴ *ibid.*

⁹⁵ Dominika Bychawska-Siniarska, Protecting the Right to Freedom of Expression under the European Convention on Human Rights (Council of Europe 2017) 32.

⁹⁶ Rebecca K Helm and Hitoshi Nasu, 'Regulatory Responses to 'Fake News' and Freedom of Expression: Normative and Empirical Evaluation' (2021) 21 Human Rights Law Review 313.

In Azerbaijan, violation of human rights is mostly identified through inquiry and applications of individuals directed to courts or specifically designated bodies such as the Commissioner for Human Rights of the Republic of Azerbaijan. However, under Article 1.8 of the Constitutional Law⁹⁷ as Commissioner for Human Rights of the Republic of Azerbaijan, the Commissioner may submit proposals to *Milli Majlis* (parliament) for the adoption, repeal, or amendment of laws to ensure the protection of human rights and freedoms. On this basis the Commissioner regularly conducts assessments to identify impediments of the exercise of human rights and fundamental freedoms, as well as gaps or contradictions in national legislation. Commissioner ensures the implementation, monitoring, and coordination of existing strategies, concepts, state programs, national action plans, and programs related to or affecting human rights and freedoms. Commissioner also prepares monthly reports on the state of legislation in the field of human rights as well as various publications such as books, articles, statements on issues of protection of human rights.^{98, 99}

Another governmental body that has the competency to conduct impact assessment particularly in the field of information technologies is the Cyber Security Service (hereafter - CSS) under the Ministry of Communications and High Technologies (hereafter - MCHT).¹⁰⁰ CSS coordinates the activities of information infrastructure entities in the field of cybersecurity, provides information on current and potential cyber threats, educates public, private organizations in the field of cybersecurity, and provides them with methodological assistance. CSS also aims to prevent violations of the Law on Personal Data by legal entities and individuals engaged in the collection, processing, and protection of personal data.¹⁰¹

2. How is personal information protected in your national legislation?

2.1. In Azerbaijan, the protection of personal information is regulated by the Constitution of the Republic of Azerbaijan and several national laws:

2.1.1. The Constitution of the Republic of Azerbaijan.

The Constitution of the Republic of Azerbaijan¹⁰² protects everyone's right to the inviolability of private life by Article 32 which also prescribes that everyone has a right to demand correction or elimination of the information collected in regard to him/her, which does not correspond to the truth or is incomplete or collected through violation of the provisions of law. Except in the cases prescribed by law, it is prohibited to access information resources carried on paper or in

⁹⁷ According to art. 156 of the Constitution states that constitutional laws are an integral part of the Constitution of the Republic of Azerbaijan and for its adoption at least 95 votes are required, whereas for other laws it is 83.

⁹⁸ 'Elmi-Analitikİş' (*ombudsman.az*) <<https://ombudsman.az/az/view/pages/56>> accessed 20 February 2021.

⁹⁹ Ombudsman, *Beynəlxalq Konvensiyaların Milli Qanunvericilikdə Təsbiti* (n 93).

¹⁰⁰ The Service was established by Decree No 708 of the President of the Republic of Azerbaijan, dated 26 September 2012.

¹⁰¹ 'Services - Cyber Security Service' (*cert.az*) <<https://cert.az/en/services>> accessed 14 March 2021.

¹⁰² Constitution of the Republic of Azerbaijan, dated 12 November 1995, <<http://www.e-qanun.az/framework/897>> accessed 28 February 2021.

electronic form in order to obtain information from a third party. Information technologies may not be used for disclosing information about private life, including beliefs, religion and ethnic identity except in the cases when the concerned person has openly expressed his or her consent or when the statistical data of anonymous nature is being processed without discrimination and in other cases prescribed by law. Scope of the personal information, as well as the conditions of their processing, collection, passing, use and protection, is prescribed by law.

2.1.2. The Law of the Republic of Azerbaijan on 'Personal Data'.¹⁰³

The Law of the Republic of Azerbaijan on Personal Data regulates the relations related to collection, processing and protection of personal data, the formation of the personal data section of the national information space, as well as issues related to the cross-border transmission of personal data, defines the rights and responsibilities of state and local self-government bodies, legal entities and individuals.¹⁰⁴ Article 2.1.1 of the Law defines personal data as any information that should directly or indirectly identify the person. According to the Article 9.6 of the Law, collection and processing of personal data may be carried out only if one of the following conditions is fulfilled:

1. if the subject gives his or her consent to the collection and processing of personal data or if this information is openly accessible;
2. when personal data is processed based on legislation defining the purposes and methods of their collection and processing;
3. when personal data is processed for the purposes of scientific and statistical research purposes conditioned with its obligatory anonymization;
4. when the collection and processing of personal data are necessary to protect the life and health of the subject.

It's also important to note that formation of information resources of personal data, creation of their information systems is carried out in accordance with the principles of legality, confidentiality, coordination of voluntariness with compulsion, in compliance with the basic human and civil rights and freedoms enshrined in the Constitution of the Republic of Azerbaijan.¹⁰⁵

2.1.3. The Law of the Republic of Azerbaijan on 'Mass Media'.¹⁰⁶

According to Article 10-1 of the Law, use of secret audio and video recordings, filming and photography or distribution of prepared materials and materials only in the following cases:

¹⁰³ Law of the Republic of Azerbaijan on Personal Data No 998-IIIQ, dated 11 February 2010, <<http://www.e-qanun.az/framework/19675>> accessed 28 February 2021.

¹⁰⁴ *ibid.*

¹⁰⁵ *ibid* art 4.1.

¹⁰⁶ Law of the Republic of Azerbaijan on 'Mass Media' No 769-IQ, dated 7 December 1999, <<http://www.e-qanun.az/framework/30>> accessed 28 February 2021.

1. if there is a written consent to this person and citizen, as well as taking the necessary measures to protect the Constitution of the Republic of Azerbaijan and the freedoms of an outsider;
2. during a demonstration by a court decision.

The use of secret audio-video recordings, cinematographic filming and their distribution in violation of the requirements of this article entails liability in accordance with the legislation of the Republic of Azerbaijan.

2.1.4. The Law of the Republic of Azerbaijan on 'Access to Information'.¹⁰⁷

First of all, it's important to mention that Article 50 of the Constitution of Azerbaijan states that everyone is free to legally seek, receive, impart, produce, and disseminate any information. The main purpose of the Law on Access to Information is to determine the legal basis for ensuring the right to information, established by Article 50 of the Constitution, based on principles of an open society and a democratic state governed by the rule of law and to create conditions for citizens to control the performance of public duties.¹⁰⁸

A slightly different definition of 'personal information' is given here. According to the Article 3.0.2 of the Law, information about personal and family life which covers facts, opinions, information about events, activities, situations that allow direct or indirect identification of the person is described as personal information.

Article 38.2 of the Law prohibits the acquisition of personal information about or related to:

1. information reflecting the political views (except for information on membership), religion and ideology of private legal entities registered within procedures established by legislation; information on ethnic origin or racial belonging;
2. information collected during litigations on crimes or other offences – until the open court or the rendering a judgment on the offence; or in cases required for protection of people's morality, private or family life, or for the sake of under age persons, victims or witnesses; or for execution of the judgment;
3. information on the state of health;
4. information on the person's individual features, abilities and other strains;
5. information on applications for social protection and social services;
6. information on mental and physical disability;
7. information on taxation, except for outstanding tax debts.

Article 38.3 of the Law restricts the acquisition of the following information about family life:

¹⁰⁷ Law of the Republic of Azerbaijan 'On Access to Information' No 1024-IIQ, dated 30 September 2005, <<http://www.e-qanun.az/framework/11142>> accessed 28 February 2021.

¹⁰⁸ *ibid* art 1.

8. information about sexual life;
9. information on registration of civil status acts;
10. information on various aspects of the family life;
11. adoption information.

According to the Article 40 of the Law, restrictions on access to personal data will be valid for up to 75 years from the date of receipt or documentation of this information or for up to 30 years after the death of the person or if the fact of death has not been established, it will be valid for up to 110 years from the date of birth of the person.

2.1.5. The Law of the Republic of Azerbaijan on ‘Telecommunication’.¹⁰⁹

The Law determines the legal, economic, and organizational bases of activity in the field of telecommunication in the Republic of Azerbaijan and regulates purposeful planning and fair use of telecommunication resources.¹¹⁰ Article 38 of the Law states that operators and providers must ensure the confidentiality of information transmitted through their networks. Disclosure of telephone conversations and information transmitted by other means of telecommunications is allowed only in cases provided by law.

According to the Article 39.1 operators and providers will create conditions for conducting the search, reconnaissance and counterintelligence activities under the law, provide telecommunication networks with additional technical means following the conditions established by the relevant executive authority, solve organizational issues and are obliged to keep the methods secret.

2.1.6. The Law of the Republic of Azerbaijan ‘On Biometric information’.¹¹¹

According to the Article 1.1.2 of the Law, biometric data are personal data that characterize the physiological characteristics of an identified or identifiable individual, allow him to be identified unambiguously or in combination with other information (fingerprints and palm prints, facial image, iris and retina of the eye, sound fragment and its acoustic parameters, results of deoxyribonucleic acid (DNA) analysis, body size, description of special features and defects of the body, writing line and signature, etc.), applied relevant standards and reflected in the material carrier.

It’s also important to note that biometric data are collected in the following areas of activity:¹¹²

1. registration of identity documents;
2. migration and border control;
3. ensuring information security and registration of electronic signature tools;

¹⁰⁹ Law of the Republic of Azerbaijan on ‘Telecommunication’ No 927-IIQ, dated 14 June 2005, <<http://www.e-qanun.az/framework/10663>> accessed 28 February 2021.

¹¹⁰ *ibid.*

¹¹¹ Law of the Republic of Azerbaijan ‘On Biometric Information’ No 651-IIIQ, dated 13 June 2008, <<http://www.e-qanun.az/framework/15144>> accessed 10 May 2021.

¹¹² *ibid* art 3.2.

4. intelligence, counter-intelligence and search operations;
5. rescue operations in connection with emergencies;
6. formation of a national DNA database;
7. protection of public order and protection of special regime facilities;
8. criminal prosecution.

The formation of biometric information resources is carried out in accordance with the principles of legality, confidentiality, coordination of voluntariness with compulsion by adhering to human rights and freedoms enshrined in the Constitution of the Republic of Azerbaijan. In the process of collection, processing, use and protection of biometric data, it's not allowed to endanger human life and health, humiliate his honour and dignity.¹¹³

2.1.7. The Law of the Republic of Azerbaijan on 'Information, Informatization and Protection of Information'.¹¹⁴

The Law of the Republic of Azerbaijan on Information, Informatization and Protection of Information states that users have equal rights to access information resources, with the exception of restricted documentary information, and are not obliged to justify the need to use the information to the owner or possessor of the information resources.¹¹⁵

Moreover, under Article 13 of the Law, the owner or possessor, as well as officials shall be liable for the violation of the rules of use of information resources, unreasonable restriction of the rights of users in accordance with the legislation of the Azerbaijan Republic.

This law also determines the restriction of placement of prohibited information to the owner of Internet information resource and its domain name or user of an information-telecommunication network: information which has insulting and slanderous nature, as well as violates inviolability of private life etc.¹¹⁶

2.1.8. The Law of the Republic of Azerbaijan on 'Operational Search Activities'.¹¹⁷

According to Article 13.1 of the Law of the Republic of Azerbaijan on Operational Search Activities when there is a court decision on the prosecution of a criminal, whose offence committed contains elements of a crime (*corpus delicti*), or there is a justified basis for prosecution, collecting personal data by intruding on private life using necessary equipment is allowed despite his disapproval.¹¹⁸ Justified basis should be understood by these elements conforming to this law: preparation for the crime, conspiracy to commit the crime, presence of criminal who has committed the crime or criminal refraining from serving punishment.

¹¹³ *ibid* art 4.

¹¹⁴ Law of the Republic of Azerbaijan on 'Information, Informatization and Protection of Information' No 460-IQ, dated 3 April 1998, <<http://www.e-qanun.az/framework/3525>> accessed 28 February 2021.

¹¹⁵ *ibid* art 11.

¹¹⁶ *ibid* art 13-2.3.

¹¹⁷ Law of the Republic of Azerbaijan on Operational Search Activities No 728-IQ, dated 28 November 1999, <<http://www.e-qanun.az/framework/2938>> accessed 10 May 2021.

¹¹⁸ *ibid*.

2.2. External instruments.

Azerbaijan as a young state, throughout its sovereignty, has adopted many legislative acts that regulate personal information. When adopting certain relevant legislative acts, the state takes into account the practice of foreign countries in a particular area. For example, the adoption of the Law on Personal Data in Azerbaijan took place after the ratification of the Convention for the Protection of Individuals with regard to Automated Processing of Personal Data which was adopted by the Council of Europe in 1981.¹¹⁹ This indicates that after the ratification, the state undertook the obligation to create a legal framework and thereby adopted the above mentioned Law.

It should be noted that the existing legislative acts do not fully correspond to the current technological realities in the field of legal regulation, it would be advisable for the legislator to change the existing legislative acts by transforming the legal norms of foreign countries into their local legislation, for example, the adoption General Data Protection Regulation¹²⁰ (hereinafter - GDPR) in the European Union is considered a big step in the field of personal data protection. Currently, a new bill is being prepared in Azerbaijan - On Personal Data and is expected to be adopted in the near future.¹²¹

3. To what extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?

Legal regulation on the processing of personal data applies to both the public and private sectors. In Azerbaijan, the public and private sector in the field of personal data is regulated by two normative legal acts: the Law on Personal Data (hereinafter – the Law) and the Decision of the Cabinet of Ministers of the Republic of Azerbaijan on approval of ‘Requirements on the protection of personal data’ (hereinafter - the Decision).¹²²

The Decision governs the relations arising in connection with the protection of personal data and relevant information systems in the collection, processing, distribution, and transfer of personal data by the owner or operator of personal data.

¹¹⁹ ‘Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data’, Strasbourg, dated 28 January 1981, <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>> accessed 28 February 2021.

¹²⁰ ‘What is GDPR, the EU’s New Data Protection Law?’ dated 25 May 2018, <<https://gdpr.eu/what-is-gdpr/>> accessed 28 February 2021.

¹²¹ ‘Digital Law: Protection of Personal data’ – the event was held by the Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan, dated 5 March 2021, <<https://mincom.gov.az/en/view/news/847/reqemli-huquq-ferdi-melumatlarin-muhafizesi-tedbiri-kechirilib/>> accessed 28 February 2021.

¹²² Decision of the Cabinet of Ministers of the Republic of Azerbaijan on Approval of ‘Requirements on the Protection of Personal Data’ No 161, dated 6 September 2010, <<http://www.e-qanun.az/framework/20046>> accessed 28 February 2021.

According to Article 2.1.10 of the Law the ‘operator of personal data’, which includes state and municipal bodies, legal entities, and natural persons.

The Decision lists the state bodies that control and monitor the implementation of the Requirements within their competence. It includes the following institutions: The Ministry of Transport, Communications and High Technologies, the Ministry of National Security, the Ministry of Internal Affairs, the Ministry of Justice of, the State Security Service, the Foreign Intelligence Service, and the Special State Security Service.¹²³

Control over the information transferred to the operator of personal data should be carried out both at the level of building information security systems and at the level of building relationships with persons to whom information is provided for processing. It should be taken into account that the requirements of the Law also apply to the representative offices of legal entities of foreign states engaged in the processing of personal data on the territory of the Republic of Azerbaijan.

According to the Law, the obligation of the operator in the course of collection and processing of personal data shall be the provision of lawfulness and safety of collection and processing of personal data. According to Article 10.1 of the Law, moral and material damage caused to the subject of personal data as a result of collection and processing of his or her data, incomplete provision of safety of such data, and the amount of such damage shall be determined by the court and reimbursed by the operator as provided for in the legislation.

Article 11.2 of the Law requires the owner or operator to inform the subject of personal data of the following, in the course of the collection of personal data:

- data identifying the owner or operator;
- purpose of personal data processing and legal substantiation of that purpose;
- level of protection of collected and processed personal data in the information system;
- data on availability of certificate of compliance for information system and on their state expert examination;
- range of provided personal data users, including information systems with which performance of information exchange is foreseen.

If the collection of personal data is provided for in the law, the owner or operator shall be obliged to inform the subject entity of the legal consequences of mandatory submission of personal data.

Some examples.

The privacy policy of eManat, which is the application intended to carry out distant online payments, contains a collection of data.¹²⁴ Followings are included in the collected data: given

¹²³ *ibid.*

¹²⁴ eManat+Privacy Policy, <<https://emanat.az/privacy/aze.pdf>> accessed 2 March 2021.

name, surname, phone number, address, e-mail address, further enables detecting geolocation, and permission on phone's camera, call, calendar, access to biometric information and SMS. Nowadays, every person hesitates whether to insert e. g bank account number and to be liable for potential high risk by virtue of their permission. Apart from this scepticism, all data required by any application or website dealing with payment or services is mandatory, if it is not represented by the subject, normal functioning of operations will become inaccessible. In this case, the customer should comply with the terms and not object to them for the sake of the required service. Consecutively, to provide transparently, adequate legal protection of data included is the obligation of service-related companies.

The next example of the private sector is Hesab.az¹²⁵ - the largest online services platform in Azerbaijan, which integrates government payments, utilities, insurance, parking fees, purchase of compulsory car insurance, tickets and other online payment services. As stated in the privacy policy of the abovementioned company, when using the service of this site, the following information is required, but this information is not exhausted, that is, if necessary, additional information may be required. Such information includes¹²⁶:

- Email address;
- Name and surname;
- Telephone number;
- Address, State, Province, ZIP/Postal code, City.

The use of cookies, transfer of data and disclosure of data are also indicated in the privacy policy. Transfer of data: if you are located outside Azerbaijan and choose to provide information, please note that this company transfers data, including personal data, to Azerbaijan and processes it there.

Hesab.az may disclose the personal data of users if it in good faith believes that such actions are necessary to¹²⁷:

- Comply with legal obligations;
- To protect the rights or property of a company;
- To prevent or investigate possible misconduct in connection with the Service;
- To protect the personal safety of users of the Service or the public;
- For protection from legal liability.

In accordance with the Decree of the President of the Republic of Azerbaijan 'On approval of the Rules for maintaining the state register of personal data information systems'¹²⁸: The State Register of Information Data Systems (hereinafter - the State Register) is a state information

¹²⁵ Hesab.az, <<https://hesab.az/#/>> accessed 27 May 2021.

¹²⁶ Privacy policy of the hesab.az, <<https://hesab.az/#/privacy-policy>> accessed 27 May 2021.

¹²⁷ *ibid.*

¹²⁸ Decree of the President of the Republic of Azerbaijan 'On Approval of the Rules for Maintaining the State Register of Personal Data Information Systems' No 341, dated 4 October 2010, <<http://www.e-qanun.az/framework/20109>> accessed 28 May 2021.

resource that reflects information about information systems. The State Register and its information system are the property of the Republic of Azerbaijan.¹²⁹ The State Register is maintained by the MTCHT of the Republic of Azerbaijan.¹³⁰

In accordance with the provisions of the 'Information systems of personal data that do not require state registration'¹³¹ approved by the Decision of the Cabinet of Ministers of the Republic of Azerbaijan, information systems containing personal data for 1000 or more subjects must be registered, and in accordance with the Law the collection, storage and processing of personal data in unregistered information systems are illegal. In this regard, for state registration and inclusion in the register of state information resources and systems belonging to them, MTCHT first addressed to all government agencies. As a next step, MTCHT addressed banks, insurance companies, internet providers and telecommunications companies operating in the Republic of Azerbaijan, with a request to take appropriate measures to register their information resources and systems in the state register, and also posted relevant announcements in a number of mass media.

The legislator does not establish in what form (written or oral) the personal data operator must provide the data subject with the above information. Consequently, a response to such a request can be issued in any form agreed by the parties. This information must be provided by the personal data operator when the personal data subject contacts him orally or upon receipt of a corresponding written request from the subject of personal data, as well as a request in the form of an electronic correspondence.

A distinction should be made between the public and the private sector for the purposes and mission of the processing of personal data. The difference in the architecture of these spheres exists not only in other countries, but also in Azerbaijan.

As can be seen from the above, self-regulation of the private sector is not observed and the latter in its activity in the field of data protection is based on the legal norms of the relevant acts of the state and in case of non-compliance with the requirements of legislative legal norms, appropriate responsibility is provided.

Unfortunately, the existing Laws does not disclose how and to what extent the public and private sectors interact or should interact; there are no specific criteria for such cooperation between them.

It would be advisable to include such legal provisions in the future in the relevant regulations.

¹²⁹ *ibid* art 3.

¹³⁰ *ibid* art 6.

¹³¹ Decision of the Cabinet of Ministers of the Republic of Azerbaijan 'Information Systems of Personal Data that Do Not Require State Registration' No 237, dated 17 December 2010, <<http://www.e-qanun.az/framework/21060>> accessed 28 May 2021.

4. What is the process of judicial review of cases data protection breaches?

4.1. Is the right to data privacy defined in your legal system? If not, is it a part of another right protected the national law?

Article 32 of the Constitution enshrines the right to inviolability of private life in order to ensure confidentiality and to eliminate unlawfulness. Except in some cases provided for by law, illegal intrusion into private or family life is prohibited. According to Article 2.1.1 of the Law of the Republic of Azerbaijan on Personal Data (hereinafter - Law on Personal Data), private life includes personal data or information about an individual, which enables to determine the identity of this person directly or indirectly.¹³² Article 4.1 of the Law states that the collection, processing, and protection of personal data are based on the principles of legality, confidentiality, a juxtaposition of voluntariness with compulsion. To what extent voluntariness and compulsion can be adjusted? It is a bit of a contradictory issue. For instance, authorised individuals collect personal data on a specific matter. Considering the confidential character of some information about a person, how can this kind of data be collected compulsorily? Based on this principle, voluntariness shall be applied in collecting confidential data. According to Article 32.4 of Constitution if there is a necessity to prevent the commission of crimes, or reveal the truth, confidential information transmitted by telephone conversations, mail, telegraph, and other means of communication may be obtained compulsorily. However, it would be better to classify the principle of a juxtaposition of voluntariness with compulsion as a 'voluntariness' and 'compulsion' respectively.

Taking into account advanced developments in the mass media, it is not uncommon to see malicious information or fake news about individuals. According to Article 32 of the Constitution, every person is entitled to the right to be acquainted with materials collected concerning themselves, to demand correction or elimination of information collected, which does not reflect the truth or is incomplete or collected by illegal methods. Spreading of sensitive information about an individual, which reveals the identity, belief, religion of the person will entail undesirable consequences. For instance: disclosure of gender of the person may cause discrimination, breaching inviolability of honour and dignity alongside with violation of the privacy of private life. This is evident in the case of the incident in May 2019 a person who was an employee of Azerbaijan Airlines (AZAL) shared an ID card belonging to a transgender person in his Facebook profile and turned it into an object of ridicule. The move was condemned on social media, and as a result, AZAL has fired the employee who disclosed the confidential information and apologized for the event. This was an instance of breaching the inviolability of privacy by disclosing the person's identity directly.¹³³

¹³² Law of the Republic of Azerbaijan on Personal Data (n 103).

¹³³ Official statement from AZAL regarding the distribution of the transgender person's document <<https://minorityaze.org/262-azal-aciqlama-verdi>> accessed 14 March 2021.

The establishment of electronic information resources, wide usage of information technologies has made the protection of personal information necessary. Access to information resources in electronic form or on paper to obtain information about third parties is prohibited, except as provided by law under Article 32 of the Constitution.

The right to privacy is protected by the state, and violation of this right creates liability established by law. In Chapter 32 of the Code of Administrative Offenses of the Republic of Azerbaijan¹³⁴ there are administrative sanctions for administrative violations of the rules for the use, dissemination, and protection of information. For instance, for refusing to consider on the merits the requests of citizens, enterprises, departments, organizations, and state authorities of the Republic of Azerbaijan on the disclosure of confidential information, restriction of the right to access public information by the owner of the information or intentional misrepresentation of information to the requester, administrative sanctions are envisaged. This Code provides for a fine of approximately one hundred and forty-four euros to two hundred and forty-four euros for the collection or processing of personal data in an information system that requires state registration but is not registered by the Law on Personal Data.

An example of such breach and judicial review of it is the case from 2020 date in the Sumgayit Court of Appeal of the Republic of Azerbaijan¹³⁵.

The accused person required a thousand three hundred and fifty AZN (six hundred fifty-two euros) from the victim by threatening her to disclose pictures, which referred to private and family life at the time of their actual marital relationship, to seize her property. In order to not be disgraced, the victim complied with the request partially. In June 2018, the victim gave him eight hundred AZN (three hundred eighty-six euros) through her sister, as the victim was outside the Republic of Azerbaijan. Subsequently, the victim applied to law enforcement agencies by filing a complaint petition. The accused person shared eight photos of their private relationship on Instagram by hiding his face. He caused these photos to be seen by other people and violated the inviolability of privacy of the victim. Other laws related to personal data are not considered by the court. As a final decision, the accused person was considered guilty under Article 156.1, which contains breaching inviolability of privacy, and Article 182.1 of Criminal Code¹³⁶, which stipulates requiring property by threatening with the dissemination of derogatory information. Alongside these provisions, the constitutional right to protection of honour and dignity is breached.

¹³⁴ Code of Administrative Offenses of the Republic of Azerbaijan No 96-VQ, dated 29 December 2015, <<http://e-qanun.az/framework/46960>> accessed 14 March 2021.

¹³⁵ Decision of the Sumgayit Court of Appeal of the Republic of Azerbaijan (2020).

¹³⁶ Criminal Code of the Republic of Azerbaijan, № 787-IQ, dated 30 December 1999, <<http://e-qanun.az/framework/46947>> accessed 14 March 2021.

4.2. Can the data subject restrict or object the data processing? What are the circumstances and exceptions to this option?

There are special conditions related to data processing. These conditions are considered exceptional. Article 8 of the Law on Personal Data requires the written consent of the subject of data in the form of an electronic document with an enhanced electronic signature for collecting, using, and spreading personal data. The period of validity, terms of withdrawing and archiving the data shall be shown in the written consent. Pursuant to Article 7 of this Law the subjects of personal data can restrict or object to data processing at any time, withdraw the written consent which they represented, and apply to the relevant executive body or court when data is obtained illegally, except in cases such obtainment is mandatory. Those cases are related to prosecution and investigation issues. The objection of a subject should be represented in written form to the owner or the operator of the data. It is not required to justify the objection. This data shall be excluded from the information system. According to Article 9 of the Law, when there is a high probability of risk of health and life security of the subject of personal data collecting personal data is allowed.

4.3. Khadija Ismayilova v. Azerbaijan case¹³⁷

Khadija Ismayilova was pursued due to her investigative report against the government. In order to keep her under control, there was an agreement between the government and State-owned Baktelecom to install a second telephone line to Ms Ismayilova's house. Many cameras were placed in her bedroom. The sensitive materials obtained by utilising this unlawful equipment, which referred to her privacy, were posted on the Internet. Newspapers published it under the name of immoral behaviour, ineffective report. After Ms Ismayilova found many hidden cameras in her bedroom, prosecution authorities launched an investigation. However, the activities of prosecution authorities were ineffective. Subsequently, Ms Ismayilova made a civil claim on disclosing her privacy, which also included her address, full names and occupations of her friends, colleagues, family members, and the identity of her boyfriend.

Ismayilova complained that the domestic courts had breached her right to a fair hearing, which is stipulated in Article 125, 127 of the Constitution. Every person has a right to demand compensation for the damage caused to them as a result of unlawful actions of government bodies or officials under Article 68 of the Constitution. Furthermore, the Law of the Republic of Azerbaijan on Compensation for damage caused to natural persons as a result of illegal actions of investigation, prosecutor's office and judicial bodies is intended to eliminate such unlawful actions. It is inadmissible to suppress the freedom of expression of a person stated in Article 47 of the Constitution, thus the victim was free to make any investigative report. Also, pursuant to Article 163 of the Criminal Code interference in the legitimate activities of journalists is

¹³⁷ *Khadija Ismayilova v Azerbaijan* App no 65286/13 (ECHR, 10 January 2019).

punishable. Dissemination of film of private life is criminalised according to Article 156 of Criminal Code - breaching inviolability of privacy. To pursue, record video or photo, the voice of an individual without their acknowledgement shall create criminal responsibility under Article 155 of Criminal Code.

The final decision of the European Court of Human Rights, fifteen thousand euros for non-pecuniary damage, a thousand seven hundred and fifty euros for pecuniary damage shall be paid by the government.

4.4. In case of data protection breaches, what is the process to notify the data subject? Are there any exceptional grounds not to notify the data subject? If such grounds exist, what would be the ideal or optimal balance for necessity and proportionality?

The Decision of the Cabinet of Ministers of the Republic of Azerbaijan on 'Requirements for the protection of data privacy'¹³⁸ specifies disclosure of illegal intrusion and transfer through forgery, a threat to personal data on time. In addition to this, adequate protection involves notifying the subjects about possible threats or current violations. Pursuant to the Law on Information, informatisation, protection of information¹³⁹ the relevant executive authority shall notify the hosting provider, the owner of a domain name, and Internet information resource about the dissemination of prohibited information. Conforming to Law on Personal Data the owner's responsibilities during the collection and processing of personal data are to ensure the legality and security of the collection and processing of personal data. This Law does not provide for notifying the owner of information about the violation of personal data. However, in order to ensure the right of the owner of the information to go to the court, the operator must notify the subject of the violation of personal data, as well as ensure the legality and security of the collection and processing of personal data. However, MCHT of the Republic of Azerbaijan alerts the people about threats publicly. For instance, cybercriminals try to trap people by creating fake websites under the name of Azerpocht LLC (National postal operator) and obtain data about bank accounts.¹⁴⁰ A special website is provided for the citizens of the Republic of Azerbaijan to report cybersecurity incident and infringement on personal data.¹⁴¹ As a result, the measures are taken to eliminate the negative situation related to the restoration of violated rights in accordance

¹³⁸ Decision of the Cabinet of Ministers of the Republic of Azerbaijan on approval of 'Requirements on the protection of personal data' (n 122).

¹³⁹ Law of the Republic of Azerbaijan on 'Information, Informatization and Protection of Information' (n 114).

¹⁴⁰ Cyber fraudsters try to lure people into trap by creating fake websites on behalf of 'Azerpost LLC', dated 14 December 2020,

<<https://mincom.gov.az/en/view/news/1085/kiberdeleduzlar-azerpocht-mm-nin-adina-saxta-saytlar-yaradaraq-in-sanlari-telev-salmaga-chalishir/>> accessed 14 March 2021.

¹⁴¹ Electron Security Government of the Ministry of Transport, Communications and High Technologies <<https://cert.az/>> accessed 14 March 2021.

with the Decree of the President of the Republic of Azerbaijan ‘On deepening reforms in the judicial system’ serve to accelerate the process of forming justice.¹⁴²

5. Does the review constitute effective protection of data privacy?

There are cases of unwarranted intrusion into private life in the country through the media and social media. The facts obtained by the legislation and the observation method are analyzed in detail. Legislation prohibits any intrusion into private life, surveillance of correspondence, and illegal collection and dissemination of information, but the State Security Service and the Ministry of the Interior have uncovered reports of wiretapping and Internet interference by public activists, foreigners, and human rights defenders. Frequent complaints about postal services were verbally investigated and a report was posted on the website of the US Embassy in Azerbaijan¹⁴³. To prevent this, Azerbaijan has ratified¹⁴⁴ the Convention on the Protection of Persons in connection with the Automated Processing of Personal Data, signed by the states of the Council of Europe¹⁴⁵. The purpose of the Convention is to ensure that the fundamental rights and freedoms of individuals, regardless of nationality or place of residence, are respected in the territory of each Party, including the right to privacy in connection with the automated processing of personal data. The Convention provides for the right to the protection of personal data under the name of privacy. By becoming a party to this convention, Azerbaijan has undertaken to maintain and use the information of individuals for the purposes of justice and lawful purposes. Azerbaijan undertakes to establish appropriate sanctions and remedies in case of violation of the provisions of the domestic law on the protection of information established by the Convention. The Ministry of Justice of the Republic of Azerbaijan is the authorized executive body to provide information on legislation and administrative practice in the field of protection of personal data in cooperation with other partner countries¹⁴⁶. The provisions of the legislation of the Republic of Azerbaijan regulating the inviolability of privacy and the use of personal data are contained in the European Convention on Fundamental Human Rights and Freedoms¹⁴⁷, the Covenant on Civil and Political Rights,¹⁴⁸ the Convention on the Protection of Persons with Automated Processing of Personal Data¹⁴⁹ and others. A review of international documents

¹⁴² Decree of the President of the Republic of Azerbaijan on Deepening Reforms in the Judicial System, dated 3 April 2019 <<https://president.az/articles/32587>> accessed 14 March 2021.

¹⁴³ Report on Human Rights In Azerbaijan in 2017, <https://az.usembassy.gov/wp-content/uploads/sites/284/Azerbaijan_HRR-2017_Aze.pdf> accessed 14 March 2021.

¹⁴⁴ Law of The Republic of Azerbaijan on ‘Approval of The Convention for the Protection of Individuals with regard to Automatic Processing Of Personal Data’, № 879-IIIQ, dated 30 September 2009, <<http://e-qanun.az/framework/18625>> accessed 14 March 2021.

¹⁴⁵ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (n 119).

¹⁴⁶ Ministry of Justice of the Republic of Azerbaijan <justice.gov.az> accessed 14 March 2021.

¹⁴⁷ European Convention on Human Rights, signed 4 November 1950

<https://www.echr.coe.int/Documents/Convention_ENG.pdf> accessed 14 March 2021.

¹⁴⁸ International Covenant on Economic, Social and Cultural Rights, adopted 16 December 1966, 993 UNTS 3 <<https://www.ohchr.org/en/professionalinterest/pages/ccpr.asp>>.

¹⁴⁹ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (n 119).

reveals that local legislation is inadequate and there are some inconsistencies with the listed international regulations. Legislation that facilitates intrusion into private life has been incorporated into local law, in defiance of obligations under international conventions. The norm that allows individuals to listen to spatial information and conversations is set out in Article 39¹⁵⁰ of the Law on Telecommunications. It was also found that victims lost their chances of appealing to local and European Court of Human Rights law enforcement agencies when they were unaware of violations such as the transmission of location information and wiretapping.

Which bodies conduct such a review?

In Azerbaijan the Ministry of Defense of the Republic of Azerbaijan, the Prosecutor General's Office of the Republic of Azerbaijan, the Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan conduct some review.

The Ministry of Defense of the Republic of Azerbaijan¹⁵¹ - is an official state body carrying out military defense and activities. There is a wide range of indirect information storage and control capabilities. Prosecutor General's Office of the Republic of Azerbaijan¹⁵² - is a single centralized body based on the subordination of territorial and specialized prosecutor's offices to the Prosecutor General of the Republic of Azerbaijan, including the judiciary the Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan¹⁵³ - is the central executive body implementing state policy and regulation in the field of communications (telecommunications and post) and high technologies.

The responsibility of the Ministry of Transport, Communications and High Technologies is to control the collection, processing, and protection of personal data in the information systems included in the State Registry to ensure their compliance with the requirements of the Personal Data Law and the declared objectives of the information system and the methods of their processing.

Furthermore, the Ministry must:

- assure the confidentiality of the personal data obtained in the course of its activity; and
- maintain the state registry of information systems of personal data.

¹⁵⁰ Law 'On Telecommunication' (n 91) art 39. Interaction of operators, providers with bodies carrying out search operations, intelligence and counter-intelligence activities 39.1. Operators, providers shall create conditions for conducting search, reconnaissance and counter-intelligence activities in accordance with the law, provide telecommunication networks with additional technical means in accordance with the conditions established by the relevant executive authority, resolve organizational issues and are obliged to keep the methods secret. 39.2. The operator or provider shall be liable for violation of these requirements in accordance with the law.

¹⁵¹ The Ministry of Defence of the Republic of Azerbaijan, <<https://mod.gov.az/en/news-791/>> accessed 14 March 2021.

¹⁵² Prosecutor General's Office of the Republic of Azerbaijan, <<https://genprosecutor.gov.az/project/32/history>> accessed 14 March 2021.

¹⁵³ The Regulation on the Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan, No 1785, dated 12 January 2018, <<https://mincom.gov.az/en/view/pages/2/>> accessed 14 March 2021.

The Ministry also has the following powers:

- making inquiries to the data controllers or data processors in the manner prescribed by law, as well as receiving the necessary information on a free of charge basis from the state authorities, data controllers, or data processors;
- checking the information provided by the data controller during the state registration of information systems of personal data, including the relevance of information systems to the project;
- organising the state expertise of information systems in the prescribed manner;
- requiring state authorities, legal entities and physical persons involved in the collection, processing, and protection of personal data to eliminate violations of the Personal Data Law; and
- taking measures, in accordance with the established procedure, to bring to justice those who violate the requirements of the relevant legislation in the field of collection, processing, and protection of personal data.¹⁵⁴

What is the process of judicial review for cases of data protection breaches?

The law prohibits any intrusion into private life, control of correspondence, and illegal collection and dissemination of information. In some cases, these prohibitions are not followed. Police continued to threaten, harass, and sometimes arrest family members of suspected criminals, members of political opposition, and leaders.^{155, 156} The fact that individuals do not have access to information about themselves and are not familiar with the orders issued about them also indicates that the violations are also in the direction of freedom of access to information. Dissemination of investigative information and details is considered an intrusion on an individual's privacy and freedom of expression and political opinion. The subject has the right to appeal to the relevant executive authority or court in case of violation of his rights as a result of illegal collection and processing of personal data, failure to ensure its protection, as well as non-compliance with the Law on Personal Data, as well as to claim compensation for moral and material damage has¹⁵⁷. However, these cases cannot be considered sufficiently developed in practice.

Does the review provide effective remedies to the data protection breaches? If so, please specify.

¹⁵⁴ Law of the Republic of Azerbaijan on Personal Data (n 103).

¹⁵⁵ U.S. Embassy in Azerbaijan, 'Human Rights Report 2017: Azerbaijan', https://az.usembassy.gov/wp-content/uploads/sites/284/Azerbaijan_HRR-2017_Aze.pdf accessed 14 March 2021.

¹⁵⁶ U.S. Embassy in Azerbaijan, '2018-ci İldə Azərbaycanın İnsan Hüquqlarına Dair Hesabat' <https://az.usembassy.gov/az/2018-ci-ild%C9%99-az%C9%99rbaycanda-insan-huquqlarina-dair-hesabat/> accessed 14 March 2021.

¹⁵⁷ Law of the Republic of Azerbaijan on Personal Data (n 103).

For example, what kind of sanctions are imposed as penalties or what remedies are available?

The Law on Personal Data of the permits the transfer of personal data without consent of the data subject when the transfer of confidential personal data is in connection with the performance by state bodies or local self-government bodies of the tasks assigned to them, provided that the requirements for information systems of personal data established by law are observed. The formation of information resources of personal data and creation of the information systems must be carried out in accordance with the principles of legality, confidentiality, harmonisation of voluntariness with coercion, while observing the fundamental rights and freedoms of persons and citizens, granted by the Constitution of Azerbaijan. The collection, processing, and protection of Personal Data must not create danger to life, health, or cause humiliation of honour and dignity of persons. In order to freely ensure the right to freedom of information enshrined in Article 50 of the Constitution, the legislature adopted the Law of the Republic of Azerbaijan ‘On Access to Information’¹⁵⁸. This Law regulates the obligations of the owner of information to obtain information, protection of information and their liability in case of illegal actions and inactions. The applicant shall have the right to appeal to the court or to the Commissioner for Human Rights (Ombudsman) of the Republic of Azerbaijan against the refusal or improper execution of the request. The owner of the information requesting the information shall explain this right of the requester to him / her and state it in the response (information) submitted¹⁵⁹. The law on personal data¹⁶⁰ requires personal information systems to be registered with the Ministry of Transport, Communications and High Technologies. Collection and processing of personal data in the information system without registration may result in administrative liability under Article 375 of the Code of Administrative Offenses,¹⁶¹ including a fine of AZN 300 (approximately €148) and AZN 500 (approximately €247). Also, according to the Code of Administrative Offenses, an administrative fine of up to AZN 300 (approximately €148) or up to AZN 500 (approximately €247) may be imposed for failure to do so. In addition, the formation of data sources and the creation of personal data information systems is a licensed activity. Failure to obtain a license may result in criminal liability, including a fine of four times the proceeds of such unlicensed activity and / or imprisonment for up to seven years (Article 192 of the Criminal Code).¹⁶² The state has the right to take measures to bring to justice the persons who violated the requirements of the relevant legislation in the field of collection, processing and protection of personal data on issues related to liability and measures of liability for violation of the requirements of this law. Persons found guilty of violating this law shall be prosecuted in accordance with the legislation of the country.

¹⁵⁸ Law of the Republic of Azerbaijan ‘On access to information’ (n 107).

¹⁵⁹ *ibid* art 27-1.

¹⁶⁰ Law of the Republic of Azerbaijan on Personal Data (n 103).

¹⁶¹ Code of Administrative Offenses of the Republic of Azerbaijan (n 134).

¹⁶² Criminal Code of the Republic of Azerbaijan (n 136).

Criminal legal sanctions for violations are provided for in Articles 155¹⁶³ and 156¹⁶⁴ of the Criminal Code of the Republic of Azerbaijan. Violation of the secrecy of correspondence is punishable by a fine or community service, and violation of privacy by a fine, public or correctional work. The subject of the crime of violation of privacy may be a general or a special (official) subject. If the crime is committed by a special subject, the person may be sentenced to deprivation of the right to hold office or imprisonment.

6. What is the process of judicial review of anti-discrimination cases?

Fundamental human rights, including the right not to be discriminated against, must be respected all over the world to ensure prosperity and peace. Discrimination is present where one person is treated less favourably than another is, has been or would be, treated in a comparable situation based on a perceived or real personal characteristic.¹⁶⁵ The legislation of Azerbaijan doesn't exactly define discrimination, however, it deems discrimination as a violation of the right to be treated equally under Article 25 of the Constitution. The Constitution prohibits discrimination based on race, ethnicity, social status, language, origin, convictions, or religion.

Violation of a person's right to equality is criminalized in Article 154 of Criminal Code of the Republic of Azerbaijan by harming the rights and legitimate interests of a person depending on race, nationality, religion, language, sex, origin, property status, position of service, beliefs, membership in political parties, trade unions and other public associations. Also, Article 283 of the Criminal Code defines punishments for the actions aimed at inciting national, racial, social or religious hatred and enmity, degrading national dignity, as well as restricting the rights or determining the preferences of citizens depending on their national, racial or religious affiliation, when committed openly, including through the media.¹⁶⁶ It means that every person who experienced discrimination can apply to law enforcement agencies to file complaints. Then the issue has to be sent to the prosecutor and in the end, this issue can be examined by the court. Upon examination of the court database,¹⁶⁷ it becomes apparent that there is no available court practice of Azerbaijan in this sphere. Its main reason can be that the police and prosecutor's office don't take this problem seriously and then they don't pay enough attention to it. Therefore, citizens' trust in state agencies is broken.

¹⁶³ *ibid.*

¹⁶⁴ *ibid.*

¹⁶⁵ Justyna Maliszewska-Nienartowicz, 'Direct and Indirect Discrimination in European Union Law – How to Draw a Dividing Line?' (International Journal of Social Sciences, III(1), 2014) 41
<https://www.iises.net/download/Soubory/soubory-puvodni/pp041-055_ijoss_2014v3n1.pdf> accessed 14 March 2020.

¹⁶⁶ Criminal Code of the Republic of Azerbaijan (n 136).

¹⁶⁷ Electron Court System of the Republic of Azerbaijan, <<https://e-mehkeme.gov.az/Public/Cases>> accessed 14 March 2021.

Which bodies conduct such a review? What are the elements that are taken into consideration when such a review is conducted? Does the review constitute effective protection against discrimination?

There are committees and executive bodies like the State Committee on Family, Women, and Children, State Committee for Work with Religious Organizations, The Ministry of Labour and Social Protection which should be engaged in raising people's awareness about discrimination in Azerbaijan. They have their own hotlines and online appeals that people who have encountered discrimination on a certain ground can get help from.

One of the functions of the State Committee for Family, Women and Children is to work systematically with men and women to implement gender principles,¹⁶⁸ and one of the tasks of the State Committee for Work with Religious Organizations is to promote mutual understanding and tolerance between religious organizations of different faiths, to help, strengthen, prevent conflicts and discrimination on religious grounds, and other negative manifestations.¹⁶⁹ The annual reports for 2015-2019 are posted on the website of the State Committee for Family, Women and Children show the activities of the Committee during the year.¹⁷⁰ It is seen from the reports of the Committee that they have conducted works that mostly related to increasing awareness of women and men about gender equality by arranging different trainings and events. The promotion of women to entrepreneurship and the work done by the Committee in this regard have been aimed at creating equal opportunities for women and men in this sphere.¹⁷¹

Also, the Human Rights Commissioner has operated in Azerbaijan since 5 March 2002.¹⁷² One of the activities of the Commissioner Institute is the protection of certain groups of people. These groups include refugees, internally displaced persons, migrants, women, the elderly, children, prisoners, persons with disabilities, and others.¹⁷³ People can submit their complaints to the Commissioner by various means like mail and e-mail, an online application on the official website, a reception room in the office and regional centers, hotline, etc.¹⁷⁴

¹⁶⁸ Charter on the State Committee for Family, Women and Children of the Republic of Azerbaijan, No 444, dated 9 August 2006, <<http://scfwca.gov.az/en/page/komitenin-esasnamesi>> accessed 14 March 2021.

¹⁶⁹ Charter on the State Committee for work with Religious Organizations of the Republic of Azerbaijan, No 544, dated 20 July 2001, <<http://www.e-qanun.az/framework/4392>> accessed 14 March 2021.

¹⁷⁰ For the reports of the State Committee for Family, Women and Children regarding the promotion of gender equality, <<http://www.scfwca.gov.az/page/illik-hesabatlar>> accessed 14 March 2021.

¹⁷¹ 2018 Report of the State Committee for Family, Women and Children, 'During 2011-2018, the number of women and youth participating in trainings and events was 5,500. In the past period, 102 women started entrepreneurial activities, and about 50 women were provided with additional jobs', <<http://www.scfwca.gov.az/page/illik-hesabatlar>> accessed 14 March 2021.

¹⁷² Commissioner for Human Rights of the Republic of Azerbaijan Ombudsman, <<https://ombudsman.az/az/view/pages/172>> accessed 14 March 2021.

¹⁷³ For the activities of the Commissioner regarding the protection of rights of such groups of people, <<https://ombudsman.az/az/view/allnews/19>> accessed 14 March 2021.

¹⁷⁴ Commissioner for Human Rights of the Republic of Azerbaijan Ombudsman, <<https://ombudsman.az/az/view/pages/44>> accessed 14 March 2021.

We can see from the activities of the executive bodies and Commissioner, more awareness-raising measures have been implemented against discrimination and the protection of human rights. This need stems from the lack of knowledge of the population about the country's legislation to protect themselves and refer to law enforcement agencies for these issues. As a result, there are obstacles to the widespread use of such rights. Additionally, measures related to the protection of people who belong to certain groups have been identified, addressed, and added to the annual reports.¹⁷⁵ However, there are no official statistics on the number of discriminatory civil or criminal cases heard by the courts. This is the demonstration of the low effect of procedures against discrimination. Because there is not strong knowledge and interest of people to take measures against discrimination, as well, law enforcement agencies don't pay the required attention to this issue. So laws remain on paper and do not work very well in practice.

Recommendations for improving effectiveness in preventing discrimination are set out in the Guide of European Legislation on the Prohibition of Discrimination in Azerbaijan. There is a need to improve and unify the norms related to discrimination which exist in various legislative acts, organization of trainings for relevant civil servants on mastering national and international legislation and elimination of discrimination regardless of when it occurs, awareness-raising among the population about the discriminatory nature of some cultural and socially accepted attitudes.¹⁷⁶

What is a considered role of the technical aspects that result in discrimination (such as algorithmic bias)? How are these problems tackled?

Automatic decision-making gains some advantages over human decision-making through increased speed and volume. Artificial Intelligence (hereinafter - AI) can learn from its experiences and make autonomous decisions.¹⁷⁷ No matter how much innovation of artificial intelligence can replace human labour, it is inevitable that this innovation may create several problems and one of them is discrimination against certain groups. Algorithms can cause discriminatory decision-making and it can be difficult to detect it. It can be noticed from the outcome which can be different from others for a certain group. An example can be related to the examination of CV is conducted by certain algorithms or AI in different workplaces and first cuts are implemented via them. But there is no guarantee such systems don't give a biased decision.¹⁷⁸ Therefore, particular groups may not be invited to job interviews as a result of the

¹⁷⁵ *ibid.*

¹⁷⁶ 'Updated Version of the European Legislation on the Prohibition of Discrimination, which Includes a Guide to the Legislative Framework and Guidance Mechanisms of the Republic of Azerbaijan in the Fight against Discrimination' (2013) 118, <http://iom.az/publications/ECHR_AD_Manual_2013_AZ.pdf> accessed 14 March 2021.

¹⁷⁷ Jack Copeland, 'Artificial Intelligence' <<https://www.britannica.com/technology/artificial-intelligence>> accessed 14 March 2021.

¹⁷⁸ James Manyika, Jake Silberg and Brittany Presten, 'What Do We Do About the Biases in AI?' (2019) <<https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai>> accessed 12 May 2021: 'Back in 1988, the UK Commission for Racial Equality found a British medical school guilty of discrimination. The computer program it

biased decision of AI. Also choice of data can cause discrimination. If the data used for building an algorithm are biased against a group, the algorithm will replicate the human bias in selecting them and learn to discriminate against this group.¹⁷⁹ Also, incomplete or incorrect data can cause such discrimination.¹⁸⁰ For example, if the algorithm is created using information that is characteristic of a certain group, then an algorithm will not consider other groups at the time of decision-making.

Finding discrimination in the algorithm and its reasons is not an easy task. Because huge amounts of data can be used to predict certain outcomes. Hence, there are several ways to tackle these problems like using auditing, extracting data and checking results, etc. The easiest way to detect discrimination can be to examine all data and code that have been used for the building of an algorithm.¹⁸¹ However, some results might appear discriminatory but a closer look shows that they are not.¹⁸² Since the results might demonstrate there is discrimination but as the result of the examination, it can be proved that there are reasonable differences that don't cause discrimination.

The Republic of Azerbaijan ranks 65th in the global index of artificial intelligence (2020).¹⁸³ Therefore there is no expanded use of AI or such autonomous decision-making algorithms in Azerbaijan. The main reason for this is the lack or poor teaching of robotics and coding in schools, as well as the lack of interest in higher education institutions.¹⁸⁴ But it doesn't mean that AI will not expand in our country and we will not encounter discrimination cases as the result of its decisions. Therefore, to develop this area and adapt to the requirements of a modern period, several measures are planned. The Institute of Information Technology of the Azerbaijan National Academy of Sciences will research the impact of artificial intelligence technologies on various sectors of society. Also, this year research on the formation and development of the intellectual e-government is planned.¹⁸⁵

was using to determine which applicants would be invited for interviews was determined to be biased against women and those with non-European names.'

¹⁷⁹ European Union Agency for Fundamental Rights, 'Big Data: Discrimination in Data-Supported Decision Making' (2018) 4, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-fundamental-rights-report-2018_en.pdf> accessed 1 March 2021.

¹⁸⁰ *ibid.*

¹⁸¹ *ibid.*, 6.

¹⁸² Toon Calders and Indre Zliobaite, 'Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures' (2013) 43-57.

¹⁸³ Oxford Insights 'AI readiness Index 2020' <<https://www.oxfordinsights.com/government-ai-readiness-index-2020>> accessed 14 March 2021.

¹⁸⁴ Newspaper Kaspi, 'Azərbaycanda süni intellekti necə inkişaf etdirmək olar?' (2020) <<http://kaspi.az/az/azerbaycanda-suni-intellekti-nECE-inkisaf-erdirmek-olar>> accessed 14 March 2021.

¹⁸⁵ 'Azərbaycanda süni intellektin müxtəlif sahələrə təsiri araşdırılacaq' (2021), <<https://apa.az/az/xeber/infrastruktur/Azərbaycanda-suni-intellektin-muxtlif-sahlr-tsiri-arasdirilacaq-628421>> accessed 14 March 2021.

Also, President Ilham Aliyev has signed a decree on the establishment of a public legal entity 'Center for Analysis and Coordination of the Fourth Industrial Revolution' under the Ministry of Economy of the Republic of Azerbaijan.¹⁸⁶ The Center cooperates and coordinates with international organizations operating in the field of the Fourth Industrial Revolution, as well as analyzes and coordinates challenges, initiatives, strategies, and projects in the digital economy. The main purpose of this Center is to ensure the rapid adoption of new technologies in our country, to take measures for their development, and, most importantly, to ensure that these technologies serve the public interest.

7. Does Azerbaijan have any specific regulations on advanced digital technologies, such as big data, Artificial Intelligence, Internet of Things?

In Azerbaijan the main law in that field is the Law on Personal Data. In our country there is no legislation applying to Big Data or Artificial Intelligence. But for protection of personal and confidential data, there are some normative legal acts in Azerbaijan and today there are some initiatives to realize some changes to those laws and make it relevant to the GDPR. These actions give us hope that maybe in the future, there probably can be specific regulation in this field.

Numerous international conventions and agreements have been ratified by Azerbaijan and this creates some obligations in the field of protection of confidential and personal information. This international normative basis sets up conditions to develop national legislation in that field.

'Convention on the Protection of Persons Related to the Automated Processing of Personal Data' which was signed by European Council states was ratified by Azerbaijan. The aim of the Convention is to provide inviolability of personal life. Azerbaijan ratified that Convention and takes a duty to get personal information in a fair way, to keep and use for legal aims. Azerbaijan takes an obligation to define sanction and legal protection means if any violation in interior state law provisions about protecting the information which is defined by that Convention.¹⁸⁷

The Ministry of Transport of Communications and High Technologies of Azerbaijan has formed a working group, whose mandate is to ensure compliance of local legal regulation with new data protection law of the European Union- the General Data Protection Regulation. For the realization of that process, firstly, it is necessary to study how the GDPR can influence citizens of non-EU countries and in which form it can be applied in general. GDPR was adopted in 2018 and the new act gives people more rights regarding the management of their personal data.

¹⁸⁶ Decree of the President of the Republic of Azerbaijan 'On the Establishment of a Public Legal Entity 'Center for Analysis and Coordination of the Fourth Industrial Revolution' Under the Ministry of Economy of the Republic of Azerbaijan' No 1245, dated 6 January 2021, <<http://e-qanun.az/framework/46604>> accessed 27 May 2021.

¹⁸⁷ Demokratik Təşəbbüslər İnstitutu, 'Şəxsi Həyatın Toxunulmazlığı Və Fərdi Məlumatların İstifadəsinə Dair Araşdırma Sənədi' (2019) 14, <https://idi-aze.org/file/pic/xeber/2019-08/1565903673_hesabat.pdf?1565903644> accessed 5 March 2021.

Finally, it can be said there are some initiatives to make the national legislation relevant to the GDPR. This gives belief that in the future AI or Big Data can also be applied in Azerbaijan. But for now, there is no Big Data, Artificial Intelligence, Internet of Things and that is why there is no specific regulation in that field in Azerbaijan.

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?

The handing over of personal information to law enforcement, such as passwords, or data in unencrypted formats, continues to be a contentious issue.¹⁸⁸ In the context of compelled decryption, the principal concern is of course interference in the private lives of individuals. If we look at the legislation of our country in this regard, we can say that Azerbaijan's legislation requires encrypted personal messages to be decrypted and accessible for criminal investigations.

The legislature adopted the Law of the Republic of Azerbaijan¹⁸⁹ 'On Personal Data' to regulate issues related to the collection, processing, and protection of personal data. The adoption of the law is based on the protection of human and civil rights, and freedoms, the protection of the right to privacy and family life. Also, the right to privacy is a constitutional right of citizens. The guiding norm in this regard is reflected in Article 32 of the Constitution of the Republic of Azerbaijan¹⁹⁰, entitled 'The right to privacy'. The collection, storage, use, and evasion of information related to an individual's private life depends entirely on his will.

Is it possible to interfere with these rights in criminal investigations?

The Law on the Regulation of the Constitution of Human Rights and Freedoms in the Republic of Azerbaijan¹⁹¹ stipulates that the right to privacy enshrined in Article 32 of the Constitution is only in the interests of state security, which changes the essence of this right may be restricted in the interests of the protection of health and morals, the rights and freedoms of individuals, the continuation of criminal activity, the development of the movement of insurgents, the maintenance of public order and economic well-being. Of course, there are limits to a state's power to interfere with this right of citizens.

Also, the law of the Republic of Azerbaijan on search operations regulates legal relations related to the implementation of search operations, collection of data and decryption of messages. Legislation allows carrying out search operations in connection with the extraction of

¹⁸⁸ Encryption and its role in criminal investigation, <<https://simargl.eu/blog/news-updates/encryption-and-its-role-in-criminal-investigation>> accessed 14 March 2021.

¹⁸⁹ Law of the Republic of Azerbaijan on Personal Data (n 103).

¹⁹⁰ Constitution of the Republic of Azerbaijan (n 102).

¹⁹¹ Constitutional Law of the Azerbaijan Republic 'On the regulation of implementation of human rights and freedoms in the Azerbaijan Republic', No 404-IKQ, <<http://www.e-qanun.az/framework/1881>> accessed 14 March 2021.

information from technical communication channels, and other technical means. inspection of postal items, telegraphs and other information to the executive authorities of the Republic of Azerbaijan and specialized anti-corruption prosecutor's offices, eavesdropping on telephone conversations of departments, enterprises and organizations, individuals and legal entities providing communication services, regardless of the form of ownership.¹⁹² However, legislation prohibits the dissemination of information obtained without the consent of any person on the inviolability of his private life, including the secrets of his private and family life, as well as his honour and dignity.¹⁹³

As well as, in the course of procedural activities, Article 199 of Criminal Procedural Code provides the protection of these rights.¹⁹⁴

Also, of considerable importance, however, are the consequences of the use of such evidence in criminal trials and the impact of this on the fairness of criminal proceedings.¹⁹⁵ Police activity in the investigation, searching, and seizing evidence must comply with the privacy guarantee. If not, there can be no question of a fair trial. Experience has shown that the law is not properly applied and leads to abuse. Sometimes the problems stem from the legislation. For example, the body conducting the criminal procedure established by the Code of Criminal Procedure may apply coercive measures as a seizure of post, telegraph and other items; interception of telephone and other devices etc. if it identifies circumstances that impede the acquisition of evidence.¹⁹⁶ It indicates that these are norms that facilitate interference in comparison with the obligations of international conventions. Therefore, national legislation should be developed.

As we know, the issue of collection and storage of personal data in the European Court of Human Rights is often touched upon. The use and disclosure of information kept in a confidential register relating to an individual's private life fall within the scope of paragraph 1 of Article 8.¹⁹⁷ In the case of Khadija Ismayilova against Azerbaijan, the fact of interference with the privacy and personal information of journalists was established. In 2012, the Prosecutor General's Office decided to make public a report on the status of the ongoing investigation. Dissemination of investigative information, in addition to interfering with a person's private life, is an interference with his or her freedom of expression and political opinion. In this case, ECHR holds that there has been a violation of Article 8 of the Convention in connection with

¹⁹² Law of the Republic of Azerbaijan on Operational Search Activities (n 117).

¹⁹³ *ibid* art 4.

¹⁹⁴ Criminal Procedural Code of the Republic of Azerbaijan, № 907-IQ, dated 14 July 2000, <<http://e-qanun.az/framework/46950>> accessed 14 March 2021.

¹⁹⁵ 'Encryption, the Challenges for Criminal Investigation Authorities and the Role of Human Rights Guarantees', para IV,

<<https://www.contralegem.ch/2019-2-1-encryption-the-challenges-for-criminal-investigation-authorities-and-the-role-of-human-rights-guarantees/#top%3Elast>> accessed 14 March 2021.

¹⁹⁶ Criminal Procedural Code of the Republic of Azerbaijan (n 194), art 177.

¹⁹⁷ European Convention on Human Rights (n 147) art 8,

<https://www.echr.coe.int/documents/convention_eng.pdf> accessed 14 March 2021.

the domestic authorities' failure to comply with their positive obligation to investigate effectively very serious intrusions into the applicant's private life, disclosure of the private information published in the authorities' report on the status of the investigation.¹⁹⁸

As mentioned above, the law prohibits any intrusion into private life, surveillance of correspondence, and illegal collection and dissemination of information. However, it can be claimed that gaps in the legislation governing the acquisition and use of information create conditions for abuse by public authorities. The Law of the Republic of Azerbaijan 'On Telecommunications'¹⁹⁹ was adopted in order to determine the legal, economic and organizational bases of activities in the field of telecommunications and to regulate the purposeful planning and fair use of telecommunication resources. Article 39 of the law stipulates a norm that allows individuals to listen to spatial information and conversations. After the latest amendments to the law, it allows mobile operators to place surveillance equipment on networks and monitor people. In response to a request²⁰⁰ from the Ministry of Transport, Communications and High Technologies private companies make it possible to listen to telephone conversations of individuals and legal entities, extract information from technical communication channels and other technical means. The postal services are dependent on government agencies, and there have been reports of letters being monitored by certain groups to determine whether they are politically motivated.

Rapid technological developments allow personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties. Those developments require the building of a strong and more coherent framework for the protection of personal data. Together with the local regulations of personal data in Azerbaijan international regulations shall also be taken into consideration. The provisions of the legislation of the Republic of Azerbaijan governing the inviolability of privacy and the use of personal data are contained in the European Convention on Fundamental Human Rights and Freedom, the Covenant on Civil and Political Rights²⁰¹, the Convention on the Protection of Persons with Automated Processing of Personal Data etc. A close review of international instruments reveals that local legislation is inadequate and it needs to be improved. In order to increase confidence in the power structures of the state, norms on liability for violation of the secrecy of the investigation should be applied. As well as the legal responsibility of public officials who allow unlawful interference with private life must be actually implemented.

¹⁹⁸ *ibid.*

¹⁹⁹ Law on 'Telecommunication' (n 91).

²⁰⁰ Jamila Ibrahimova, 'How is Personal Information Protected in Azerbaijan?' (7 February 2019) <<https://www.bbc.com/azeri/azerbaijan-46875038>> accessed 14 March 2021.

²⁰¹ The Covenant on Civil and Political Rights, <<https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>> accessed 14 April 2021.

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?

One of the urgent issues related to human rights is to ensure the legal protection of personal data. In this case, it is difficult or impossible for the person to whom the personal information belongs to control it. In addition to the requirements of the legislation against data collectors, processors and users, the determination of the rights of personal data subjects in the protection of personal data, the effectiveness of the guarantees provided to them by law are a decisive factor.²⁰² In parallel to adopting substantive laws, regulations, decisions about the protection of human rights, the scrutiny on the activities of public, private sector or natural, legal persons in order to ensure proper implementation of these legal norms is crucial.

Article 7 of the Law of the Republic of Azerbaijan ‘On personal data’ states the rights of the subject of personal data, *inter alia* to get acquainted with the content of personal information collected about himself in the information system; to demand a ban on the collection and processing of personal data about himself; to receive information on the sources of personal information collected and processed in the information system, to demand proof of the legality of that information; to demand protection of personal information collected and processed in the information system.

According to Article 3 of the Law of the Republic of Azerbaijan ‘On Information, Informatization and Protection of Information’, one of the main directions of state policy in the field of informatization is to create the necessary conditions for the formation and protection of state information resources.²⁰³

The right to confidentiality of information transmitted by means of communication is one of the basic rights of citizens enshrined in the Article 32 Constitution. This right is related to the exchange of information. The exchange of information is one of the essential elements of private life. A person can transmit information (data) to communicate with other persons. To do this, an individual uses the telephone, mail, telegraph, and other means of communication. In this case, the person shall apply to the communication organization to exercise the right to provide (transmit) information. In carrying out its professional activities and duties (for example, when transmitting telegrams), the communication organization gets acquainted with the content of the information transmitted by the citizen through the means of communication. A citizen may demand the confidentiality of this information. As it is related to the professional activity of the communication organization, this secret is considered as a communication secret (professional

²⁰² Günel Vəliyeva, 'Fərdi Məlumat Subyektlərinin Hüquqlarının Təhlili' in 'İnformasiya Təhlükəsizliyinin Aktual Multidisipliner Elmi-Praktik Problemləri' Respublika Konfransı (29 November 2019) p. 156 <https://ict.az/uploads/konfrans/info_sec_2019/RS37_ANALYSIS_OF_THE_RIGHTS_OF_PERSONAL_.pdf> accessed 14 April 2021.

²⁰³ Law of the Republic of Azerbaijan on 'Information, Informatization and Protection of Information' (n 114) art 3.

secret).²⁰⁴ The secrecy of communication (confidentiality of communication), i.e., the confidentiality of letters, telephone conversations, postal items, telegrams, and other information transmitted through electric and postal networks is protected by the laws of the Republic of Azerbaijan.

Considering minors and juveniles as a vulnerable category of people, they need to be guarded in the online environment much more than other persons. So, the Law on Information, informatisation and protection of information specifies a warning to eliminate the information disseminated, which is prohibited under the Law.²⁰⁵ Meanwhile, juveniles tend to dive into advanced technologies, like hacking accounts, obtaining some personal information. Deficiency in the knowledge of juveniles with respect to private life may entail grave consequences like disclosing undesirable data of a hacked person, which may humiliate their dignity. To what extent are minors protected on Internet platforms? Comparing with the Children's Online Privacy Protection Act (COPPA)²⁰⁶ of the USA, which aims to protect the privacy of children under 13, the Law of the Republic of Azerbaijan on Protection of children from harmful information²⁰⁷ does not specify parents' permission to collect data on children and the way that this data may then be held and processed. This Law aims at guarding different age groups of children from malicious information and providing the exercising the right of children to acquire information appropriate to their age.

Regrettably, notifying the subject of personal data about threats or breaching of privacy in the online arena is not mentioned in the duties of operators, although it is unattainable for a subject to determine it. However, MCHT of the Republic of Azerbaijan alerts the people about threats publicly. For instance, cybercriminals try to trap people by creating fake websites under the name of Azerpocht LLC - national postal operator - and obtain data about bank accounts.²⁰⁸ A special website is provided for the citizens of the Republic of Azerbaijan to report cybersecurity incidents and infringement on personal data.²⁰⁹

²⁰⁴ A G Kalina and A I Maslyeva (eds), Civil Law. Textbook. Part 1 (Moscow, 1997) 142.

²⁰⁵ Schneider (n 82); Law of the Republic of Azerbaijan on 'Information, Informatization and Protection of Information' (n 114) art 13-3.

²⁰⁶ Children's Online Privacy Protection Act 1998

<<https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>> accessed 14 March 2021.

²⁰⁷ Law of the Republic of Azerbaijan on Protection of children from harmful information 2018, No 1310-VQ <<http://www.e-qanun.az/framework/40764>> accessed 14 March 2021.

²⁰⁸ 'Kiberdöləduzlar 'Azərpoçt' MMC-nin Adına Saxta Saytlar Yaradaraq İnsanları 'Tələyə Salmağa Çalışır' (Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan, 14 March 2021) <<https://mincom.gov.az/az/view/news/1085/kiberdeleduzlar-azerpocht-mmc-nin-adina-saxta-saytlar-yaradaraq-in-sanlari-teleye-salmaga-chalishir>> accessed 14 March 2021.

²⁰⁹ Electron Security Government of Ministry of Communications and High Technologies <<https://cert.az/>> accessed 14 March 2021.

10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the coming 5 years?

Considering the fact that information technologies diffuse into every aspect of our lives and digitalisation of governance is becoming one of the priorities, it can be presumed that legislation will keep up with this trend.

Furthermore, the digitalisation and development of information technologies have created a new race for dominance among superpowers such as the US and China.²¹⁰ In this new techno-political power struggle data plays a crucial role, because extraction, collection and processing of sheer amount of data is a key to the development of Information technologies, particularly Artificial Intelligence. However, Europe and the rest of the world are lagging behind in this technological race.²¹¹ Therefore, it is of utmost importance to set the proper data protection regime in order not to be a digital colony of technology giants. In that regard, Azerbaijan should follow the footsteps of the European Union and implement the concepts of 'digital sovereignty' which is focusing on 'the key ethical and legal principles, such as human dignity, self-determination, privacy, security, democracy, justice, solidarity and sustainability'.²¹²

As previously mentioned, Azerbaijan attempts to speed up the digitalisation of governance and it requires proper and modern e-governance legislation in which data protection is a key element.²¹³ And based on this fact it could be presumed that there will be a substantial improvement of current legislation in the coming years. In fact, signs of some attempts toward improvement are already felt. For instance, According to the development concept of Azerbaijan titled 'Azerbaijan 2020: Outlook to the Future' full digitalization of the government services and the ensuring of transition to an information society are established as future development priorities.²¹⁴ For this purpose, the development concept acknowledges the necessity of establishing the proper information infrastructure and legal framework.²¹⁵

In addition, the Republic of Azerbaijan is planning to implement the concept of 'Smart City' across the country, particularly, in the newly liberated regions of Karabakh.²¹⁶ Creating smart cities requires proper technical and legal frameworks and it would not be a mistake to assume that, in the coming years the country will try to meet these requirements taking into account the European standards which prioritize human rights.

²¹⁰ Schneider (n 82) 11.

²¹¹ *ibid.*

²¹² *ibid* 12.

²¹³ See first question.

²¹⁴ 'Azerbaijan 2020: Look Into The Future Concept of Development' (2021) <https://president.az/files/future_en.pdf> accessed 13 March 2021.

²¹⁵ *ibid* 20.

²¹⁶ 'Qarabağ 'Smart Region' a Çevriləcək' (*Vergilər Qəzeti*, 2021) <<https://vergiler.az/news/economy/11706.html>> accessed 27 March 2021.

Overall, there is hope to be optimistic, as cooperation between Azerbaijan and the EU is growing and expanding every aspect of the socio-political sphere and this includes information technologies and their regulation. EU4DIGITAL initiative is a perfect example of the approximation in regard to digital transition, as it aims to support the digital reform agenda of the Republic of Azerbaijan.²¹⁷ There is no doubt that the approximation with the EU will incentivise Azerbaijan to bring its legislation on digital rights in line with the EU standards.

Conclusion

In the end, to realize the reasons for any existing situation and solve it, it is necessary taking into account the origin of this issue. Azerbaijan acquired its independence and democratic governance in 1991 and before it was under the pressure of imperialist and authoritarian regimes. It is obvious that in this situation, several human rights have been at risk and a few people have been aware of such rights. If we would compare the human rights issue today and 30 years before, laws have been predominantly progressive in Azerbaijan. Firstly, the Constitution of Azerbaijan provides for fundamental human rights, and they are also binding on other laws that have less force. In addition, according to Article 151 of the Constitution of Azerbaijan, ratified international treaties by Azerbaijan is a party have priority over the laws of Azerbaijan, excluding the Constitution of the Republic of Azerbaijan and acts adopted by referendum. Secondly, Azerbaijan's ratification of the Convention on the Protection of Individuals with regard to Automated Processing of Personal Data²¹⁸ which was adopted by the Council of Europe in 1981, and the adoption in the same year of the Law on the Protection of Personal Data at the legislative level, clearly shows that accession and ratification of international treaties is more relevant to local law in order to develop legal areas that are barely regulated.

Thirdly, if we make a brief overview of the above-mentioned legal norms, which are enshrined in regulatory legal acts and governing human rights and technology, we can conclude that despite the short period of state independence, a sufficient number of legislative acts were adopted in order to regulate the existing problems. Despite this, it should be noted that legislation has a lot to do in adopting new legislative acts or changing existing laws so that they can meet international standards in balancing human rights and new technologies.

So the main issue was the right to privacy and data protection in this research. The abuse of the right to privacy is the most frequently violated human right in Azerbaijan as a lack of proper data protection regime leaves the citizens of the country vulnerable in cyber, facilitating the violations even more.²¹⁹ At present, legal reforms are being carried out in our country to protect personal

²¹⁷ 'Azerbaijan | Eu4digital' (*EU4Digital*, 2021) <<https://eufordigital.eu/countries/azerbaijan/>> accessed 27 February 2021.

²¹⁸ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (n 119).

²¹⁹ Demokratik Təşəbbüslər İnstitutu (n 187) 4.

data, taking into account international experience. It should be noted that the gaps in the legislation governing the acquisition and use of information create favorable conditions for government agencies and legal entities and individuals whose activities are directly related to the use of this information to avoid liability. For this reason, the legislation should be further improved and the recommendations of international organizations' reports on the human rights situation in Azerbaijan should be taken into account. It is also impossible to prevent intrusion into personal information without an information security culture. Along with measures to protect personal data, it is necessary to form and develop a culture of information security in society.

The development of technology and science also raises the matter of data protection. Although there is not large use of advanced digital technologies in Azerbaijan, this is inevitable for the future.

Having made an analysis of the above norms, it can be clearly seen that in the local state in no way there are relevant legal norms that could regulate issues related to artificial intelligence. Azerbaijan, as a young country following the development path of developed countries, it would be expedient in the future to transform into its legislation the norms that have been or will be adopted by these countries.

Table of legislation

Provision in Azerbaijani	Corresponding translation in English
Azərbaycan Respublikasının Konstitusiyasının 32-ci və 50-ci maddəsi	Article 32 and 50 of the Constitution of the Republic of Azerbaijan
‘Azərbaycan Respublikasında insan hüquq və azadlıqlarının həyata keçirilməsinin tənzimlənməsi haqqında’ AR Konstitusiya Qanununun 3.6-cı maddəsi	Article 3.6 of Constitutional Law of the Republic of Azerbaijan ‘On regulation of implementation of human rights and freedoms in the Republic of Azerbaijan’
“Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanununun 2.1.1, 9.6, 4.1-ci maddələri	Article 2.1.1, 9.6, 4.1 of Law of the Republic of Azerbaijan ‘On personal data’
“Kütləvi informasiya vasitələri haqqında” Azərbaycan Respublikasının Qanununun 10-cu maddəsi	Article 10 of Law of the Republic of Azerbaijan ‘On mass media’
“İnformasiya əldə etmək haqqında” Azərbaycan Respublikasının Qanununun 1, 3.0.2, 38.2, 38.3, 40.2-ci maddəsi	Article 1, 3.0.2, 38.2, 38.3, 40.2 of Law of the Republic of Azerbaijan ‘On access to information’
“Telekommunikasiya haqqında” Azərbaycan Respublikasının Qanununun Article 38, 39.1 –ci maddəsi	Article 38, 39.1 of Law of the Republic of Azerbaijan ‘On telecommunication’
“Biometrik informasiya haqqında” Azərbaycan Respublikasının Qanununun 1.1.2, 3.2, 4-cü maddəsi	Article 1.1.2, 3.2, 4 of Law of the Republic of Azerbaijan ‘On biometric information’
“İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanununun 11, 13, 13-2.3-cü maddəsi	Article 11, 13, 13-2.3 of Law of the Republic of Azerbaijan ‘On information, informatization and protection of information’
Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu 11.05.2010	The Law of the Republic of Azerbaijan ‘On the personal data’ 11.05.2010
Fərdi məlumatların mühafizəsinə dair Tələblərin təsdiq edilməsi haqqında Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı 06.09.2010.	The decision of the Cabinet of Ministers of the Republic of Azerbaijan on approval of ‘Requirements on the protection of personal data’ 06.09.2010.
“Dövlət qeydiyyatına alınması tələb olunmayan fərdi məlumatların informasiya sistemləri”nin təsdiq edilməsi haqqında	The Decision of the Cabinet of Ministers of the Republic of Azerbaijan ‘Information systems of personal data that do not require state

Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı, № 237, 17.12.2010	registration', № 237, Dated on 17.12.2010, < http://www.e-qanun.az/framework/21060
Azərbaycan Respublikasının İnzibati Xətlər Məcəlləsi, № 96-VQ, Dated on 29.12.2015	The Code of Administrative Offenses of the Republic of Azerbaijan, № 96-VQ, Dated on 29.12.2015, < http://e-qanun.az/framework/46960 >
Fərdi Məlumatların İnformasiya Sistemlərinin Dövlət Reyestrinin Aparılması Qaydalarının Təsdiq Edilməsi Haqqında Azərbaycan Respublikası Prezidentinin Fərmanı, № 341, 04.10.2010	The Decree of the President of the Republic of Azerbaijan 'On approval of the Rules for maintaining the state register of personal data information systems" № 341, Dated on 04.10.2010, < http://www.e-qanun.az/framework/20109 >
"Əməliyyat-Axtarış Fəaliyyəti" Haqqında Azərbaycan Respublikasının Qanunu 28.11.1999	The Law of the Republic of Azerbaijan on Operational Search Activities, № 728-IQ, Dated on 28.11.1999, < http://www.e-qanun.az/framework/2938 >

Bibliography

English titles

Legislation

Constitution of the Republic of Azerbaijan.

Criminal Code of the Republic of Azerbaijan.

Law of the Republic of Azerbaijan ‘On personal data’.

Law of the Republic of Azerbaijan ‘On operational search activities’.

Decision of the Cabinet of Ministers ‘On requirements for the protection of data privacy’.

Law of the Republic of Azerbaijan ‘On information, informatization and protection of information’.

Turkish Personal Data Protection Law.

Constitution of the Republic of Azerbaijan dated 1999.

Books

Majidli S, International Media Law (2015)

Digital resources

Minority Azerbaijan, ‘Azal Açıqlama Verdi’ <https://minorityaze.org/262-azal-aciqlama-verdi>

GDPR.eu, ‘What is GDPR, the EU’s New Data Protection Law?’ <https://gdpr.eu/what-is-gdpr/>

Ministry of Digital Development and Transport of Azerbaijan, ‘Rəqəmli Hüquq: Fərdi Məlumatların Mühafizəsi’
<https://mincom.gov.az/az/view/news/847/reqemli-huquq-ferdi-melumatlarin-muhafizesi-tedbiri-kechirilib/>

Council of Europe, ‘Recommendation on Protection of Personal Data’
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31>

European Court of Human Rights, ‘Judgment in the Case of S. and Marper v. the United Kingdom’ [https://hudoc.echr.coe.int/eng#{%22itemid%22:\(%22001-78227%22\)}](https://hudoc.echr.coe.int/eng#{%22itemid%22:(%22001-78227%22)})

Deloitte Azerbaijan, 'Data Privacy and GDPR'
<https://www2.deloitte.com/az/en/pages/legal/articles/data-privacy-gdpr.html>

DataGuidance, 'Azerbaijan - Data Protection Overview'
<https://www.dataguidance.com/notes/azerbaijan-data-protection-overview>

European Union Agency for Fundamental Rights, *Big Data: Discrimination in Data-Supported Decision Making* (2018)
https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf

Oxford Insights, 'Government AI Readiness Index 2020'
<https://www.oxfordinsights.com/government-ai-readiness-index-2020>

Heilweil R, 'Artificial Intelligence Will Help Determine If You Get Your Next Job' (Vox, 12 December 2019)
<https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen> accessed 11 February 2021

Maliszewska JN, 'Direct and Indirect Discrimination in European Union Law – How to Draw a Dividing Line?' (2014) 3(1) *International Journal of Social Sciences* 41
https://www.iises.net/download/Soubory/soubory-puvodni/pp041-055_ijoss_2014v3n1.pdf

National Academies of Sciences, Engineering, and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers* (2018) <https://www.nap.edu/read/25010/chapter/2>

Contra Legem, 'Encryption, the Challenges for Criminal Investigation Authorities and the Role of Human Rights Guarantees' (2019)
<https://www.contralegem.ch/2019-2-l-encryption-the-challenges-for-criminal-investigation-authorities-and-the-role-of-human-rights-guarantees/#top>

Simargl EU, 'Encryption and Its Role in Criminal Investigation' (20 March 2020)
<https://simargl.eu/blog/news-updates/encryption-and-its-role-in-criminal-investigation>

Council of Europe, *European Convention on Human Rights*
https://www.echr.coe.int/Documents/Convention_ENG.pdf

Olufohunsi T, 'Data Encryption' (December 2019) 1
https://www.researchgate.net/publication/337889039_DATA_ENCRYPTION_Olufohunsi_T

US Embassy in Azerbaijan, *Report on Human Rights in Azerbaijan in 2017*, 7
https://az.usembassy.gov/wp-content/uploads/sites/284/Azerbaijan_HRR-2017_Aze.pdf

Case-law

Khadija Ismayilova v. Azerbaijan [2019] ECHR

Anonymised decision of Sumgayit Court of Appeal of the Republic of Azerbaijan [2020]

Rotaru v. Romania [2000] ECHR

Amann v. Switzerland [2000] ECHR

Azerbaijani titles

Digital resources

‘Azərbaycanda süni intellekti necə inkişaf etdirmək olar?’ (2020)
<http://kaspi.az/az/azerbaycanda-suni-intellekti-nece-inkisaf-etdirmek-olar>

‘Azərbaycanda süni intellektin müxtəlif sahələrə təsiri araşdırılacaq’ (2021)
<https://apa.az/az/infrastruktur/Azrbaycanda-suni-intellektin-muxtlif-sahlr-tsiri-arasdirilacaq-628421>

Gender (Kişi və Qadınların) Bərabərliyinin Təminatları Haqqında Azərbaycan Respublikasının Qanunu (2006) http://www.e-qanun.az/alpdata/framework/data/12/c_f_12424.htm

Ombudsman.az, ‘Sosial Xidmət Müəssisələrindəki Əlilliyi Olan Şəxslərin və Ahılların Hüquqlarının Müdafiəsi Ombudsmanın Diqqət Mərkəzindədir’
<https://ombudsman.az/az/view/news/1799/sosial-xidmet-muessiselerindeki-elilliyi-olan-shexsl-erin-ve-ahillarin-huquqlarinin-mudafiesi-ombudsmanin-diqqet-merkezindedir>

State Committee for Family, Women and Children Affairs, ‘Komitənin Əsasnaməsi’ (2006)
<http://www.scfwca.gov.az/page/komitenin-esasnamesi>

Criminal Procedure Code of the Republic of Azerbaijan, art 177 (177.3.4, 3.5, 3.6)
<http://www.e-qanun.az/code/14>

Constitution of the Republic of Azerbaijan, art 32 <http://www.e-qanun.az/framework/897>

Investigation Document on Privacy and the Use of Personal Data (2019) 22 [unpublished]

Law of the Republic of Azerbaijan on Personal Data [2010] 998-IIIQ
<http://www.e-qanun.az/framework/19675>

Law of the Republic of Azerbaijan on Search Operations [1999] 728-IQ, art 5(IV)
<http://www.e-qanun.az/framework/2938>

Law of the Republic of Azerbaijan on Access to Information, art 38
http://www.e-qanun.az/alpdata/framework/data/11/c_f_11142.htm

Law of the Republic of Azerbaijan on Telecommunications [2005] 927-IIQ
<http://www.e-qanun.az/framework/10663>

ELSA HUNGARY

Contributors

National Coordinator

Kamilla Bodori

National Academic Coordinator

dr. Zsolt Gáspár

National Researchers

Alexandra Török

Bálint Imre Bodó

Bence Tumó

Dávid Szkladán

Dóra Horváth

Enikő Takács

Kínga Kálmán

Zsófia Márta Tengölics

National Technical Editors

Kamilla Bodori

Zsófia Márta Tengölics

1. Which human rights issues do Advanced Digital Technologies pose in your country?

It has been almost 9 years since the UN Human Rights Council (hereinafter: HRC) pronounced that the same rights that people have offline must also be protected online.²²⁰ This was reaffirmed two years later by the 47 members of HRC with the resolution 26/13. Advanced digital technologies and services, which also contain artificial intelligence (hereinafter: AI) bring an extraordinary promise to the future with themselves. Advanced digital technologies include AI, blockchain and automatization. AI refers to systems that display intelligent behaviour by analysing their environment and acting – with some degree of autonomy – to achieve specific goals.²²¹

Another founding scholar, John McCarthy defines AI as ‘the science and engineering of making intelligent machines’.²²² A recent Stanford University report subscribes AI as ‘a science and a set of computational technologies that are inspired by—but typically operate quite differently from—the ways people use their nervous systems and bodies to sense, learn, reason, and take action’.²²³ These technologies have already caused substantial development, particularly in the form they improve effectiveness, precision, quickness and benefits across a range of digital services. Digital advances can support and accelerate achievement of each of the 17 Sustainable Development Goals – from ending extreme poverty to reducing maternal and infant mortality, promoting sustainable farming and decent work, and achieving universal literacy.²²⁴

However, yet the benefits have been also accompanied by a wide range of risks concerning their potential individual and collective harmful effects. Many commentators claim that advances in networked digital technologies, including those currently referred to as AI technologies, are powering the emergence of a ‘New Industrial Revolution’ that will provoke far-reaching changes across every aspect of social life, of a magnitude and scale that will be as disruptive and unsettling as those wrought by the original Industrial Revolution.²²⁵ One example is the Israeli company called Facepion, which categorizes itself as a ‘facial personality analytics technology company,’ and states it can categorize people into personality types based solely on their faces. The classifiers it uses include ‘white collar offender,’ ‘high IQ,’ ‘paedophile’ and ‘terrorist.’ The

²²⁰ Art 19 of HRC.

²²¹ European Parliamentary Research Service, Definition of the European Commission (Study, 2018) <[https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU\(2020\)641547_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf)> accessed 15 June 2018.

²²² COMEST, Report of COMEST on Robotics Ethics (2017) 17.

²²³ John McCarthy, ‘What Is AI? / Basic Questions’ (Jmc.Stanford.Edu, 2018) <<http://jmc.stanford.edu/artificial-intelligence/what-isai/index.html>> accessed 15 February 2021.

²²⁴ United Nations, ‘The Impact of Digital Technologies’ (UN, n.d.) <<https://www.un.org/en/un75/impact-digital-technologies>> accessed 15 February 2021.

²²⁵ Boyd and Crawford 2013. Skilton and Hovsepian 2017.

company has not released any information about how its technology can correctly label people based only on their faces.²²⁶

The report of the Vienna-based EU Agency for Fundamental Rights (hereinafter: FRA), which is based on interviews with more than a hundred public and private organizations using artificial intelligence, highlights the dangers of its use, especially in the areas of early warning policing, medical diagnoses, social benefits and targeted advertising. The FRA has called on the EU and the Member States to ensure that fundamental rights are respected and that redress is available when using artificial intelligence. The relationship between human rights and AI has reached a milestone these days as the U.S. Patent Office rejected two applications filed on behalf of the AI called Dabus as patent rights can only be obtained by natural persons.

AI systems may systematically threaten several rights. The background of it is that we are increasingly turning to machines (indirectly algorithms) for ‘advice’ and even delegating specific decisions to them. AI poses a myriad of threats to human rights, with a focus on the inviolability of human life. However, in today’s digital environment, we inevitably share a wealth of private information about ourselves. We report on where, with whom and when we are, what we read, where we vacation, what we think about specific events. These are then suitable for setting up a complete profile of our behavior and choice preferences.

1.1. Complete profile of behaviour, choice preferences in the light of art. 8 of ECHR

Data-driven profiling is based on the collection of data from individuals in the entire population to be able to profile individuals and groups within the population to determine their preferences and interests²²⁷ and needs. Using this technology, some countries in the world are developing a new device, digital authoritarianism, in front of the eyes of the world. Public authorities that use these technologies and carry out mass surveillance are good examples of the serious impact these technologies can have on individual rights. In 2013, Edward Snowden's leaks about large-scale Internet and telephone surveillance programs by intelligence services in some states raised serious concerns about the threats to privacy, democratic governance and freedom of expression of surveillance activities.

Technologies that allow mass surveillance and the globalized storage and management of personal data, as well as mass access to data, may be contrary to the very essence of the right to privacy. In addition, they can have a negative impact on political culture, democracy, creativity and innovation. The mere fact that the state can constantly monitor and analyze the behavior and activities of citizens can discourage them from expressing their views on certain issues and

²²⁶ Paul Lewis, ‘I Was Shocked It Was So Easy: Meet the Professor Who Says “Facial Recognition Can Tell If You’re Gay”’ *The Guardian* (7 July 2018).

²²⁷ As the Council of Europe, Parliamentary Assembly’s Committee on Culture, Science, Education and Media has observed at para 18 ‘The primary business model of the internet is built on mass surveillance’: Council of Europe 2017.

can lead to suspicion or caution. In Hungary there aren't any applications or systems established which can be used for example in train stations, at a concert or even in school to be able to monitor the attendants.

1.2. The right to freedom of expression of Art 10 of the ECHR

In the digital age, individuals are no longer confronted with a well-known ambiguous model of regulating expression. There are two central actors in the ambiguous model: the power of the state threatens the individual's right to free speech. Instead, the digital age brought with it a plural model of speech regulation. In the plural model, individuals can be controlled, censored and supervised not only by the state, but also by the owners of various private infrastructures across different jurisdictions and across national borders.

The majority of online platforms impose certain limits (general terms and conditions) on users of their services and, in the event of a breach of these rules, generally restrict the publication of content and, in some cases, users' access to the platform. Decisions made on the basis of a typically difficult-to-transparent system of norms have a serious impact on the enforcement of the constitutional right to freedom of expression, as the platforms themselves determine the limits of freedom of expression and its supervisory procedures - without constitutional guarantees. All this also raises a problem of national sovereignty.

However, difficulties can occur in case of enforcing rights on social media platforms as online platforms rarely respond to formal inquiries, which makes it very difficult to prosecute, for example, privacy violations. Locating U.S.-based companies is cumbersome for domestic authorities, mostly taking longer than the statutory retention period. Improving traceability requires updating data retrieval practices and setting up special contact channels for online services for official inquiries.

Without transparency in the operation of the algorithms (or 'codes' governing the operation of the platform) that play a key role in mass decisions on online platforms, it is not possible to determine the principles and criteria for users to prioritize certain content and delete or push others to the background.

The operation of the platforms puts a strain on the practical implementation of the most important restrictions on freedom of expression. Key bans should also apply to platforms, and platforms should not be neutral actors that could idle hate speech, terrorism, or otherwise harmful content, but should actively take action against this type of user content. The relevant regulation can also be created within the state framework

There is a need for strict and enforceable international digital regulation in social media, which will also allow large internet companies to be held accountable. Not only the European Commission aims to introduce a digital regulation, as the same process is continuing in Hungary.

1.3. Right to privacy and data protection: Article 8 of ECHR

‘Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.’²²⁸

The protection of personal data and respect for privacy are important fundamental rights. The European Parliament has always emphasised the need to strike a balance between enhancing security and human rights, including data protection and privacy. In May 2018, new EU data protection rules came into force, strengthening citizens' rights and simplifying rules for businesses in the digital age.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and Regulation (EC) No 95/46 (General Data Protection Regulation) entered into force in May 2018. The legislation aims to protect all EU citizens from privacy and data breaches in an increasingly data-centric world, while creating a clearer and more consistent framework for businesses. Citizens' rights include a clear and affirmative consent to the data they are to be processed and the right to clear and comprehensible information about them; the right to end the storage of personal data: citizens can request the deletion of their data; the right to transfer data to another service provider (eg switching from one social network to another); and the right to know the fact that personal data have been breached. The new rules apply to all companies operating in the EU, even if these companies are based outside the EU. In addition, corrective measures, such as warnings and orders, can be issued or fines imposed on businesses that break the rules.

Learning from China's example, the legal framework for artificial intelligence needs to be developed in time. AI can serve to maximize human well-being, but it can also lead to a rethink of our fundamental rights. The solution has two key elements. On the one hand, ‘sensitizing’ algorithms. These programs must be designed to carry the value system of humanity, or at least to be able to learn it. The problem is also rooted in the definition of these values, as different cultures and different socio-economic backgrounds want to be present. On the other hand, private sector companies and public actors need to be brought closer together, and the public needs to be involved in the dialogue. Therefore, the European Commission published the white paper in accordance with the legal frameworks of AI in 2020.²²⁹ The Hungarian legislation also

²²⁸ Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 8

<<https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data>> accessed 15 February 2021.

²²⁹ European Commission, White Paper on Artificial Intelligence: A European Approach to Excellence and Trust (2020) <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 15 February 2021.

aims to establish the legal framework for the so-called big tech companies, therefore a white paper is also published.²³⁰

2. How is personal information protected in your national legislation?

2.1. How is personal information defined by your national legislation (or by a legal framework that affects your national legislation, e.g. GDPR)?

According to the European Committee, personal information is data about an identified or identifiable living person. For example name, address, identity card number, location data, IP address, cookie ID, phone ad ID, data stored by a hospital or doctor that allows a person to be uniquely identified.²³¹ Also belongs to this group personal data which has been rendered inoperable, encrypted or pseudonymous and which may be used to re-identify a person and such data which is regulated by the general data protection regulation.²³² In Hungary, General Data Protection provides a kind of guidance. The laws in Hungary have been brought into line with this guideline. We need to highlight, Regulation CXII of 2011 on the right to information self-determination and the regulation of freedom of information (hereinafter: Info TV.) which interpret General Data Protection. I will examine below the relation between Regulation CXII of 2011 on the right to information self-determination and the regulation of freedom of information and General Data Protection. In addition to the CXII of 2011 on the right to informational self-determination and on the freedom of information regulation, several Hungarian laws have been harmonized with the General Data Protection Regulation. The General Data Protection Regulation emphasises that personal data have to be protected in a technology-neutral way. The protection should not depend on what device the data is stored. It can be stored on the IT system, in video surveillance, on paper or any device which can store the information. These implements have to correspond with The General Data Protection Regulation.²³³ It cannot be considered as personal data which have been anonymised and the information or the subject of the data cannot be identified and cannot be resettable.²³⁴ This information was issued on the basis of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: General Data Protection Regulation).

2.2. If your country is a Member State of the European Union, please provide a concise analysis of the extent to which your country's laws regarding protection of personal information are compatible with EU law, particularly the General Data Protection Regulation (GDPR).

²³⁰ Government of Hungary, Fehér Könyv: A Digitális Szabadság Alapjai (2020) <https://digitalisszabadsag.kormany.hu/download/f/31/a2000/Feh%C3%A9r_k%C3%B6nyv_HU_20200702.pdf> accessed 15 February 2021.

²³¹ European Commission, *What Is Personal Data?* (EU, n.d.) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hu> 15 February 2021.

²³² *ibid.*

²³³ *ibid.*

²³⁴ *ibid.*

The best way to demonstrate the protection of personal data and the scope of the General Data Protection Regulation in the country is to present the regulation CXII of 2011 on the right to informational self-determination and on the freedom of information regulation (hereinafter: Infotv.). Section 1 contains the aim of the legislation. The legislation, which is cited states that the main task of the law is to find a balance between privacy of individuals and the interests of data controllers. Furthermore, wishes to regulate access to data of public interest or data on public interest grounds and the transparency of public affairs. Section 2 (1) indention is specified in the scope of the Act. This section held one of the most important stipulations. The base of this regulation is it regulates every personal data, data of public interest and data accessible on public interest.²³⁵ This paragraph clarifies that personal data is not the only one which is covered by this law. Section 2 (2) indention explains the scope of the General Data Protection Regulation extends to Hungary as well. I explain this regulation below. This Act Section 2 (3) indention that "This Act shall apply to the processing of personal data for law enforcement, national security and national defence purposes."²³⁶ This also supports my statement above that not only personal data is regulated by law, but all data is regulated. Such an area is also a case of criminal law. According to Section 2 (4) indention, there are cases when the data is not personal data besides, the General Data Protection Regulation and certain provisions of this Act shall apply.²³⁷ The next indention has highlighted the provisions of the General Data Protection Regulation that apply. Section 2 (6) and (7) paragraphs contain exceptions. Which cases are not covered by this law and another law must be applied.²³⁸ For example, this Act cannot apply 'natural persons processing data exclusively for their own personal purposes'.²³⁹ The personal data in this Act defined as 'means any data relating to the data subject'²⁴⁰ This is not as detailed a definition as the one created by the European Committee in the General Data Protection Regulation, but this law refers back to it in many places, so it did not need to be further elaborated.

2.3. How do external instruments (such as the abovementioned GDPR) influence the data protection in your country (N.B. can be applicable to non-EU countries as well).

As can be seen from the above, the General Data Protection Regulation has a very strong influence in Hungary. Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: General Data Protection Regulation or GDPR) is a document relevant to the protection of natural persons and the protection of personal data. This document covers the territory of the EEA States. It regulates the data of natural persons and the flow of this information in these areas. The decree entered into force on 24 May 2016 and has been applicable in Hungary since 25 May 2018. From the 2016/679 Regulation is Article 2, 3 and 4.

²³⁵ Section 2 (1) Infotv.

²³⁶ Section 2 (2) Infotv.

²³⁷ Section 2 (4) Infotv.

²³⁸ Section 2 (6) and (7) Infotv.

²³⁹ Section 2 (6) Infotv.

²⁴⁰ Section 3 3) point Infotv.

Article 2 is about the scope of the regulation. This paragraph is the material scope of the regulation. The policy covers all personal data that is included in the registration system or is intended to be included later.²⁴¹ The second paragraph contains cases which are not covered by the material scope of the Regulation. For example, ‘in the course of an activity which falls outside the scope of EU law’²⁴². The regulation does not only cover cases closely linked to the European Union, this is the point raised. The data do not need to be linked to EU law. But outside of this section, the General Data Protection Regulation mentions several exceptions. Article 3 is the territorial scope. First paragraph explains that the processing of personal data is regulated not only within the EU, but also outside it if the data controller or a processor is a member of the EU. A regulation may apply to goods, services, and their behaviour within the EU on the basis of their territorial scope. These points represent a much more business-like area that the regulation separates from the personal sector. The definition of personal data in the fourth article has already been mentioned above.

3. To which extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?

Self-regulation means that small interest groups independently decide of their own free will in favour of state regulation for themselves; another set of rules are also adopted. There is no obstacle to certain legal entities as long as their conduct does not violate the legal rules.²⁴³ It is not a typical method in Hungary for data protection. Below, I aim to show how the public sector relates to the private sector which was mentioned above.

The Fundamental Law of Hungary Article VI. (4) paragraph explains how it relates to each other in the private and public sector. The private sector has a right to protect people’s rights meanwhile, the public sector has a right to get to know data that can influence the public interest. To be transparent and to ensure that these rights not be damaged is controlled by an independent authority. Regulations on this authority are adopted by cardinal law.²⁴⁴ Which means that two-third majority of the members of parliament has to elect the rules which are controlling the authority.²⁴⁵ Furthermore ‘... its president is appointed by the head of state upon the motion of the prime minister...’.²⁴⁶ The president is elected for nine-year and can be reappointed for one

²⁴¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data [2016] OJ L119/1, art 2.

²⁴² *ibid.*

²⁴³ Lóránt Sink and Annamária Mayer, ‘Variációk a Szabályozásra’ in *MEK* <<https://mek.oszk.hu/13500/13526/13526.pdf>> accessed 20 February 2021.

²⁴⁴ Nora Chronowski, ‘The New Hungarian Fundamental Law in the Light of the European Union's Normative Values’ <<https://poseidon01.ssrn.com>> accessed 22 February 2021.

²⁴⁵ *ibid.*, 121.

²⁴⁶ *ibid.*

occasion.²⁴⁷ The president of the Hungarian National Authority for Data Protection and Freedom of Information appointed a vice president for an indefinite period.²⁴⁸ The president exercises the employer's rights over public officials and civil servants.²⁴⁹

This authority so-called the Hungarian National Authority for Data Protection and Freedom of Information. The National Hungarian Authority for Data Protection and Freedom of Information main responsibilities are the right to the protection of personal data, the right to freedom of information and the monitoring and facilitation of the free movement of personal data within the European Union.²⁵⁰ Above these are the organisations responsible for those cases which are connected with Schengen Information System (SIS), the Customs Information System (CIS), Europol, Eurodac and the Visa Information System (VIS).²⁵¹ Over and above it is in charge of the representation of Hungary as an authority in common data protection supervisory of the European Union.²⁵² The National Hungarian Authority for Data Protection and Freedom of Information is an autonomous state administration body, which means that the organisation is only accountable for the law and cannot be influenced by anyone.²⁵³

Act CXII of 2011 on the right to informational self-determination and on the freedom of information law's Section 3 5) point define the data of public interest. This paragraph emphasises that every data which is generated after the activity of the state and institutions which are connected with this activity.²⁵⁴ This is important data and requires special attention because the population of Hungary can monitor the activity of the political area and can make decisions. On the other hand, the sixth point defines data accessible on public interest grounds, which means that '...any data, other than data of public interest, the disclosure, availability or accessibility of which is prescribed by an Act for the benefit of the general public'.²⁵⁵ Section 26 (1) paragraph contains more details about how a person or organisation acts if they are in the government area. This part details the government area and data in that field. This data can react back to the government and they can be requested about how they are leading the country. Furthermore, people can decide about future leadership. Section 27 lists the exceptions. The first paragraph states, if data of public interest or data of public interest contain classified data. it cannot make it known.²⁵⁶ Classified data has two kinds. The first group is about information from the national

²⁴⁷ Hungarian National Authority for Data Protection and Freedom of Information, 'About the Authority' <<https://naih.hu/about-the-authority>> accessed 22 February 2021.

²⁴⁸ *ibid.*

²⁴⁹ *ibid.*

²⁵⁰ *ibid.*

²⁵¹ *ibid.*

²⁵² *ibid.*

²⁵³ *ibid.*

²⁵⁴ Section 3 5) point Infotv.

²⁵⁵ Section 3 6) point Infotv.

²⁵⁶ Section 27 Infotv.

public sector.²⁵⁷ The second subsection is about information from the foreign public sector.²⁵⁸ These pieces of information can be issued by the European Union, Member State acting on behalf of the European Union, a foreign party or international organisation, organisations of the European Union, a Member State acting on behalf of the European Union, a third country or party, and an international organisation.²⁵⁹ Moreover, the right to access data of public interest or data accessible on public interest grounds can be denied and be limited in the interests of national defence, national security, the prosecution and prevention of criminal offences etc.²⁶⁰

After we examine the public and private sector, we can see law enforcers and legislators are in a difficult position because they need to be aware of which interests should prevail in the event of a conflict between the private and public sectors.

4. What is the process of judicial review of cases data protection breaches?

4.1. Is the right to data privacy defined in your legal system? If not, is it a part of another right protected by the national law?

Ensuring the right to the protection of personal data limits the processing of individual data independently of the data subject's will and ensures that one has control over such data. In Hungary, the right to the protection of personal data is interpreted as a right of informational self-determination, the content of which is that each person himself provides for the fate, discovery and use of his personal data. Information self-determination was formulated as a principle in No. 15/1991 (IV. 13) Constitutional Court decision: 'the right to the protection of personal data is not interpreted as a traditional right of protection, but also as a disciplined and informational right of self-determination'²⁶¹. The right of communication is intended to protect the private sector: 'The essential conceptual element of the private sector [...] is that, against the will of the data subject, others are not able to enter or enter it.'²⁶²

The October 1989 amendment to Act XX of 1949 already recognises the right to the protection of personal data and the right to know data of general interest, which has been entrenched in the two-thirds regulation of the 1990 Constitution. Constitutional law discusses infringements in connection with freedom of information, given that these two rights together ensure that, in the sense of information, the individual does not become vulnerable to the State.²⁶³ The right to informational self-determination is the content of the individual's right to the protection of

²⁵⁷ Section 3 (1) The Act CLV of 2009 on the Protection of Classified Information.

²⁵⁸ *ibid.*

²⁵⁹ *ibid.*

²⁶⁰ Section 27 (2) Infotv.

²⁶¹ No. 15/1991 (IV. 13) Constitutional Court Decision.

²⁶² No. 36/2005 (X. 5) Constitutional Court Decision.

²⁶³ Bernadette Somody, Máté Dániel Szabó, Beatrix Vissy, and Dalma Dojcsák, *Fundamental Rights Doctrines I* (HVG-ORAC 2018) 102.

personal data provided for in Section 59 of the Constitution, according to which each person has the right to reveal and use his or her personal data.²⁶⁴

In view of the lack of comprehensive regulation on the processing and recording of data, the Parliament, in accordance with its constitutional obligation, adopted the LXIII Act of 1992 on the protection of personal data and the publicity of data of general interest (Avtv). The Avtv. data protection in its wording reads: ‘The purpose of this Law is to ensure that, unless the legislation provided for in this Law makes an exception, everyone has their own personal data and that the data of general interest are known to all.’²⁶⁵

After Avtv the Constitution of Hungary and the CXII Act of 2011 on the right to information self-determination and freedom of information became the most important laws. The Constitution frames the protection of personal data in the following way: ‘Everyone has the right to the protection of their personal data and to the knowledge and dissemination of data of general interest.’²⁶⁶ ‘The right to the protection of personal data and the right to know data of general interest shall be monitored by an independent authority established by a cardinal law.’²⁶⁷ The Civil Code Act V of 2013 (Civil Code) refers to it as a named right of personality, ‘It constitutes a violation of personal rights in particular [...] violation of the right to privacy and the protection of personal data.’²⁶⁸

The 2011 Communication on the right of information self-determination and freedom of information was based on the 2011 Communication on the right of information self-determination and freedom of information. The purpose of the CXII Act of 2010 (Infotv.) is to regulate data protection in accordance with the Constitution: ‘The purpose of this Act Hungary is to define basic rules for the processing of data in the subjects covered by it, in order to ensure that the privacy of natural persons is respected by data controllers and that the transparency of public affairs is achieved by enforcing the right to know and disseminate data in the public interest and in the public interest.’²⁶⁹ Restrictions on the collection, processing and use of personal data and the protection of the persons concerned are of paramount importance in Hungary. So-called special data are more tightly protected than personal data. Such information shall be deemed to relate to racial origin, membership of a national and ethnic minority, political opinion, or party position, religious or other worldview beliefs, membership of a representative organisation. Special data include health status, disease and addiction, sex life data, and criminal personal data. The processing of this data requires either consent or legal authority. The Hungarian legislation is in line with the GDPR, which calls for a categorical prohibition on the

²⁶⁴ No. 15/1991 (IV. 13) Constitutional Court Decision

²⁶⁵ Section 1 of the LXIII Act of 1992 on the protection of personal data and the publicity of data of general interest.

²⁶⁶ Section 3 of the Hungarian Constitution Article VI.

²⁶⁷ Section 4 of Hungarian Constitution Article VI.

²⁶⁸ Section 2:43 e) Civil Code.

²⁶⁹ Section 1 of Infotv.

processing of data relating to ethnicity, race, political, religious or worldview, trade union membership, health or sex life, with the exception of the explicit consent of the data subject or the procedure on his or her own account.²⁷⁰ Based on the abovementioned laws, we can formulate the following eight principles of data protection in the Hungarian legal system:

- principle of limiting data collection
- data quality principle
- purpose-bound principle
- principle of limited use
- principle of data security
- principle of openness
- principle of personal participation
- liability principle.²⁷¹

4.2. Can the data subject restrict or object the data processing? What are the circumstances and exceptions to this option?

Among other things, the Data Protection Commissioner is known in Hungary to be the data processing institution. The National Data Protection and Freedom of Information Authority ('NAIH') has replaced the Commissioner as an autonomous administrative body. The NAIH supervises the legality of the operation of the data controllers and this body can be complained to by those who believe that data about them have been unlawfully collected and stored. The data subject shall have the right, at his request, to restrict or block the processing of data if the following conditions are met:

- the person disputes the accuracy of his/her personal data. In this case, the limitation applies to the period that allows the controller to verify the accuracy of these personal data;
- the processing is unlawful, and the data subject opposes the deletion of personal data and instead requests restrictions on their use;
- the controller no longer needs the personal data for the purposes of processing, but the person requires them for the purpose of asserting, enforcing, or defending legal claims;
- the data subject objected to the processing. In this case, the limitation applies to the period until it is established whether the legitimate reasons of the controller take precedence over your legitimate reasons.²⁷²

²⁷⁰ Hungarian Civil Liberties Union (TASZ), 'Mit Jelent az Adatvédelem?'

<<https://tasz.hu/mit-jelent-az-adatvedelem>> accessed 22 February 2021.

²⁷¹ GDPR Tanácsadás, 'Adatkezelési Alapelvek' <<https://gdpr-tanacsadas.hu/adatkezelesi-alapelvek/>> accessed 12 March 2021.

²⁷² Hungarian National Authority for Data Protection and Freedom of Information, 'Érintetti Jogok'

<<https://naih.hu/erintetti-jogok>> accessed 22 February 2021.

Infotv. is the legal basis for the processing and its general conditions, based on which the data subject may restrict the processing. Authorization to process data may, as a general rule, be obtained with the consent of the data subject, a purpose based on the public interest prescribed by law, and, exceptionally, in a narrow scope, by general statutory authorization.

Additional guarantees for special data are provided by law, the legal basis of which is written consent, the range of legitimate purposes for which the processing of certain special data can be compulsorily ordered. However, criminal personal data may only be processed by data controllers specified by law.²⁷³

Consent must be based on the free will of the data subject, the use of any coercion is prohibited. Infotv. establishes as a condition the so-called discretion, or self-determination, which begins in children from the age of 16, but must also be examined in the case of persons who are unable to act for other reasons.

The stipulation of information means that the data subject has received a complete and real picture of the consequences of data processing and its impact on his or her rights. The data controller is obliged to provide information.

Vulnerability can exist when, due to complexity, publicity is not ensured, and a lack of legal knowledge enters due to lack of time.

Due to the principle of determination, unambiguous consent is required, so there is no place to presume consent. There are two exceptions to the above rule, as it can be presumed in cases initiated at the request or possibly initiated by the data subject with regard to the data provided by him, in addition, it can be considered provided in connection with data provided in the public domain.²⁷⁴

4.3. In case of data protection breaches, what is the process to notify the data subject? Are there any exceptional grounds not to notify the data subject? If such grounds exist, what would be the ideal or optimal balance for necessity and proportionality?

The person who is concerned is able to request notification of the processing of your personal data, rectification, deletion or blocking of your personal data given by the Infotv. The data subject shall have the right to process personal data processed by the controller and the processor acting on their behalf or on their behalf under the conditions laid down in this Law.

The data controller is responsible for compliance with data protection rules and requirements and for enforcing the rights of the data subject.²⁷⁵ The obligation to protect the privacy of data

²⁷³ Section 5 Infotv.

²⁷⁴ Section 6 Infotv.

²⁷⁵ Section 14 Infotv.

subjects during data processing is also the duty of the data controller.²⁷⁶ The development of internal regulations is an obligation for data security, technical and organizational measures, and the development of procedural rules. In the event of a damage event, the data controller is responsible for compensating the data subject for the damage caused by the data processor.²⁷⁷

Infotv. has a specific chapter to ensure the rights of the data subject. Among other things, the right to information, the right of prior information, the right of access, the right of rectification, the right to restrict processing, the right to erasure, the initiation of NAIH proceedings for the enforcement of rights, the right to bring a case to court and the right to compensation.

The data subject's rights are guaranteed by the principles of openness, data quality and limited use. By the principle of openness, we also mean the right to information and the right to access data in accordance with Infotv. Also included is the retention of personal data in the register for a period of less than 5 years. From the submission of the application max. Within 25 days, in a comprehensible form, in writing fulfilment of the information obligation of the data controller. If the data subject does not comply with the data subject's request, the law provides for the possibility of refusal and limited data transfer, in order to protect the rights of others only in writing. It must be communicated within 25 days, stating the reasons and information on the remedy. The principle of data quality basically means the right to rectification and erasure. Correction may be requested if the data do not correspond to reality. There is a place for cancellation if the treatment is illegal if the person concerned is covered by the Infotv. Pursuant to Section 14 c), it requests if the data is incomplete or incorrect if the purpose of the data processing has ceased or it has been ordered by a court or an Authority. In these cases, the data controller has a notification obligation. If the controller fails to do so, he must provide a reasoned written notice within 25 days, indicating the remedy.²⁷⁸

The principle of limited use is filled with content by the right to protest and to delete and block. The protest is the statement of the data subject objecting to the processing of his / her personal data and the termination of the data processing, respectively. asks you to delete the processed data. The legal basis for this is Infotv. Section 21 (1), according to which, personal data processing and transmission is necessary only for the fulfilment of the legal obligation of the data controller. In addition, data management and data processing can take place due to direct business acquisition, public opinion research and scientific research. Deleting data by making data unrecognizable in such a way that it is no longer possible to recover it.²⁷⁹ Data blocking is the identification of a data to limit its further processing permanently or for a specified period of time.²⁸⁰ The right to data security includes the right to complain, based on a decision of the

²⁷⁶ Section 15 Infotv.

²⁷⁷ Section 16 Infotv.

²⁷⁸ Section 17 Infotv.

²⁷⁹ Section 3 point 13 Infotv.

²⁸⁰ Section 3 point 15 Infotv.

Court of Justice of the European Union, which also forms the basis of the GDPR.²⁸¹

The right to enforce a claim is guaranteed by the principle of responsibility. According to this, the sole responsibility lies with the data controller, the data processor is only liable to the data controller, not to the data subject. The burden of proof also falls on the controller. In the case of illegal data processing, it is liable to the data subject, in the case of damage, an obligation to pay compensation, and in the case of a violation of personal rights, an obligation to pay damages arises. The data controller shall be released if it was caused by an unavoidable cause outside the scope of data processing, or if the data subject's intentional, gross negligence may have contributed.²⁸²

5. Does the review constitute effective protection of data privacy?

5.1. Which bodies conduct such review?

Until the introduction of the new Data Protection Act in 2012²⁸³, the review of data protection issues was carried out by the Data Protection Commissioner. 'The main activities are the most important operations necessary to achieve the objectives of the controller or processor.'²⁸⁴ Infotv. designates the NAIH to carry out these reviews.

In order to ensure the right to the protection of personal data, NAIH will initiate data protection authority proceedings at the request of the data subject. If the person wishes to initiate the procedure as not a subject, they may initiate the NAIH investigation procedure by filing a public interest notification, but in this case this person may not request the opening of a data protection authority procedure. An application for the initiation of an official procedure may be submitted by post or, if it has electronic identification²⁸⁵, by means of an authentication service for the document traced back to identification, by e-mail to the URL of the document electronically authenticated, sent to the Authority's e-mail address or personally by NAIH customer service. Unless otherwise specified in the GDPR, the data protection authority procedure is subject to the provisions of the administrative regulations. shall apply with the derogations provided for in the Infotv. In the data protection authority procedure, the time limit for administration is one hundred and fifty days. The procedure shall start on the day following the date on which the

²⁸¹ Section 21 Infotv.

²⁸² Section 22 Infotv.

²⁸³ *ibid.*

²⁸⁴ Regulation (EU) 2016/679, art 37 1 (b)-(c).

²⁸⁵ National Infocommunications Service Company (NISZ), 'AVDH – Azonosításra Visszavezetett Dokumentumhitelesítés'

<<https://nisz.hu/hu/avdh-%E2%80%93-azonos%C3%ADt%C3%A1sra-visszavezetett-dokumentumhiteles%C3%ADt%C3%A9s>> accessed 23 February 2021

application is received by the Authority. The period of suspension, suspension and default or delay of the client shall not be counted in the time limit for administration.²⁸⁶

The NAIH is only obliged to initiate official proceedings if it detects the likelihood of unlawful data processing that affects a wide range of persons or that may cause a great harm to the interests or damage. In the event of the detection of unlawful data processing concerning such data, the authority is obliged to initiate official proceedings ex officio, regardless of the number of data subjects or the size of the breach of interest. If the desired result cannot be achieved due to the official procedure, the NAIH may also initiate a lawsuit, which will be heard in the name of a lawsuit initiated for the illegal processing of personal data. The burden of proof also falls on the controller. Illegal data processing enforcement mechanisms include the official notification provided by Infotv. Section 52. Anyone may initiate an investigation with the NAIH on the grounds that there has been or is an imminent threat of an infringement of the processing of personal data or the exercise of rights of access to data of public interest or public interest. Following the notification, it is possible to conduct a privacy lawsuit. There is also a data protection lawsuit in the event that the data recipient goes to court against the data controller, which conducts the proceedings out of turn.²⁸⁷

The specialty of the data protection lawsuit lies in the fact that the burden of proof is on the data controller, NAIH can intervene on the plaintiff's side as an intervener. Sanctions and consequences may include the provision of information, the rectification, blocking, erasure of data, the annulment of a decision made by automated data processing, the obligation to respect the right of the data subject concerned, the obligation to release data requested by the data subject.²⁸⁸

During the NAIH procedure, where the available data are insufficient, it may carry out an evidentiary procedure. In its proceedings, any evidence capable of clarifying the facts may be used. The rules of act CL of 2016 on the General Administrative Order apply to the conduct of the procedure.²⁸⁹

Depending on the outcome of the proceedings, NAIH may initiate lawsuits, criminal or misdemeanour proceedings, which are reported by Infotv.

5.2. What is the process of judicial review for cases of data protection breaches?

There is no administrative appeal against the Authority's decision, but within 30 days of its communication, an application to the Metropolitan Court may be challenged in an administrative

²⁸⁶ Hungarian National Authority for Data Protection and Freedom of Information, 'Adatvédelmi Hatósági Eljárás (GDPR)' <<https://naih.hu/adatkezeles-erintettjekent-fordulok-a-hatosaghoz/adatvedelmi-hatosagi-eljaras-gdpr>> accessed 23 February 2021.

²⁸⁷ Section 64 of Infotv.

²⁸⁸ Section 60 of Infotv.

²⁸⁹ Section 62 of act CL of 2016 on general administrative order.

action. The application must be submitted to the Authority electronically, which forwards it to the court together with the file. The application for a hearing must be indicated in the application. For those who do not receive full personal tax exemption, the court review procedure is subject to a fee of HUF 30,000 and the lawsuit is subject to the right to record the tangible levy. Legal representation is mandatory in proceedings before the Metropolitan Court. Data relating to the processing at issue may not be deleted or destroyed until the time limit for bringing an action to challenge the decision or, in the case of an administrative action, until the final decision of the court has been taken.²⁹⁰

NAIH's decision can only be challenged in administrative proceedings by the data subject, for which the Rules of Procedure Act I of 2017 on the Code of Administrative Procedure are laid down.

The legal remedy may be conducted in court on the basis of the administrative procedure, and may be requested by the client, the prosecutor and, in the relevant part, the other participant in the proceedings.²⁹¹ It is against the decision of the court of first instance, if the appeal is excluded, against the decision of the court of second instance and against its appealable order to change or annul them.

An appeal may be lodged by the client and other participants in the proceedings in the relevant sections on the basis of a legal basis for breach of law or damage to interests.²⁹²

There is a place for a review of a first-instance decision if it is made by the head of a district office or a local government body or a local body of a law enforcement agency, and against a first-instance order if permitted by law.²⁹³

The appellate authority may, based on the decision on the action, decide to uphold, annul, or alter the earlier decision. If the appeal is admissible, it shall be possible within 15 days of notification of the decision.²⁹⁴

The Office itself, the competent authority or anyone to whom it becomes aware may initiate supervisory legal proceedings against any decision alleging an infringement of the law. Following the assessment, the supervisory body may decide to uphold, annul, or change the previous decision.²⁹⁵

²⁹⁰Hungarian National Authority for Data Protection and Freedom of Information, 'Adatvédelmi Hatósági Eljárás (GDPR)'.

²⁹¹ Section 115 of Act I of the Code of Administrative Procedure of 2017.

²⁹² Section 116 of Act I of 2017 on the Code of Administrative Procedure of 2017.

²⁹³ Section 117 of Act I of 2017 on the Code of Administrative Procedure of 2017.

²⁹⁴ Section 118 of Act I of 2017 on the Code of Administrative Procedure of 2017.

²⁹⁵ Section 119 of Act I of 2017 on the Code of Administrative Procedure of 2017.

Any decision may be revoked or amended ex officio based on an infringement of the law, during which the decision-making body acts.²⁹⁶

5.3. Does the review provide effective remedies to the data protection breaches? If so, please specify. For example, what kind of sanctions are imposed as penalties or what remedies are available?

Based on the review, unlawful processing is a consequence of data deletion, court action, damages, and prosecution in categories of non-material damages, infringement proceedings, employment law litigation or criminal proceedings.

The data subject may claim damages under the rules of civil law , ‘who is in breach of their right to privacy, may claim damages for non-material damage suffered by them’²⁹⁷, and damages ‘may be claimed from the infringer in accordance with the rules of liability for damage caused unlawfully.’²⁹⁸

The Civil Code by introducing the institution of damages instead of non-pecuniary damages as a subjective sanction for violations of the rights of the individual, takes a clear position on the issue that damages can only be a pecuniary disadvantage that can be clearly expressed in money and only in the case of a violation of any individual rights; order the offender to pay compensation for non-pecuniary damage. The function of damages is twofold to compensate the person concerned for non-pecuniary damage to him or her as a result of a violation of his or her personality, as well as, a private penalty. It is not necessary to prove the occurrence of an actual disadvantage in order to be entitled to damages, but it is still in the interest of the claimant to prove the actual disadvantage and its extent, as this is also taken into account by the court when determining the amount of damages. It is not clear from the Civil Code whether the circumstances of the case include the personality of the injured party in determining the amount of damages. The consideration of the gravity of the violation, the degree of imputability and the repetitive nature when determining the amount of the damages is set out in a questionable provision, as this further strengthens the punitive nature of the damages. In addition to damages, it is also possible to enforce a claim for compensation for property damage caused by a personal injury.²⁹⁹

The real difference between liability for damages and damages is that the person entitled to compensation suffers damage as a result of a violation of his or her personal rights, so he or she can claim damages from the infringer under the rules of liability for unlawful damage.³⁰⁰

²⁹⁶ Section 121 (1)-(4) of Act I of 2017 of the Code of Administrative Procedure of 2017.

²⁹⁷ Section 2:52 Civil Code.

²⁹⁸ Section 2:53 Civil Code.

²⁹⁹ Section 2:52 Civil Code.

³⁰⁰ Section 2:53 Civil Code.

Personal rights can only be enforced in person, so these claims are not transferable or inheritable, so if the rightsholder dies, his successor cannot sue in his own right, but if the rightsholder dies in a lawsuit that has already been initiated, his successor can enter the lawsuit. In the event of the death of the infringer, the claimant may act against his or her heir, and his claim is considered a burden of inheritance.³⁰¹

The protected legal object of personal data misuse is the social interest in personal data, and a passive subject is the natural person to whom the data relate. The object of the offense is personal data: data that can be linked to the data subject and a conclusion that can be drawn from the data about the data subject. The offending behaviours are data management, failure to take security measures and failure to provide information.

The Criminal Code Act C of 2012 dedicates a separate criminal offence to the misuse of personal data. Data management covers any operation or set of operations on data, in particular: collection, recording, recording, systematisation, storage, alteration, use, retrieval, transmission, disclosure, coordination or interconnection. Personal data may be lawfully processed if the data subject consents to it, or is ordered by law or regulation by a local government decree for a purpose in the public interest, or if obtaining the data subject's consent would be impossible or would involve disproportionate costs. Condition for processing of special data: written consent of the data subject. Not required if necessary, for the implementation of an international agreement.

You will fail to take security measures if you fail to take steps to ensure data security. Failure to provide information is only possible by operation of law. The data controller is obliged to provide information in writing in a comprehensible form within the shortest time from the submission of the request, and within a maximum of 30 days. If you fail, you will commit the crime.

It can be deduced from the facts of the law that the offense may harm the personal or property interests of the passive subject. Shapes containing the result become complete when the interests of at least one passive subject are significantly harmed. Direct intent is an essential condition for carrying out an unlawful profit. In the Criminal Code negligent offenses are not punishable. Criminal cases are offenses committed against special personal data or criminal personal data and when committed as an official or on behalf of a public authority.³⁰²

The protected legal object of misuse of public interest data is the social interest in accessing public interest data, although it can be anyone. The object of the offense is the data of public interest itself, but public data from the public interest is not covered by criminal law protection. The offenses are concealment, failure to provide information, making inaccessible, falsification,

³⁰¹ Section 2:54 Civil Code.

³⁰² Section 219 of the Criminal Code Act C of 2012.

making available or disclosing false or falsified information. The existence of data of public interest must be understood as a denial that the data controller has the required information. The body performing the public task handling the data shall comply with the request for access to the public data as soon as possible, but not later than within 15 days, which may be extended by 15 days at a time. may contact the claimant. Making data inaccessible can be done by hiding or destroying data of public interest. In the case of falsification, any change to the data which results in it not reflecting reality. Disclosure or disclosure of false or falsified data means allowing others to disclose or disclose data that does not reflect reality. It is more severely punishable by law if these acts are committed for profit.³⁰³

6. What is the process of judicial review of anti-discrimination cases?

Advanced digital technology (ADT) is transforming the world we live in, including posing new sorts of threat against achieving social equality. Hungary has a legal framework on anti-discrimination that seems to be adequate for the traditional forms of discrimination. ADT, however, may challenge its conformity.

6.1. Which bodies conduct such review?

Until January 2021, the review of anti-discrimination cases were carried out primarily by the Equal Treatment Authority, which was set up in 2005 based on Act No. CXXV of 2003 on equal treatment and the promotion of equal opportunities (the ETA Act), and was abolished by Act No. CXXVII of 2020³⁰⁴ in which the tasks laid down in the ETA Act were transferred to the Commissioner for Fundamental Rights. Administrative procedure is generally preferred to court proceedings, as it is considered to be more time-effective besides also having an impressive legal toolkit of sanctions. The authority can impose a fine, the amount of which can range from fifty thousand to six million forint,³⁰⁵ and order the publicity of the decision, as well as order the ending of unlawful situations and prohibiting the unlawful conduct.³⁰⁶ The decision of the Authority can be challenged at the Capital Regional Court.³⁰⁷ Laws and their provisions as well as court decisions concerning the principle of equal treatment shall be examined – upon request – by the Constitutional Court³⁰⁸ in conformity and under the conditions set by Act No. CLI/2011 on the Constitutional Court (ACC), that lays down the different forms of requests (e.g. constitutional complaint, posterior norm control, judicial initiative). The Constitutional Court shall annul the challenged decision/law/its provision in case it is found to be contrary to the

³⁰³ Section 220 of the Criminal Code Act C of 2012.

³⁰⁴ Section 2 (8) of Act No. CXXVII of 2020 on amending certain laws to ensure more effective enforcement of the requirement of equal treatment.

³⁰⁵ Section 17/A (5) of the ETA Act.

³⁰⁶ Section 17/A (1) of the ETA Act.

³⁰⁷ Section 13 (2) of the ETA Act.

³⁰⁸ Article 24 (2)-(4) of the Fundamental Law.

Fundamental Law or international treaty.³⁰⁹ In case of an omission the Constitutional Court – acting ex officio – ‘shall call upon the organ that committed the omission to perform its task and set a time-limit for that.’³¹⁰

6.2. What are the elements that are taken into consideration when such review is conducted?

Until 2012, before the Fundamental Law was adapted, the Constitutional Court has already played a significant role in laying down the fundamental principles of the theory of equal treatment, adapting an extensive interpretation of Article 70/A of the Act XX of 1949 The Constitution of the Republic of Hungary (Constitution) in two different ways.³¹¹ Firstly, the Constitutional Court established, the constitutional principle of equal treatment is also applicable in cases when the discriminatory conduct does not restrict fundamental right, if it results in the violation of human dignity.³¹² Secondly, the Constitutional Court in Decision 9/1990 (IV.25.) AB,³¹³ established that the scope of protection against discrimination is not limited to the state-citizen (vertical) relations, stemming from the grammatical interpretation of Section 70/A, but it expands on the whole legal system.³¹⁴ The Fundamental Law entered into force on 1 January 2012, and similar to regulation of the Constitution, it states that ‘Hungary shall guarantee the fundamental rights to everyone without discrimination and in particular without discrimination on grounds of race, colour, sex, disability, language, religion, political or other opinion, national or social origin, property, birth or any other status.’³¹⁵ The extensive interpretation adopted by the Constitutional Court of the principle of anti-discrimination presented above has been reinforced by the Court.³¹⁶

The legal framework gradually adjusted to the theories established in the early case law of the Constitutional Court. The ETA Act was adapted with the view of conforming with secondary union law, thus the scope of protection laid down in ETA Act covers not only the public sector, but also considerable parts of the private sector,³¹⁷ that is essential, as it forms the legal ground for protection against discrimination caused by civil legal entities such as employers, credit-institutions, or other organizations using a selection mechanism that could potentially be

³⁰⁹ Article 24 (3) (a)- (c) of the Fundamental Law.

³¹⁰ Section 46 of the ACC.

³¹¹ Lóránt Csink, Balázs Schanda, András Zs. Varga (eds), *The Basic Law of Hungary – A First Commentary* (Clarus Press Ltd 2012) 171

<www.eui.eu/Documents/General/DebatingtheHungarianConstitution/TheBasicLawofHungary.pdf> accessed 25 February 2021.

³¹² Attila Menyhárd, ‘Diszkrimináció-tilalom és polgári jog’ (PJK, 2006/3) 8-15

<www.ptk2013.hu/polgari-jogi-kodifikacio/menyhard-attila-diszkriminacio-tilalom-es-polgari-jog-pjk-20063-8-15-o/256> accessed 12 February 2021. See also: Decision 20/1999. (VI. 25.) AB, ABH 1999, 159, 163.

³¹³ ABH 1990, 46.

³¹⁴ Menyhárd (n 312); Decision 61/1992. (XI. 20.) AB (ABH 1992, 280).

³¹⁵ Article XV (2) of the Fundamental Law.

³¹⁶ e.g. Decision 30/2017. (XI. 14.) AB; Decision 42/2012. (XII. 20.) AB; Decision 3086/2013. (III. 27.) AB; Decision 32/2015. (XI. 19.) AB.

³¹⁷ Section 4 - 5 of the ETA Act.

discriminatory. The ETA Act specifies different forms of discrimination: negative and positive, direct and indirect forms of discrimination, harassment, unlawful segregation, and victimisation.³¹⁸ With exceptions provided for by the ETA Act (namely: segregation, direct negative discrimination on the basis of sex, race, nationality, origin, or colour³¹⁹), there is possibility of justification either according to the necessity-proportionality test stemming from Article I (3) of the Fundamental Law, or – when discrimination does not concern a fundamental right – on ‘reasonable grounds upon impartial consideration.’³²⁰

Advanced Digital Technology poses a new challenge to the traditional judicial and legal framework regarding the principle of equal treatment. General Data Protection Regulation No. 2016/679 (GDPR) – that also forms the basis of the national legal framework concerning data protection – has addressed the issue of all-determined discrimination restricting and safeguarding ‘solely’ automated decision-making [Article 22 (1)], and prohibiting discrimination [Article 71]. Regarding individual enforcement of rights, Directive 2000/43/EC states that plaintiffs ‘need to establish facts from which it may be presumed that there has been direct or indirect discrimination.’³²¹ This means that they need to establish ‘at a very minimum, [...] a statistical disparity between the impact of the algorithmic process on the protected and a comparable group’.³²² The question this raises concerns whether such a requirement from the victim is reasonable, or if it requires too much information, that may cut off victims already at this very first stage as they do not possess the information necessary. The ETA Act lays down a legal framework that could be more favourable to the victim, as in cases of suspected discriminatory conduct, the injured or entitled party is only obliged to render the disadvantage and the possession of a protected characteristic (defined in Article 8) probable.³²³ Then the opposite party has to prove that ‘the circumstances rendered probable [...] did not prevail, or one did observe the principle of equal treatment, or that one was not obliged to observe the principle of equal treatment in respect of the relevant relationship.’³²⁴ This means that victims don’t even have to establish a *prima facie* case in a way it is required by European law.

6.3. Does the review constitute effective protection against discrimination?

Despite the fact that it is not explicitly required by Section 19 (1) (a) of the ETA Act, in order either to establish a *prima facie* case of discrimination, or just to presume the disadvantage itself, the opponent needs information on persons in a comparable position to him/her, to whom the

³¹⁸ Section 7 (1) of the ETA Act.

³¹⁹ Section 8 a)-e) of the ETA Act.

³²⁰ Section 7 (2) (b) of the ETA Act (see also: Decision 30/1997. (IV. 29.) AB).

³²¹ Council Directive 2000/43/EC of 29 June 2000 on implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L180/22, art 8.

³²² Philipp Hacker, ‘Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law’ (2018) 55(4) Common Market Law Review 1166

<file:///H:/ELTE-%20JOG/8.%20szemeszter/munka/ELSA/SSRN-id3164973.pdf> accessed 18 February 2021.

³²³ Article 19 (1)-(2) of the ETA Act.

³²⁴ *ibid.*

disadvantage (less favourable treatment) is realised, as disadvantage is understood can mostly be proved in a relative sense.³²⁵ The friction between data protection and anti-discrimination law manifests itself through the fact that the collection of information on data relating to attributes such as race, religion, or sexual orientation are specifically prohibited for automated decision making by data protection regulation.³²⁶ Although the controller needs to provide ‘meaningful information about the logic involved as well as the significance and envisaged consequences of such processing for the data subject’ according to Article 15 (1) (h) GDPR, the exact obligations regarding the obligations of the data controller is unclear.³²⁷ With reference to individual access rights, a rule in the new Code of Civil Procedure of Hungary adapted in 2016³²⁸ may be of assistance to the victim, according to which in case of incapacity to allege, the statement of fact affected by the incapacity shall be accepted by the court as the truth, if it does not have any doubt regarding its veracity.³²⁹ In technology-based discrimination cases this provision may be of help to the opponent. A party is in a privileged case of incapacity to allege ‘if he does not have the information necessary to prove a scientific fact, and the party with opposing interests, who holds the information in question, does not prove a specific fact, and the party with opposing interests, who holds the information in question, does not provide the information despite being called upon to do so.’³³⁰ By applying this rule, the obligation to state the fact can also be transferred to the opposing party in cases when the victim cannot get access to data needed in order to render the disadvantage presumably.

Both rules set above were already considered by some to impose an almost disproportionate burden on the defendant in traditional forms of discrimination, and yet in cases of all-determined discrimination, the legal framework in this regard may still come across as insufficient for the protection of the victim.

6.4. What is a considered role of the technical aspects that result in discrimination?

Access rights only cannot resolve the problem of bias which – due to the complexity and opacity of all-determined decision making – go unnoticed.³³¹ This problem is becoming especially relevant in the field of crime prevention, because secret surveillance is by nature non-transparent for the public. In 2014 seventy CCTVs with facial recognition capabilities were set up in District 8 in Budapest. The collection and processing of such data could be considered potentially

³²⁵ Katalin Gregor, Judit Varga, Adél Lukovics, and Veronika Molnár, *Az Egyenlő Bánásmódról és az Esélyegyenlőség Előmozdításáról Szóló 2003. Évi CXXV. Törvény Alkalmazása* (Egyenlő Bánásmód Hatóság 2018) 11.

³²⁶ Hacker (n 322) 1175.

³²⁷ *ibid*, 1169.

³²⁸ Act CXXX of 2016 on the Code of Civil Procedure.

³²⁹ Section 184 (2) of Act No. CXXX of 2016 on the Code of Civil Procedure.

³³⁰ Definition of ‘állítási szükséghelyzet’ provided for by the data base on legal terminology of the Ministerium of Justice (<https://termin.im.gov.hu/>).

³³¹ Bence Ságvári, ‘Diszkrimináció, átláthatóság és ellenőrizhetőség’ (2017) *Replika* 3/103 64-72

<www.epa.oszk.hu/03100/03109/00006/pdf/EPA03109_replika_103_061-079.pdf> accessed 28 February 2021.

discriminative, given that the roma population in District 8 is relatively high.³³² Thus, the recommendation of Hungarian Civil Liberties Union (HCLU) and Privacy International (PI) was to ‘ensure that the deployment of CCTV cameras with facial recognition technology comply with the requirements of right to privacy and protection of personal data and do not result in discrimination against the Roma.’³³³ Revolving around the legislation on secret surveillance, a case in 2016 was brought before the ECHR concerning the fact – that has also been pointed out in a recommendation of HCLU and PI – that there is no requirement for prior judicial authorisation of surveillance for purposes of national security, instead, the authorisation is provided by the Minister of Justice.³³⁴ The European Court of Human Rights, assessed that the challenged provisions were in conflict with Article 8 of the European Convention on Human Rights.³³⁵ Both cases - referred to above - raise the question of the need for effective control on the operation of government bodies i.e. law enforcement authorities, especially the ones carrying out secret surveillance. In Hungary the requirement of such control falls mostly upon the judicial branch.³³⁶

6.5. How are these problems tackled?

According to the case law of the Court of Justice of the European Union (CJEU) ‘an opaque system needs to be made transparent concerning the criteria used for anti-discrimination cases.’³³⁷ The data controller, however, can do this without any obligation ‘to specifically explain the factors that led to the algorithmic output.’³³⁸ Such obligation would most likely infringe copyright,³³⁹ and in addition, algorithms can be biased in several different ways, most forms of which are very difficult to tackle or prove. A major issue is that it is now on the courts to decide whether an algorithm carried out a discriminative decision, but without proper investigation bodies, the necessary tools and knowledge to examine the training data and functioning of the mechanism, they end up being satisfied with formal reasoning, and procedure even if the victim can set up a *prima facie* case of discrimination.³⁴⁰ To tackle this the European Commission's White Paper on Artificial Intelligence puts forward specific, practical proposals, i.e. to adjust or

³³² Hungarian Civil Liberties Union and Privacy International, The Right to Privacy in Hungary Stakeholder Report Universal Periodic Review 25th Session – Hungary (2015) 8

<file:///H:/ELTE-%20JOG/7.%20szemeszter/munka/ELSA/JS8_UPR25_HUN_E_Main.pdf> accessed 28 February 2021.

³³³ *ibid.*

³³⁴ *ibid.* 4. The Constitutional Court had previously conducted a review on this case and found that the lack of judicial authorisation was not in conflict with the Fundamental Law. Decision 32/2013. (XI. 22.) AB.

³³⁵ *Szabó and Vissy v Hungary*, App no. 37138/14 (ECHR, Judgment of 12 January 2016).

³³⁶ Emese Pásztor, ‘Magánélet és bizonytalanság’ – A jogi kontrollmechanizmusok szerepe a nemzetbiztonsági célú titkos információgyűjtés alapjogi kockázatainak mérséklésében’ (2017) *Információs Társadalom* XVII/1 24-44 <file:///H:/ELTE-%20JOG/8.%20szemeszter/munka/ELSA/Maganelet_es_bizonytalansag_-_A_jogi_kontrollmechanizmusok_szerese_a_nemzetbiztonsagi_celu_titkos_informaciogyujtes_alapjogi_kockazatainak_mers ekl eseben.pdf> accessed 17 February 2021.

³³⁷ CJEU, Case 109/88, *Danfoss*, EU:C:1989:383 cited by Hacker (n 322) 1165.

³³⁸ Hacker (n 322) 1160.

³³⁹ Ságvári (n 331) 73-75.

³⁴⁰ Hacker (n 322) 1147.

clarify existing legislation in certain areas that set out specific requirements for the quality of teaching data sets and test procedures for detecting and correcting bias, which filter out negative discriminatory effects at an early stage, and ensure continuous monitoring and supervision of compliance with existing equality legislation throughout its life cycle.³⁴¹

7. Does your country have any specific regulations on Advanced Digital Technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?

7.1. Introduction

When it comes to assessing the upper question in Hungary, it cannot be argued that external legislative developments are not crucially influential in our country. Hungary is part of the European Union (EU), meaning that EU Legislation³⁴² is directly applicable. Just as much public and private international law and international criminal law are applicable in the usual manners. Leaving us with the consequence that there is an enormous influence on Hungary from abroad.

7.2. Big Data

Over the course of nearly a decade and a half, more and more research results have emerged at the frontiers of sociology, economics, and social geography, the empirical material of which was some Big Data source.

The scientific exploitation of Big Data is by no means a novel curiosity today. Interdisciplinary research centres have been established in many universities worldwide to conduct research on various topics; prestigious international conferences on the subject have been held for years, and international journals in the field have also been published.³⁴³

This process can already be observed in Hungary, even if the number of published empirical research results is low and there are relatively few people who deal with this field.

This study does not aim to explain what we mean by Big Data, as several Hungarian scholars have already done it in recent years.³⁴⁴

³⁴¹ European Commission, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust* COM (2020) 65 final, 14-22
<https://www.ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf>
accessed 17 February 2021.

³⁴² According to the jurisprudence created in and after the case of *Flaminio Costa v E.N.E.L.* - Judgment of the Court of 15 July 1964. - ECLI identifier: ECLI:EU:C:1964:66.

³⁴³ Ságvári (n 331) 2019.

³⁴⁴ Baji 2017, Dessewffy–Láng 2015, Giczi–Szőke 2017, Jakobi 2014, Kmetty 2018, Nagy–Veroszta 2018, Németh 2015, Ságvári 2017a, 2017b, 2017c, Székely 2015, Vukovich 2015, Jakobi–Lócsei 2016, Z. Karvalics 2018.

Are the Harvard University data scientists right that the Big Data revolution is nothing more than a peculiar way in which humanity now creates a historical record that can be preserved from its activities?

That the main consequence of this would be a transformation of the image of ourselves through new perspectives that make it possible to know and understand the nature of society more effectively? Furthermore, whether a new scale of quantifiability of human communities and activities leads to a radical transformation of the social sciences and humanities.

7.3. Artificial Intelligence (AI)

In today's technological developments, we are witnessing a substantial rise in artificial intelligence (AI)³⁴⁵, which will continue growing in the future.

John R. Searle treated the concept of AI according to its quality. According to him, we shall distinguish between weak and strong AI. The former refers to systems that 'act' intelligently and the latter to systems that can think in reality.³⁴⁶

The starting point for the authors Ioannis Revolidis and Alan Dahi, is the House of Lords Special Committee on Artificial Intelligence report, which distinguishes between 'narrow', general, and super AI.³⁴⁷

This approach is also used in the definition of the European Union.³⁴⁸ The essence of 'narrow' AI is that the capabilities of machines are similar to human capabilities.

In connection with the legal assessment of AI, three trends emerge in the literature in which AI is evaluated: as a software, as a legal entity, and as a thing. Therefore, we examine the software and study its material nature, and then we turn to the issue of legal entities.

If we consider AI as software, it is subject to the Act LXXVI of 1999 on copyright. (hereinafter: Copyright Act). The Copyright Act defines software as follows: 'computer program creations and their documentation recorded as source code, object codes or in any other form, including application programs and operating systems'.³⁴⁹

³⁴⁵ McCarthy (n 223), az elnevezés 1956-ban született egy Dartmouthban tartott találkozón, amelyen a téma legjelesebb kutatói vettek részt. Az MI és AI kifejezések egyaránt a mesterséges intelligenciát jelentik, így a továbbiakban szinonimaként alkalmazzuk e rövidítéseket.

³⁴⁶ Balázs Csanád Csáji, *A Mesterséges Intelligencia Filozófiai Problémái* (kézirat, ELTE Filozófia Szak 2002) 4 <http://old.sztaki.hu/~csaji/CsBCs_MI.pdf> accessed 28 February 2021.

³⁴⁷ Ioannis Revolidis and Alan Dahi, 'The Peculiar Case of the Mushroom Picking Robot: Extra-contractual Liability in Robotics' in Marcelo Corrales, Mark Fenwick, and Nikolaus Forgó (eds), *Robotics, AI and the Future of Law* (Springer 2018) 59.

³⁴⁸ *ibid.* Artificial Narrow Intelligence (ANI): 'which can be defined as »the ability of machines to resemble human capabilities in narrow domains.'

³⁴⁹ Section 1. (2) b).

The Copyright Act does not contain any rules regarding the damage caused by software or the liability of software. In practice, these questions are settled in the licence agreement between the parties, and in most cases, the liability for damages is placed on the user.³⁵⁰

The Copyright Act's main problem is that it focuses on the protection of the author and the work he creates.

This is the purpose of the Act, but it is not enough in terms of AI. The problem with AI is that, although it can be considered as software, it is also capable of actions that other programs have not been able to do before. AI is, therefore, more than an average software as it is a human-like actor.

The Communications of the European Commission 'Towards a common European data space' (2018) and 'Artificial Intelligence for Europe' include the creation of a digital single market.

Hungary has developed its AI strategy following EU provisions; therefore, it is planned to set up a data asset agency and a data marketplace.³⁵¹

Of the wide range of intellectual property, we would now like to highlight only copyrighted works and neighbouring rights, as the Act names software among them.³⁵²

As discussed above, AI qualifies as software under applicable law and is therefore subject to copyright law. All in all, it can be concluded that AI can even be interpreted as an intangible asset.

The Civil Code defines thing as follows: 'physical objects that can be taken into possession can be objects of ownership'³⁵³. The European Commission intends to develop guidelines for the proper interpretation of product liability rules for AI in the future.³⁵⁴

According to Attila Menyhárd, 'taken into possession' means that things have physical characteristics and are accessible to persons. It is an abstract possibility of possession.³⁵⁵

³⁵⁰ Dániel Eszteri, *A Mesterséges Intelligencia Magánjogi Viselkedéséért Való Magánjogi Felelősség Az Online Játékokban* (Pályamunka, Budapest 2014)
<<https://jogaszvilag.hu/a-jovo-jogasza/a-mesterseges-intelligenciaviselkedeseert-valo-maganjogi-felelosseg-az-onlin-e-jatekokban/>> accessed 28 February 2021.

³⁵¹ '2020 Végére Akár Százezren Szerezhetnek Alapismereteket a Mesterséges Intelligenciáról Magyarországon' (Kormány.hu, 2020)
<<https://www.kormany.hu/hu/innovacios-es-technologiai-miniszterium/hirek/2020-vegere-akar-szazezrenszerezhetnek-alapismereteket-a-mesterseges-intelligenciarol-magyarorszagon>> accessed 28 February 2021.

³⁵² *ibid*, Section 25. (7) b).

³⁵³ Section 5:14 (1) Civil Code.

³⁵⁴ 'Mesterséges Intelligencia: A Bizottság Felvázolja a Beruházás Ösztönzésére és Az Etikai Iránymutatások Kidolgozására Vonatkozó Európai Megközelítést' (European Commission, 2018)
<https://ec.europa.eu/commission/presscorner/detail/hu/IP_18_3362> accessed 14 February 2021.

³⁵⁵ Attila Menyhárd, *Dologi Jog* (ELTE Eötvös, Budapest 2014).

Staying with the classical approach, AI can appear as software, which can be considered incorporeal (*res incorporales*) in the absence of physical character. Hungarian regulations have never accepted incorporeal things as things in the classical sense.

Similarly to the Hungarian Civil Code, the German BGB says that objects shall only be qualified as ‘things’ if they are corporeal.³⁵⁶ By contrast, the Austrian Civil Code (ABGB) does not interpret the concept of thing so strictly.³⁵⁷

The Hungarian legislator also plans to adopt the ABGB’s approach; accordingly, AI can be interpreted as a thing in the classical sense due to the tools needed for its proper operation.

In May 2020, Hungary adopted a new comprehensive AI strategy including goals for developing and widening the use of AI.

7.4. Internet of Things (IoT)

The number of different smart devices, smart technologies (e.g. smartphones, smart homes or smart city technologies) is proliferating.

Some assume that the number of ‘things’ connected to the internet has exceeded 50 billion by 2020.³⁵⁸

From one part, our social acceptance, fears, and prejudices need to be examined in combination with our knowledge of technology, yet they make ground for another field of profession – social studies and/or psychology - when it comes to the internet things.

The researchers did not find any clue concerning whether the Hungarian legislator is willing to regulate this particular field. Therefore, it is now to be taken as granted that international law and international practice are relevant in Hungary.

7.5. Encryption

According to an action plan to fight terrorism drafted by the Hungarian Ministry of Interior in 2016, a person using a service providing encrypted communication could be imprisoned for up to two years under the new Hungarian Criminal Code, as detailed under Question 8.³⁵⁹

³⁵⁶ Jürgen Ellenberger, 'Abschnitt 2. Sachen und Tiere' in Palandt (hg.) (ed), Kommentar zum BGB (Beck 2019) 70.

³⁵⁷ Bernard A. Koch, 'Product Liability 2.0 – Mere Update or New Version?' in Sebastian Lohsse, Reiner Schulze, and Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things* (Münster Colloquia on EU Law and the Digital Economy IV, Nomos 2019) 103.

³⁵⁸ SM Pujar and KV Satyanarayana, 'Internet of Things and Libraries' (2015) 62 *Annals of Library & Information Studies* 186-190 <http://op.niscair.res.in/index.php/ALIS/article/view/9800> accessed 14 February 2021.

³⁵⁹ 'Hungarian Government Plans to Enforce Encryption Backdoors' (TASZ) <<https://tasz.hu/cikkek/hungarian-government-plans-to-enforce-encryption-backdoors-1>> accessed 21 February 2021.

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?

8.1. Introduction

Nowadays, more and more crimes are committed in the IT environment, so electronic communications (telecommunication and internet) service providers receive many requests for the release of user data.³⁶⁰

It is essential to mention that in Hungary, electronic communications service providers have a legal obligation to release data for law-enforcement purposes. The following acts provide the legal bases for this: Act XC of 2017 on Criminal Proceedings (hereinafter: Criminal Procedure Code, CPC.), which entered into force on 1st of July 2018. Furthermore, Act C of 2003 on Electronic Communication (hereinafter: Electronic Communication Act.) and Act CVIII of 2001 on certain issues of electronic commerce services and information society services). All the before mentioned acts emphasize the service providers' responsibilities regarding crime prevention, detection and law-enforcement.

8.2. When may be a decryption be conducted about the potential or real consequences of such requirement?

The CPC prescribes the electronic communications service providers' obligation to cooperate to transfer data during criminal proceedings.³⁶¹ In addition, there are also law enforcement agencies that can request information for crime-prevention and crime-detection purposes, regulated by Act XXXIV of 1994 on the Police.³⁶² Moreover, data can also be requested for national security purposes, which is governed by Act CXXV on the National Security Services³⁶³, and the Electronic Communication Act.³⁶⁴

The service provider's obligation to cooperate in criminal proceedings is regulated by the CPC and the Criminal Code. Section 335 of the CPC gives the opportunity for authorities to render electronic information reversibility inaccessible. This is strongly connected to Section 77. of the Criminal Code, which regulates 'Irreversibly Rendering Electronic Information Inaccessible' as a measure that can be imposed by the court at the end of criminal proceedings. The enforcement

³⁶⁰ Deutsche Telekom, *Átláthatósági Jelentés*

<<https://www.telekom.com/en/corporateresponsibility/data-protection-data-security/news/hungary-363562>> accessed 1 February 2021. BBC News, 'Google and Apple Report Jump in Requests for User Data' (2 October 2017) <<https://www.bbc.com/news/technology41442857>> accessed 1 February 2021. Stephen Nellis, 'Apple Sees Steep Increase in US National Security-Related Data Requests' Business Insider (25 May 2018) <<https://www.businessinsider.com/apple-sees-steep-increase-in-us-national-security-related-data-requests-2018-5>> accessed 1 February 2021

³⁶¹ CPC Section 244. (6).

³⁶² *ibid*, 68. (1).

³⁶³ *ibid*, 41. (1) b).

³⁶⁴ *ibid*, 92., 155. § (5).

of the before mentioned measure is governed by Section 92/A of the Electronic Communication Act. The procedure of cooperation between the service provider and the authorities is regulated by Government Decree 180/2004. (V.26.). This decree is about the modalities of cooperation between organisations providing electronic communications services, and organisations authorised to collect information (including secretly).³⁶⁵

Major telecommunications service providers (Hungarian Telekom, Vodafone, Telenor) are obliged to enter into an agreement with the police, the prosecutor's office, and for national security purposes, the Ministry of the Interior. This agreement has to regulate the conditions and the means of (e.g. legal requirements) contribution in data requests (Section 3 of the Government Decree). Police and intelligence agencies cooperate with telecommunications service providers via their officers. These are secret agreements that by no means can be disclosed to the public.

8.3. Sanction against service providers

In criminal proceedings, the service provider or any organisation contacted with a data request may be 'punished' by a disciplinary fee if it fails to comply with the request within the time limit (thirty days by default, and eight days in case of an urgent action), or it unreasonably refuses to comply with the request or violates the rules of informing the authorities. This could be the case, for instance, if the service provider informs the person concerned by the request, or provides information about the request to a third party.³⁶⁶ If the conditions are met, a coercive measure against the service provider, such as the seizure of the requested data, may also be applied.³⁶⁷

If the electronic communications service provider fails to comply with its obligation to render electronic data reversibility or irreversibility inaccessible, the supervising National Media and Communications Authority may impose a fine.³⁶⁸

8.4. Under Hungarian legislation is there too much power given for the authorised body?

The CPC contains the list of the bodies that may make a request to the service provider for information³⁶⁹; these are as follows: the investigative authorities and the police's internal crime prevention and detection body, as well as its counter-terrorism body.

According to the CPC, approval from the prosecutor is required for the authorised bodies to request data inter alia from the electronic communications service provider. [CPC Section 262 (1) c)].

³⁶⁵ 180/2004. (V. 26.) kormányrendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről.

³⁶⁶ CPC Section 265. (1).

³⁶⁷ *ibid.*

³⁶⁸ Electronic Communication Act Section 92/A. (3).

³⁶⁹ CPC Section 262. (1).

An automatic (electronic) data transfer system was developed within the e-government project. This project involved the – National Tax and Customs Administration of Hungary (hereinafter: NTCA), the Counter-Terrorism Centre (CTC), the National Police Headquarters (ORFK), the Budapest Police Headquarters (BRFK) and the prosecution's office. However, not all authorities with investigative powers can request information automatically due to technical and organisational reasons.

For example, the prosecutor's office is connected to the service provider via a direct interface, through which the prosecutor can search directly in the service provider's database. This allows for a more direct and faster search without having to fill out electronic forms like within the police's automated search system (in Hungarian: Robotzsaru).

8.5. Clause of necessity and proportionality

Such a clause can be found in the CPC, as it requires the prosecutor's office to approve the data requests³⁷⁰. However, if the court requests information, then this approval is not needed.³⁷¹

The CPC also introduces the necessity and proportionality³⁷² and, purpose limitation clauses³⁷³. Furthermore, the CPC regulates the obligation of data-deleting regarding information that is not needed for the success of the investigation.

According to the CPC, the person who is subject to the data request has to be notified. This notification may be postponed if it would jeopardize the effectiveness of the criminal proceeding³⁷⁴. Furthermore, the service provider may not provide information about the request to anyone other than the person concerned³⁷⁵.

In practice, it is not typical for a service provider to refuse a request for data. Although there are some formal and substantive limits (e.g., legal reference, purpose limitation), these are observed by the law-enforcement authorities.

As technology advances, paper-based administration is increasingly lagging, and it is more and more common that the investigating authority is requesting data that is not specifically regulated by legal provisions. An example of this is that in the past, only paper-based customer contracts were made, but now a contract can be concluded electronically. There is no customer signature on the electronically concluded contracts, so there is no proof of their copy, only the IP addresses used by the customer at the time of conclusion of the contract. At this point, a consultation was needed with the investigating authority: whether the IP address used when entering the webshop or dynamic IP addresses allocated during the time spent navigating the

³⁷⁰ *ibid.*

³⁷¹ *ibid.*, 261 (1).

³⁷² *ibid.*, 264 (4).

³⁷³ *ibid.*

³⁷⁴ *ibid.*, 267 (4).

³⁷⁵ *ibid.*, 264 (7).

webshop was necessary for proof. On issues such as this, consultation with the investigating authority is ongoing.

Electronic communication service providers have so-called ‘decoding obligations’ that are required by law.

The service provider is also obliged to decrypt the information if the encryption was performed by it and not by a user.³⁷⁶ The CPC says that ‘all contacted organisations’ have to encrypt the requested data. Data that have been encrypted or otherwise rendered inaccessible shall be restored to their original condition, or the content of the data shall be made available according to Section 264. (3) of the CPC.

The service provider is also obliged to ensure in case of the collection of confidential information that during interception, the authorised persons can get acquainted with the encrypted information. According to the before mentioned Government Decree, if the communications service provider changes, encodes, or compresses the content of the communication initiated or received by the user, the content of the communication shall be understood as the decrypted, decoded form. However, the service provider is not obliged to decrypt the communication encrypted by the user.

8.6. Is there any individual protection in force?

E-commerce and communications service providers have a growing role to play in obtaining evidence, as the mass of data processed in their systems can be substantial evidence even in the event of a simple crime. The Council of Europe Convention on Cybercrime is the most comprehensive international document today and guides the Member States on the arrangements for the transfer of data stored in the computer system.

The new draft regulation presented by the European Commission in this study aims to ensure that this section is fully operational in international cooperation on human rights in order to ensure a faster transfer of data. The question is whether the service provider, as a market operator, can be obliged to extend its powers to this extent and, if so, where the rule of law remains. Nevertheless, no individual protection was put in place.

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?

In this section, we would like to summarize the Hungarian legislation in terms of the questions detailed above and then provide an answer regarding the adequate balance between digital advancements and the level of human rights protection in Hungary.

³⁷⁶ *ibid*, 264. (2).

Considering data protection in Hungary, only one relatable case can be mentioned before the National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információbiztonság Hatóság, hereinafter: NAIH). In 2020, the authority said that Google AdWords violated the applicant's data subject rights for not fulfilling its obligations related to appropriate information supply on its automated data processing practice.³⁷⁷ In May 2020, the Hungarian Government published a decree³⁷⁸ which suspended data subjects' rights provided in the GDPR when it comes to COVID-19 related data processing operations. According to the regulation, when personal data is processed for the purpose of preventing and analysing COVID-19 infections, data subjects' rights provided by the GDPR, like right to rectification, erasure or access are suspended until the end of the official state of emergency. Given that the GDPR is a directly applicable EU regulation, derogating from its provisions to the aforementioned extent was questioned by the European Data Protection Board.³⁷⁹ In March 2020, during the state of emergency, the minister for innovation and technology was enabled to access and handle 'any available data' to combat the COVID-19 pandemic.³⁸⁰

In Hungary, the deployment of facial recognition technology is not systematic and most often used to identify wanted or missing persons, although the real situation of its deployment is not transparent for the public. It has been revealed that the main state institution authorised to collect and control confidential information with facial recognition technology is the Special Service for National Security (SSFNS).³⁸¹ We also emphasized under Question 6 that currently, there is no requirement for prior judicial authorisation of surveillance for purposes of national security by the Counter Terrorism Centre and in some cases by National Security Services. Instead, the authorisation is provided by the Minister of Justice.³⁸²

To conclude the facts regarding the Hungarian situation of data protection, we can state that the human rights issues do and can not hinder technological enhancements. The NAIH has narrow case law in this field, and the legislative framework is full of omissions. It seems that national security and health crises constitute such exceptional circumstances, where broader application of new technology is possible, without data protection taken duly into account.

In Hungary, encryption has detailed rules. There is no obligation to hand over the encryption keys; however, the service and application service providers must ensure that law enforcement bodies can easily access the requested data at any time. Legal interception data is collected

³⁷⁷ 2020/5533. NAIH resolution.

³⁷⁸ Government Decree No. 179/2020. (V. 4.).

³⁷⁹ *Thirtieth Plenary Session: EDPB Response to NGOs on Hungarian Decrees and Statement on Article 23 GDPR* (European Data Protection Board).

³⁸⁰ Government Decree 46/2020 (III. 16.).

³⁸¹ *In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World* (International Network of Civil Liberties Organizations) <<https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf>> accessed 12 March 2021.

³⁸² see Question 6.

without the personal involvement of the employees of the service and application service providers.³⁸³ Service providers offering encrypted information exchange applications are required to provide access to the content of encrypted information generated by their clients for authorized intelligence agencies, if the communication is not end-to-end encrypted.³⁸⁴ Encryption providers are obliged to retain the encrypted messages and metadata of their clients for one year. Upon request from authorized intelligence agencies, the encrypted communication service providers are obliged to provide the client's ID address, port identifying information, username, and the start and end date/time of the service period.³⁸⁵ Taking into consideration that all these procedures can be initiated after ministerial authorization, it can be concluded that human rights to privacy are undermined in case of surveillance or criminal investigation. Encryption service providers can freely operate in Hungary, so the country is basically a fruitful territory for digital enhancements.³⁸⁶

The Digital Transformation Enablers' Index and the Digital Technology Integration Index ranks Hungary as one of the countries with the most outdated technology.³⁸⁷ More efforts could be made regarding digital infrastructure and human skills. To further push forward digital transformation, the Hungarian Government has recently launched policies aiming at increasing entrepreneurial spirit through a business e-portal and helping more women to become entrepreneurs.³⁸⁸ Hungary is facing a number of challenges regarding digitalisation. To address these issues, a number of strategic documents suggest that the Hungarian government sees digitalisation as an important priority and is willing to cooperate with the stakeholders to launch new initiatives.³⁸⁹

Regarding IoT, artificial intelligence and other technological developments, Hungary does not have any regulation in effect. The Government published its Artificial Intelligence (AI) strategy in September 2020. The AI Strategy consists of three main pillars for facilitating AI adoption. First it details the foundations to be laid, like creating a supportive R&D system and infrastructure, or adopting a regulatory/ethical framework. Secondly, the Strategy pinpoints which sectors will be in focus: manufacturing and automated systems, state administration,

³⁸³ Section 92 of Act C of 2003 on Electronic communications.

³⁸⁴ Section 44 of Act CVIII of 2001 on Online Trade Services and Services Connected to the Information Society.

³⁸⁵ *ibid*, 46.

³⁸⁶ The NRA may impose a fine on the service provider, up to a maximum amount of 0.5% of the revenue of the service provider. If a service provider fails to disclose sales figures or revenue data, the amount of the fine shall be at least HUF 50,000 but not more than HUF 100,000,000, and may be imposed repeatedly. In case of repeated infringements, the NRA may impose a fine between HUF 50,000 - 3,000,000 on the executive officer of the service provider. In the worst case scenario, the NRA may suspend the service for 90 days or even prohibit the service.

³⁸⁷ Monitoring Progress in National Initiatives on Digitising Industry: Country Report Hungary 32.

³⁸⁸ *Digital Transformation Scoreboard 2018: EU Businesses Go Digital: Opportunities, Outcomes and Uptake* (European Commission) 112

<https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Digital%20Transformation%20Scoreboard%202018_0.pdf> accessed 12 March 2021.

³⁸⁹ Monitoring Progress in National Initiatives on Digitising Industry (n 387).

energy, and transport. Thirdly the Strategy outlines specific programs to apply AI, for example, autonomous vehicles, automated administration, and climate driven agriculture.

The research shows us that Hungary has a catching atmosphere for digital investments. Given the fact that Hungary is left behind by other countries pioneering in technology, human rights issues, human rights protection has not been discussed at the state level so far. Concerns have arisen only in the field of data protection and privacy of humans, where bigger emphasis shall be put on fundamental rights, even in the event of crime investigations or national security matters.

10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the upcoming five years?

The development of legal regulation of artificial intelligence is a rather complex but necessary task, as it is essential that the law keeps pace with development. Because of the opacity that characterizes AI, it is important to build trust in technology, of which ethics and legitimacy are important building blocks. Legality itself presupposes ethics, so it is essential that the general ethical principles and moral values prevail in the development and application of AI, and that they might even be assessed in the context of legal regulation.

The legal interpretation and definition of technology may be foreign and omitted for many, yet it is important to see that technological development and its various achievements that also appear in everyday life are gradually transforming our classical legal concepts. Therefore, the creation of an appropriate legal environment can be facilitated by the legal definition of AI in the relevant areas of law. In addition, the solution may be to develop sectoral regulations, i.e. concentrating on specific areas of law, which are able to respond specifically to the specific problems of the given area. All in all, it can be said that the development of the legal regulation of artificial intelligence is such an important and urgent task, in the solution of which, in addition to lawyers, representatives of other disciplines - programmers, engineers - must also participate.

10.1 Upcoming legislation in the EU

Although the existing European rules on civil liability cover most possible scenarios, AI technologies still raise several issues. For example, if a mistake slips in the use of artificial intelligence, it is quite difficult to distinguish between intentional and negligent offense. Who is responsible if an artificial intelligence robot injures a pedestrian in a public area or just makes a mistake during an operation?

The Commission's White Paper of February 2020 emphasises that AI developers and operators must already meet data protection, privacy, non-discrimination, consumer protection, product safety and liability requirements. For example, the GDPR already requires information to be

provided to natural persons when they are subject to automated decision-making (which can also occur in the case of AI-based operation).

In addition, the persons concerned have the right to be informed of the existence of automated decision-making and individuals have the right not to be subject only to automated decision-making, except in certain situations.

In addition, Article 9 of the GDPR and Article 10 of Directive 2016/680 / EU require biometric data to be used to identify natural persons by AI (e.g. facial recognition, automatic border control) in the public interest, with good reason and in a proportionate manner, may affect people's fundamental rights (eg. freedom of expression, non-discrimination). At the same time, AI has features (beyond the black box effect) that challenge the current regulatory framework and needs to be reviewed and, if necessary, supplemented to be able to effectively address the risks posed by AI.

For example, according to the EU Commission's White Paper, the legal problems to be clarified stem from the following circumstances (beyond the black box effect): a reliable, widely available data set; product safety and liability rules.

One year later, at the plenary session of the European Parliament on 20 January 2021, a majority of MEPs present, with the support of 364 MEPs and 274 votes against, adopted a report³⁹⁰ calling for a framework for clearer regulation of European artificial intelligence systems. ensure that clear and ethical principles guide the artificial intelligence developed and used on the continent.

Regulation may be much needed in the light of recent events, such as the recent question of how wise it is to create robots that kill on their own. Human Rights Watch, a human rights organization that has been campaigning³⁹¹ on the subject since 2013 under the name 'Campaign to Stop Killer Robots,' published the results of a survey³⁹² mapping the attitudes of different countries last August, which does not paint a reassuring picture of the situation. While a possible robot war would undoubtedly save the lives of many soldiers, this type of warfare would also take the burden of responsibility away from people and make fighting more acceptable and digestible, potentially undermining peace efforts.

³⁹⁰ European Parliament, Resolution on the Digital Services Act (TA-9-2021-0009) European Parliament, *Resolution on the Digital Services Act* (TA-9-2021-0009)

<https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html> accessed 1 March 2021.

³⁹¹ *Stop Killer Robots* <<https://www.stopkillerrobots.org/>> accessed 1 March 2021.

³⁹² Human Rights Watch, *Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and the Need for a Preemptive Ban* (10 August 2020)

<<https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and>> accessed 1 March 2021.

Despite the increasing innovation, although substantive proposals have been made for regulation, there are still unanswered questions: If damage is caused by a technology, who will be responsible? What would happen if these artificial devices took power over humans? Businesses and individuals need to be given priority protection against ever-emerging innovative solutions. In this way, artificial intelligence needs to be not only declarative by law, but also by regulation that is justified by ethical principles. Based on all this, the European Parliament has taken on a kind of pioneering role, as so far no one has addressed the issues mentioned above. The recommendation adopted by Parliament covers the following issues.

10.1.1. Intellectual property rights

If the Union were to take the lead on global regulation of artificial intelligence, it is important that European patents and intellectual property, as well as its legal system, are not compromised. Technological developments must therefore not run counter to the standards of the Union or be to the detriment of the people. In this way, it is necessary to declare the fact that intellectual property rights can only belong to man and man-made creation. In this way, AI cannot be compared to people and the works they make, as it does not have legal personality either³⁹³.

10.1.2. Questions regarding liability

Artificial intelligence carries significant risk factors, so there is a need to clarify liability for any damage that may occur. This includes broad forms of activity, as in addition to the activity performed, virtual activities can also be a potential source of danger. In its recommendation³⁹⁴ Parliament called for this to be remedied by setting up a liability insurance scheme like that used for motor vehicles, thus helping to ensure transparent and safe situation management.

10.1.3. Ethical dimension

Finally, in parallel with the creation of robotics and other technologies, the obligations and principles along which development and innovation can be implemented must be defined. This means that there will be an explicit expectation for AI to be human-created in all cases and to be people-centred in their operation. Make sure that it is a non-discriminatory and unbiased technology that is transparent and accountable. Furthermore, in order to comply with data protection rules and fundamental rights, they must always be fully compliant. In the case of technologies that are already capable of self-learning, it is important that each component in the

³⁹³ World Intellectual Property Organization, *Artificial Intelligence and Intellectual Property* <https://www.wipo.int/about-ip/en/artificial_intelligence/policy.html> accessed 1 March 2021.

³⁹⁴ European Parliament, *Resolution on the Digital Green Certificate* (TA-9-2020-0276) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html> accessed 1 March 2021.

design process is designed so that all its operating points are man supervised³⁹⁵. This is because there is a risk that if a function would cause a serious misconduct, the control over the technology would not be lost, and thus the process performed independently could be blocked by human intervention.³⁹⁶

10.2. AI and law in Hungary

During our research, we examined three trends in the legal assessment of AI: the quality of AI software, material and legal entities, and we intend to review them in the future, focusing on liability issues. The AI program, which consists of algorithms and source code, is the Act Nr. LXXVI of 1999 on Copyright. The provisions of the law shall apply, but damage caused using the software and the related liability issues shall not be settled by law.

In connection with software belonging to the field of intellectual products, during our research we examined the possibility of regulating them as an asset or a thing. In this context, we concluded that AI - as software - is even legal as an asset with a view to creating a single EU data market. In addition, we also studied the material quality of intellectual products and software, which may be special since AI does not have physical scope. The current Hungarian legislation defines a thing as a physical object that can be taken possession of. Extending the concept of a thing to intellectual products is not new.

After comparing the legal definition of AI and the thing, it can be stated that technology cannot be assessed as a thing in the narrower sense, but rather as an disembodied thing, which, however, is not recognized by the domestic regulations, so it cannot be the subject of property rights. However, it is important to note that software does not work on its own, it assumes a certain physical device - hardware - which is essential for operation, so the concept of a thing can even be extended to technology.

In this connection, we must also talk briefly about the natural forces that can be utilized in the way of things, which are unusual things, to which the rules of things also apply. As a result of the comparison, it can be concluded that in view of the natural forces that can be brought under human rule, the possibility of applying the analogy may even arise in connection with the assessment of the material nature of AI. At the same time, the settlement of liability issues is problematic in this case as well, as the relevant regulations are not known in Hungarian law. In this connection, as regards liability for damage to third parties, it is necessary to mention the existence of liability under French law, under which the custodian is liable for damage caused by

³⁹⁵ *On AI and Robotics* (Policy at Manchester)

<https://policyatmanchester.shorthandstories.com/on_ai_and_robotics/index.html> accessed 1 March 2021.

³⁹⁶ European Parliament, *Study on Artificial Intelligence in the Context of Civil Liability* (2020) IPOL_STU(2020)621926

<[https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU\(2020\)621926_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf)> accessed 1 March 2021.

things. Therefore, in the case of a material assessment of the technology, a modification of the existing liability facts could be a solution to clarify the issues of liability for tort/delict.

In Hungary, digital technology is currently being regulated in three cases: tech companies on the one hand, the establishment of national data assets on the other, and an amendment to the Public Data Act has been announced.

10.2.1. Regulation of tech companies

Today, anyone can be arbitrarily disconnected from the online space without any formal, transparent, fair procedure and redress writes Justice Minister Judit Varga, who adds that they want to achieve nothing more than legal, transparent and verifiable operation. The announced Act is in line with a previous proposal by Data Protection Commissioner Attila Péterfy, who initiated an investigation into the suspension of personal profiles on Facebook to the Hungarian authorities at the August 2020 meeting of the Digital Freedom Working Group. The Digital Freedom Working Group was established in March 2021 by Justice Minister Judit Varga with the aim of making the operation of international technology companies transparent.

10.2.2. Establishment of national data assets

One of the defining terms of the next decade in Hungary is digital state governance, i.e. the creation of clean, machine-processable data, databases and the creation and operation of a modern public administration based on accelerated, proactive and personalized public services based on robots, algorithms and artificial intelligence. Digital government requires modern infrastructure, conscious and informed users, and an advanced digital ecosystem.

According to the Coalition, Hungary will be able to manage the national data assets, with which it will be the first in Europe to implement successful and efficient data management and governance supported by data analysis. According to the Coalition, by adopting the bill, the XXI. A national regulatory environment that responds effectively to the digital challenges of the 21st century. According to Act T/14949 on national data assets, state data should be considered not only as information to be protected but also as a marketable asset.

The tasks of the National Data Asset Agency will include the operation of the national public data portal, the creation and maintenance of a national public data cadastre, the processing and analysis of anonymised databases, and the provision of data analysis services to government, the market and citizens.

Table of legislation

Provision in Hungarian	Corresponding translation in English
Magyarország Alaptörvénye	Hungarian Constitution
VI. cikk (3)-(4):	VI. Articles 3 to 4:
(3) Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.	(3) Everyone has the right to the protection of personal data concerning him or her and to have access to and dissemination of his or her data of public interest.
(4) A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi.	(4) Independent official control of the enforcement of the true right to the protection of personal data and access to data of public interest established by a cardinal law.
XV. cikk (2):	XV. Article 2 (2):
(2) A Kormány a közigazgatás legfőbb szerve, törvényben meghatározottak szerint államigazgatási szerveket hozhat létre.	(2) The Government is the supreme body of public administration, and may establish public administration bodies as specified by law.
24. cikk (2)-(4):	Article 24 (2) to (4):
(2) Az Alkotmánybíróság	(2) The Constitutional Court
a) az Alaptörvénnyel való összhang szempontjából megvizsgálja az elfogadott, de ki nem hirdetett törvényeket;	(a) laws adopted but not promulgated can actually be purchased with the Basic Law;
b) * bírói kezdeményezésre soron kívül, de legkésőbb kilencven napon belül felülvizsgálja az egyedi ügyben alkalmazandó jogszabálynak az Alaptörvénnyel való összhangját;	b) * on the initiative of a judge, review the legislation applicable in an individual case out of turn, but within at least ninety days, by playing with the Basic Law;
c) alkotmányjogi panasz alapján felülvizsgálja az egyedi ügyben alkalmazott jogszabálynak az Alaptörvénnyel való összhangját;	(c) on the basis of a constitutional complaint, review the legislation applied in the individual case by playing with the Basic Law;
d) alkotmányjogi panasz alapján felülvizsgálja a bírói döntésnek az Alaptörvénnyel való összhangját;	d) on the basis of a constitutional complaint, review the judicial decision by playing with the Basic Law;
e) * a Kormány, az országgyűlési képviselők egynegyede, a Kúria elnöke, a legfőbb ügyész vagy az alapvető jogok biztosa kezdeményezésére felülvizsgálja a	e) * review of the Government, a quarter of the members of parliament, the Speaker of the Curia, the Attorney General or the Commissioner for Fundamental Rights to

jogszabályoknak az Alaptörvénnyel való összhangját; f) vizsgálja a jogszabályok nemzetközi szerződésbe ütközését; g) az Alaptörvényben, illetve sarkalatos törvényben meghatározott további feladat- és hatásköröket gyakorol. (3) Az Alkotmánybíróság a) * a (2) bekezdés b), c) és e) pontjában foglalt hatáskörében megsemmisíti az Alaptörvénnyel ellentétes jogszabályt vagy jogszabályi rendelkezést; b) a (2) bekezdés d) pontjában foglalt hatáskörében megsemmisíti az Alaptörvénnyel ellentétes bírói döntést; c) * a (2) bekezdés f) pontjában foglalt hatáskörében megsemmisítheti a nemzetközi szerződésbe ütköző jogszabályt vagy jogszabályi rendelkezést; illetve sarkalatos törvényben meghatározott jogkövetkezményt állapít meg. (4) * Az Alkotmánybíróság a jogszabály felülvizsgálni nem kért rendelkezését csak abban az esetben vizsgálhatja, illetve semmisítheti meg, ha az a felülvizsgálni kért jogszabályi rendelkezéssel szoros tartalmi összefüggésben áll.	ensure that the legislation is in line with the Basic Law; (f) investigate conflicts with international treaty law; g) exercise additional duties and powers specified in the Basic Law or in the Cardinal Law. (3) The Constitutional Court (a) * annul, in the exercise of its powers under paragraph 2 (b), (c) and (e), any act or provision contrary to the Constitution; (b) annul a judicial decision contrary to the Constitution in its power under paragraph 2 (d); (c) * annul an act or provision of law which is inconsistent with an international agreement in the exercise of its powers under paragraph 2 (f); or establishes a legal consequence specified in a cardinal law. (4) * The Constitutional Court does not provide for the review of legislation in accordance with the provisions of the decree only if it examines or annuls it if it is closely related to the provisions of the review legislation.
1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról 1. szakasz 1. § (1) E törvény célja annak biztosítása, hogy - ha e törvényben meghatározott jogszabály kivételt nem tesz - személyes adatával	Act XIII of 1992 on the protection of personal data and the publicity of data of general interest Section 1 § 1. (1) The purpose of this Act is to ensure that, unless the legislation specified in this Act makes an exception, everyone has their own

mindenki maga rendelkezzen, és a közérdekeű adatokat mindenki megismerhesse.	personal data and that everyone can get acquainted with data of public interest.
2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről	Act CVIII of 2001 on on Electronic Commerce and on Information Society Services
2003. évi C. törvény az elektronikus hírközlésről 92. szakasz: 92. § * (1) * Az elektronikus hírközlési szolgáltató köteles együttműködni a titkos információgyűjtés folytatására, illetve leplezett eszközök alkalmazására törvényben feljogosított szervezetekkel. Az elektronikus hírközlési szolgáltató az elektronikus hírközlési tevékenységét olyan módon köteles folytatni, amely nem zárja ki, nem lehetetleníti el a titkos információgyűjtést, illetve a leplezett eszközök alkalmazását. (2) * Amennyiben a Nemzetbiztonsági Szakszolgálat írásban kezdeményezi, az elektronikus hírközlési szolgáltató a külön jogszabályban meghatározott időpontig köteles megállapodni a Nemzetbiztonsági Szakszolgálattal a titkos információgyűjtés, illetve a leplezett eszközök alkalmazásának feltételeiről. (3) * Az elektronikus hírközlési szolgáltató köteles minden olyan - a 76. § (1) és (6) bekezdésében foglalt bejelentési kötelezettség hatálya alá nem tartozó - tevékenységéről, szolgáltatásáról, termékéről, illetve annak változásairól közvetlenül tájékoztatni a Nemzetbiztonsági Szakszolgálatot, amely érinti, vagy rendeltetésszerű működésében befolyásolja a titkos információgyűjtést, illetve leplezett eszközök alkalmazása érdekében az elektronikus hírközlési szolgáltató által	Act C of 2003 on Electronic communications Section 92: § 92. * (1) * The electronic communications service provider is obliged to co-operate with organizations authorized by law to continue the collection of secret information and the use of covert devices. The electronic communications service provider is obliged to carry out its electronic communications activities in a way that does not exclude or make impossible the collection of secret information or the use of disguised devices. (2) * If initiated by the National Security Service in writing, the electronic communications service provider is obliged to agree with the National Security Service on the conditions for the collection of secret information and the use of covert devices by the date specified in a separate legal regulation. (3) * The electronic communications service provider is obliged to directly inform the National Security Service about all its activities, services, products and changes thereto, which are not subject to the notification obligation contained in Section 76 (1) and (6), and which affect: or in its intended operation affects the conditions, means, methods and procedures provided or to be provided by the electronic communications service provider in order to collect secret information or use disguised devices.

biztosított vagy biztosítandó feltételeket, eszközöket, módszereket, eljárásokat. (4) * Az elektronikus hírközlési szolgáltató a szolgáltatás megkezdésével egyidejűleg az általa használt, működtetett berendezések, helyiségek és az együttműködő személyek tekintetében - külön jogszabályban meghatározottak szerint - köteles biztosítani az elektronikus hírközlő hálózatban továbbított küldemények, közlések, továbbá a szolgáltató által kezelt adatok titkos információgyűjtéssel, illetve leplezett eszközök alkalmazásával történő megismeréséhez szükséges eszközök és módszerek alkalmazási feltételeit. A szolgáltató az előzőeken túl a Nemzetbiztonsági Szakszolgálat kérésére, a szolgáltatás műszaki jellemzői alapján a szükséges mértékben köteles biztosítani a bevezetett szolgáltatással kapcsolatban a titkos információgyűjtéshez, illetve a leplezett eszközök alkalmazásához szükséges eszközöket a kilépési pontig. (5) Az elektronikus hírközlési szolgáltató köteles az elektronikus hírközlési szolgáltatáshoz a (4) bekezdésben meghatározott igényeknek megfelelő műszaki rendszert - így különösen alapképítésű monitoring alrendszer - létesíteni és ennek elérhetőségét hálózatában a kilépési pontig biztosítani a Nemzetbiztonsági Szakszolgálat részére a műszaki alapkövetelményekről történő írásbeli tudomásszerzéstől számított hat hónapon belül. Az alapképítésű monitoring alrendszer valamennyi költségét a szolgáltató viseli. (6) * A titkos információgyűjtés folytatására, illetve a leplezett eszközök alkalmazására feljogosított szervezetek részére az elektronikus hírközlési szolgáltató egyedi kérelemre szolgáltat adatot, közvetlen	(4) * Simultaneously with the commencement of the service, the electronic communications service provider is obliged to ensure the collection of consignments, communications and data managed by the service provider in the electronic communications network by secret information regarding the equipment, premises and cooperating persons used by it. , and the conditions of use of the means and methods required to become acquainted with the use of covert means. In addition to the above, at the request of the National Security Service, the service provider is obliged, based on the technical characteristics of the service, to provide the necessary means for collecting secret information and using concealed devices up to the exit point. (5) The electronic communications service provider is obliged to establish a technical system for the electronic communications service that meets the needs specified in subsection (4), in particular a basic monitoring subsystem, and to make it available in its network to the exit point. within a month. All costs of the basic monitoring subsystem are borne by the service provider. (6) * The electronic communications service provider shall provide data to organizations authorized to continue the collection of secret information or the use of covert devices upon individual request, by direct electronic data connection, on an interface set up by the electronic communications service provider in accordance with the basic technical requirements specified by the National Security Service. If the requested data is not available via the electronic data connection, the electronic communications service provider shall provide the data in writing or, if required, on an electronic data carrier. The electronic communications service provider shall provide the data to the organizations authorized to continue the collection of secret information

elektronikus adatkapcsolat útján, a Nemzetbiztonsági Szakszolgálat által meghatározott műszaki alapkövetelményeknek megfelelő, az elektronikus hírközlési szolgáltató által kiépített felületen. Amennyiben az elektronikus adatkapcsolat útján az igényelt adat nem hozzáférhető, az adatszolgáltatást az elektronikus hírközlési szolgáltató írásban vagy - erre vonatkozó igény esetén - elektronikus adathordozón teljesíti. Az elektronikus adatkapcsolat kiépítését nem igénylő titkos információgyűjtés folytatására, illetve leplezett eszközök alkalmazására feljogosított szervezetek számára az adatszolgáltatást az elektronikus hírközlési szolgáltató írásban vagy elektronikus adathordozón teljesíti. Az adatszolgáltatási felület valamennyi költségét az elektronikus hírközlési szolgáltató viseli, az adatszolgáltatást az elektronikus hírközlési szolgáltató térítésmentesen teljesíti. (6a) * A titkos információgyűjtés folytatására feljogosított szerv az adatszolgáltatás teljesítésére határidőt jelölhet meg. Az adatszolgáltatás nem tagadható meg. Az így kapott adat csak a megjelölt célra használható fel. (7) * Az elektronikus hírközlési szolgáltatónak - jogszabályban meghatározott esetekben - együtt kell működnie a kormányzati célú hálózat működtetőjével. (8) * Az Elnök rendeletében meghatározott szolgáltató köteles az ott meghatározott tartalmú, folyamatosan felülvizsgált és karbantartott kockázatelemzéssel rendelkezni, és ennek alapján az azonosított kockázatokkal arányos védelmi intézkedéseket alkalmazni. Amennyiben a szolgáltatónál sor került a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény szerinti európai vagy nemzeti	or the use of disguised devices that do not require the establishment of an electronic data connection, in writing or on an electronic data carrier. All costs of the data provision interface shall be borne by the electronic communications service provider, and the data provision shall be provided by the electronic communications service provider free of charge. (6a) * The body authorized to collect confidential information may set a deadline for the provision of the information. The provision of data cannot be refused. The data thus obtained may only be used for the specified purpose. (7) * The electronic communications service provider shall, in cases specified by law, co-operate with the operator of the government network. (8) * The service provider specified in the Decree of the President is obliged to have a risk analysis with the content specified therein, constantly reviewed and maintained, and on this basis to apply protection measures proportionate to the identified risks. Where a service provider has been designated as a European or national critical component under the Act on the Identification, Designation and Protection of Critical Systems and Facilities, the underlying identification report shall be part of the risk analysis and security measures shall be determined taking into account the operator security plan. The service provider is also obliged to have disruption, disaster recovery and business continuity plans with the content specified by law for the management of malfunctions and catastrophes.

létfontosságú rendszerelem kijelölésére, akkor az ennek alapjául szolgáló azonosítási jelentés a kockázatelemzés részét képezi, a védelmi intézkedéseket pedig az üzemeltetői biztonsági terv figyelembevételével kell meghatározni. A szolgáltató köteles továbbá az üzemzavar és a katasztrófahelyzet kezelésére jogszabályban meghatározott tartalmú zavarelhárítási, katasztrófaelhárítási és üzletmenet-folytonossági tervekkel rendelkezni. (8a) * A szolgáltató a különleges jogrend időszakára való felkészülésre vonatkozó jogszabályokban meghatározott feladatok ellátására felkészülési tervet köteles készíteni, valamint az ilyen feladatok ellátásához szükséges mértékű és összetételű tartalékkal köteles rendelkezni. (9) Minősített időszak esetében alkalmazandó intézkedési terv kidolgozása és végrehajtása érdekében az elektronikus hírközlési szolgáltatóknak külön jogszabályban meghatározott módon együtt kell működniük egymással, illetve az illetékes szervezetekkel. (10) Az elektronikus hírközlési szolgáltató minősített időszak idején az intézkedési terv alapján tett intézkedések, illetve a honvédelmi érdekek érvényesítésére vonatkozó jogszabályok szerint általa nyújtott elektronikus hírközlési szolgáltatások tényleges költségeinek megtérítésére jogosult. 92/A szakasz (3): (3) A bíróság a hozzáférést biztosító elektronikus hírközlési szolgáltatóval szemben a büntetőeljárásról szóló törvényben meghatározott mértékű rendbírságot szabhat ki. A külön törvényben meghatározott hatóság a hozzáférést biztosító elektronikus	(8a) * The service provider must draw up a contingency plan for the tasks specified in the legislation on preparation for the period of special legal order and must have a reserve of the amount and composition necessary for the performance of such tasks. (9) In order to develop and implement an action plan applicable to a qualified period, electronic communications service providers shall cooperate with each other and with the competent organizations in the manner specified in a separate legal act. (10) The electronic communications service provider is entitled to reimburse the actual costs of the electronic communications services provided by it in accordance with the measures taken on the basis of the action plan and the legislation on the enforcement of national defense interests during the qualified period. Section 92 / A (3): (3) The court may impose a fine of the amount specified in the Act on Criminal Procedure against the electronic communications service provider providing access. The authority specified in a separate law may impose a fine on the electronic communications service provider providing access in the amount specified in the separate law.

hírközlési szolgáltatóval szemben a külön törvényben meghatározott mértékű bírságot szabhat ki.	
2009. évi CLV. törvény a minősített adat védelméről 3. szakasz 1. pont 1. minősített adat: a) nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - a megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza; b) * külföldi minősített adat: ba) megjelenési formájától függetlenül az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza, bb) a Magyar Honvédség nemzetközi műveletei és gyakorlatai keretében keletkezett,	Act CLV of 2009 on the Protection of Classified Information Classified data 1: (a) national classified information: information belonging to the public interest which may be protected by the rating, containing the rating mark in accordance with the formal requirements specified in this Act and legislation issued pursuant to this Act, which the rating agent has established during the rating process that its unauthorized disclosure, unauthorized acquisition, modification or use, making available to an unauthorized person and limits its publicity and visibility in the context of the rating; b) * foreign classified information: (ba) data produced by any institution or body of the European Union, whatever its form, or by a Member State, foreign party or international organization acting on behalf of the European Union and published in accordance with an international treaty or agreement to which the European Union institutions and bodies have access; Member State acting on behalf of the European Union, another State or a foreign bb) data generated or used within the framework of the international operations and practices of the Hungarian Armed Forces, access to which is restricted by the parties participating in the operation - with the qualification according to the requirements of the operation or practice - regardless of whether the whether Hungary has an agreement with the States represented by the Parties in accordance with subparagraph (ba) for the protection and exchange of classified information, and the provisions for the handling of classified information shall be determined by the

illetve felhasznált olyan adat, amelyhez történő hozzáférést a műveletben résztvevő felek - a művelet vagy gyakorlat követelményei szerinti minősítéssel - korlátozzák, attól függetlenül, hogy a részes felek által képviselt államokkal Magyarországnak van-e a ba) alpontban foglaltaknak megfelelő megállapodása a minősített adat védelmére és cseréjére, és a minősített adat kezelésére vonatkozó rendelkezéseket a Magyar Honvédség, illetve a műveletet vagy a gyakorlatot irányító más részes fél határozza meg	Hungarian Armed Forces or other Party managing the operation or practice;
2011. évi CLI. törvény az Alkotmánybíróságról 46. szakasz 46. § (1) Ha az Alkotmánybíróság hatáskörei gyakorlása során folytatott eljárásában a jogalkotó általi mulasztással előidézett alaptörvény-ellenesség fennállását állapítja meg, a mulasztást elkövető szervet - határidő megjelölésével - felhívja feladatának teljesítésére. (2) A jogalkotói feladat elmulasztásának minősül, ha a) nemzetközi szerződésből származó jogalkotói feladat elmulasztása valósul meg, b) kifejezett jogszabályi felhatalmazásból származó jogalkotói feladat ellenére nem került sor a jogszabály megalkotására, vagy c) a jogi szabályozás Alaptörvényből levezethető lényeges tartalma hiányos. (3) Az Alkotmánybíróság hatáskörei gyakorlása során folytatott eljárásában határozattal megállapíthatja azokat az Alaptörvény szabályozásából eredő, és az Alaptörvény rendelkezéseit érvényre juttató alkotmányos követelményeket, amelyeknek a	Act CLI of 2011 on the Constitutional Court Section 46 § 46. (1) If the Constitutional Court, in the course of its proceedings in the exercise of its powers, establishes the existence of unconstitutionality caused by an omission by the legislator, it shall call upon the body committing the omission to perform its task. (2) A failure to perform a legislative task shall be deemed to exist if: a) failure to perform a legislative task arising from an international treaty, (b) the legislation has not been enacted despite a legislative task deriving from an express legislative power, or c) the essential content of the legal regulation that can be deduced from the Basic Law is incomplete. (3) In the proceedings of the Constitutional Court in the exercise of its powers, it may establish by a resolution the constitutional requirements arising from the regulation of the Basic Law and enforcing the provisions of the Basic Law, which must be complied with.

vizsgált, illetve a bírósági eljárásban alkalmazandó jogszabály alkalmazásának meg kell felelnie.	
2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 1. szakasz: 1. § * E törvény célja a hatálya alá tartozó tárgykörökben az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák, valamint a közügyek átláthatósága a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésével megvalósuljon. 2. szakasz (1): 2. § (1) * E törvény hatálya - a személyes adatok tekintetében a (2)-(6) bekezdésben meghatározottak szerint - minden olyan adatkezelésre kiterjed, amely személyes adatra, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik. 3. szakasz 3, 5, 6, 13, 15 pontok: 3. * különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok, 3a. * genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat,	Act CXII of 2011 on the right to informational self-determination and on the freedom of information regulation Section 1: § 1 * The purpose of this Act is to define the basic rules for the processing of data in the fields covered by it in order to ensure that the privacy of natural persons is respected by data controllers and to ensure transparency in public affairs . Section 2 (1): § 2. (1) * The scope of this Act - with regard to personal data as defined in paragraphs (2) - (6) - covers all data processing that relates to personal data as well as data of public interest or public data in the public interest. Section 3, points 3, 5, 6, 13, 15: 3. * specific data: all data belonging to special categories of personal data, ie personal data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data for the unique identification of natural persons, health data and personal data concerning the sexual life or sexual orientation of natural persons, 3a. * genetic data: any personal data relating to the inherited or acquired genetic characteristics of a natural person which contains specific information on that person's physiology or state of health and which is derived primarily from the analysis of a biological sample taken from that natural person;

amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered; 3b. * biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat; 3c. * egészségügyi adat: egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról; 5. közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat; 6. közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát,	3b. * biometric data: personal data obtained by specific technical procedures relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of the natural person, such as a facial image or dactyloscopic data; 3c. * health data: personal data concerning the physical or mental health of a natural person, including data relating to health services provided to a natural person which contain information on the natural health of the natural person; 5. data of public interest: information or knowledge recorded in any way or form, not covered by the concept of personal data, which is managed by a body or person performing a state or local government task and performing another public task specified by law and which arises in connection with the performance of its activity or public task, regardless of information on the way in which it is handled, whether independent or aggregate, in particular information on competence, competence, organizational structure, professional activity, evaluation of its effectiveness, types of data held and legislation governing operation, as well as information on management and contracts; 6. public data in the public interest: all data which do not fall within the concept of data in the public interest, the disclosure, disclosure or making available of which is required by law in the public interest; 13. * erasure of data: making the data unrecognizable in such a way that it is no longer possible to recover it; 15. * data management restriction: locking of stored data by marking it to restrict further processing of the data.

megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli; 13. * adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges; 15. * adatkezelés korlátozása: a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján. 5-6. szakaszok: 5. § * (1) Személyes adat akkor kezelhető, ha a) azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli, b) az a) pontban meghatározottak hiányában az az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult, c) az a) pontban meghatározottak hiányában az az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, d) az a) pontban meghatározottak hiányában a személyes adatot az érintett kifejezetten nyilvánosságra hozta és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos. (2) Különleges adat a) az (1) bekezdés c)-d) pontjában meghatározottak szerint, vagy	5-6. sections: § 5. * (1) Personal data may be processed if a) it is ordered by law or - by law, within the scope specified therein, in the case of data which does not qualify as special data or criminal personal data - by a decree of a local government for a purpose based on the public interest, b) in the absence of the provisions of point a), it is absolutely necessary for the performance of the data controller's tasks specified by law and the data subject has expressly consented to the processing of personal data, (c) in the absence of the provisions of point (a), necessary and proportionate to protect the vital interests of the person concerned or of another person and to avert or prevent an imminent threat to the life, limb or property of persons, or (d) in the absence of (a), the personal data have been explicitly disclosed by the data subject and are necessary and proportionate to achieve the purpose of the processing. (2) Special information (a) as defined in points (c) to (d) of paragraph 1, or b) may be handled if it is absolutely necessary and proportionate for the implementation of an international treaty promulgated by law, or if it is prescribed by law for the enforcement of a fundamental right guaranteed by the Basic Law, national security, prevention, detection or prosecution of criminal offenses. 3. In the case of the processing provided for in paragraph 1 (a), paragraph 2 (b) and Article 6 (1) (c) and (e) of the General Data Protection Regulation (hereinafter "mandatory processing"), the types of data to be processed,

b) akkor kezelhető, ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli. (3) Az (1) bekezdés a) pontjában, a (2) bekezdés b) pontjában, valamint az általános adatvédelmi rendelet 6. cikk (1) bekezdés c) és e) pontjában meghatározott adatkezelés (a továbbiakban: kötelező adatkezelés) esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg. (4) Kizárólag állami vagy önkormányzati szerv kezelheti az állam bűncselekmények megelőzésére, felderítésére és üldözésére irányuló, valamint közigazgatási és igazságszolgáltatási feladatainak ellátása céljából kezelt bünygyi személyes adatokat, valamint a szabálysértési, a polgári peres és nemperes ügyekre, valamint a közigazgatási peres és nemperes ügyekre vonatkozó adatokat tartalmazó nyilvántartásokat. (5) Ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adatkezelő az adatkezelés megkezdésétől legalább háromévente felülvizsgálja, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának	the purpose and conditions of data processing, the familiarity of the data, the person of the data controller and the period or periodic review of the data processing are determined by the law or local government decree ordering data processing. (4) Only a state or local government body may process personal criminal data processed for the purpose of the prevention, detection and prosecution of criminal offenses and for the performance of administrative and judicial tasks, as well as criminal, civil and non-litigation matters and administrative litigation and non-litigation matters. records containing data. (5) If the duration or the need for periodic review of mandatory data processing is not specified by law, local government decree or mandatory legal act of the European Union, the data controller shall review at least every three years from the commencement of data processing whether the processing of personal data processed is necessary for the purpose of data processing. The circumstances and results of this review shall be documented by the controller, retained for ten years after the review and made available to the Authority upon request by the National Data Protection and Freedom of Information Authority (hereinafter: the Authority). (6) In the case of processing of special data, the controller or processor acting on his or her behalf or on his or her behalf shall ensure by appropriate technical and organizational measures that only those strictly necessary for the performance of his or her tasks related to the data processing operation have access to the data.

megvalósulásához szükséges-e. Ezen felülvizsgálat körülményeit és eredményét az adatkezelő dokumentálja, e dokumentációt a felülvizsgálat elvégzését követő tíz évig megőrzi és azt a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) kérésére a Hatóság rendelkezésére bocsátja. (6) Különleges adatok kezelése esetén az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó megfelelő műszaki és szervezési intézkedésekkel biztosítja, hogy az adatkezelési műveletek végzése során a különleges adatokhoz kizárólag az rendelkezzen hozzáféréssel, akinek az adatkezelési művelettel összefüggő feladatának ellátásához feltétlenül szükséges. (7) Bűnügyi személyes adatok kezelése esetén - ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik - a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni. (8) A tudományos kutatást végző szerv vagy személy személyes adatot nyilvánosságra hozhat, ha az a történelmi eseményekről folytatott kutatások eredményeinek bemutatásához szükséges. 6. § * Kizárólag automatizált adatkezelésen - így különösen profilalkotáson - alapuló, az érintett személyére vagy jogos érdekeire hátrányos vagy az érintettet jelentős mértékben érintő jogkövetkezményekkel járó döntés meghozatalára kizárólag akkor kerülhet sor, ha azt törvény vagy az Európai Unió kötelező jogi aktusa kifejezetten lehetővé teszi és	(7) In the case of processing of personal criminal data, unless otherwise provided by law, an international treaty or a binding act of the European Union, the rules on the conditions for the processing of special data shall apply. (8) A body or person conducting scientific research may disclose personal data if this is necessary for the presentation of the results of research on historical events. § 6 * A decision based only on automated data processing, in particular profiling, which is detrimental to the data subject's personal interests or legitimate interests or which significantly affects the data subject may only be taken if expressly permitted by law or a binding act of the European Union and (a) it does not infringe the requirement of equal treatment, (b) the controller or the processor acting on his behalf or at his disposal (ba) inform the data subject, upon request, of the method and criteria used in the decision-making mechanism, (bb) at the request of the data subject, review the outcome of the decision using human assistance; and (c) it is made using non-specific data, unless otherwise provided by law or by a binding act of the European Union. 14-17. sections: § 14. * The data subject is entitled to, in respect of his or her personal data processed by the data controller and the data processor acting on his or her behalf or on his or her

a) az nem sérti az egyenlő bánásmód követelményét, b) az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó az ba) érintettet - kérelmére - tájékoztatja a döntéshozatali mechanizmus során alkalmazott módszerről és szempontokról, bb) érintett kérelmére a döntés eredményét emberi közreműködés alkalmazásával felülvizsgálja, valamint c) arra - törvény vagy az Európai Unió kötelező jogi aktusának eltérő rendelkezése hiányában - nem különleges adatok felhasználásával kerül sor. 14-17. szakaszok: 14. § * Az érintett jogosult arra, hogy az adatkezelő és az annak megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatai vonatkozásában az e törvényben meghatározott feltételek szerint * a) az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon (a továbbiakban: előzetes tájékoztatáshoz való jog), b) kérelmére személyes adatait és az azok kezelésével összefüggő információkat az adatkezelő a rendelkezésére bocsássa (a továbbiakban: hozzáféréshez való jog), c) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő helyesbítse, illetve kiegészítse (a továbbiakban: helyesbítéshez való jog), d) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatai kezelését az adatkezelő korlátozza (a	behalf, in accordance with the conditions specified in this Act * (a) be informed of the facts relating to the processing prior to the commencement of the processing (hereinafter referred to as the right to prior information); (b) upon request, provide the controller with personal data and information related to their processing (hereinafter: right of access); (c) at his request and in the other cases provided for in this Chapter, his personal data be corrected or supplemented by the controller (hereinafter: the right to rectification), (d) at his request and in the other cases provided for in this Chapter, the processing of his personal data is restricted by the controller (hereinafter: the right to restrict the processing), (e) at the request of the controller and in the other cases provided for in this Chapter, delete his or her personal data (hereinafter referred to as the right to delete). § 15. * (1) In order to facilitate the exercise of the rights of the data subject, the data controller shall take appropriate technical and organizational measures, in particular: (a) comply with any notice and information to be provided to the data subject in the cases specified in this Act in an easily accessible and legible form, with concise, clear and comprehensible content, and (b) examine the application submitted by the data subject for the exercise of his rights as soon as possible after its submission, but not later than twenty-five days, and notify the data subject of his decision in writing or, if the application has been submitted by electronic means, by electronic means.

továbbiakban: az adatkezelés korlátozásához való jog), e) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő törölje (a továbbiakban: törléshez való jog). 15. § * (1) Az adatkezelő az érintett jogai érvényesülésének elősegítése érdekében megfelelő műszaki és szervezési intézkedéseket tesz, így különösen a) az érintett részére az e törvényben meghatározott esetekben nyújtandó bármely értesítést és tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal teljesíti, és b) az érintett által benyújtott, az őt megillető jogosultságok érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb idő alatt, de legfeljebb huszonöt napon belül elbírálja és döntéséről az érintettet írásban vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti. (2) Az adatkezelő a 14. §-ban meghatározott jogok érvényesülésével kapcsolatban az e törvényben meghatározott feladatait - a (3) bekezdésben meghatározott kivétellel - ingyenesen látja el. (3) Ha az érintett a) a folyó évben, azonos adatkörre vonatkozóan a 14. § b)-e) pontjaiban meghatározott jogai érvényesítése iránt ismételt kérelmet nyújt be, és b) e kérelme alapján az adatkezelő vagy az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatainak helyesbítését, törlését vagy az adatkezelés korlátozását az adatkezelő	(2) The data controller shall perform the tasks specified in this Act in connection with the enforcement of the rights specified in Section 14, with the exception specified in paragraph (3), free of charge. (3) If the person concerned a) in the current year, re-applies for the exercise of the rights specified in Section 14 b) -e) for the same data set, and (b) the controller lawfully waives the rectification, erasure or restriction of the processing of personal data processed by the controller or by a processor acting on its behalf or at its request, on the basis of this request, the controller may claim from the data subject the costs directly incurred in connection with the repeated and unjustified exercise of the data subject's rights under points (a) and (b). (4) If it can be reasonably assumed that the person submitting the application for the enforcement of the rights specified in Section 14 b) -e) is not the same as the data subject, the data controller shall execute the request after a credible proof of the identity of the person submitting it. § 16. * (1) In order to exercise the right to prior information, the data controller shall make it available to the data subject immediately before the commencement of data processing operations performed by him or her or on his or her behalf or at the latest after the commencement of the first data processing operation. (a) the name and contact details of the controller and, if a processing operation is carried out by a processor, the processor,

jogszerűen mellőzi, az adatkezelő az érintett jogainak az a) és b) pontban foglaltak szerinti ismételt és megalapozatlan érvényesítésével összefüggésben közvetlenül felmerült költségeinek megtérítését követelheti az érintettől. (4) Ha megalapozottan feltehető, hogy a 14. § b)-e) pontjában meghatározott jogok érvényesítése iránt kérelmet benyújtó személy az érintettel nem azonos személy, az adatkezelő a kérelmet az azt benyújtó személy személyazonosságának hitelt érdemlő igazolását követően teljesíti. 16. § * (1) Az előzetes tájékozódáshoz való jog érvényesülése érdekében az adatkezelő az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek megkezdését megelőzően vagy legkésőbb az első adatkezelési művelet megkezdését követően haladéktalanul az érintett rendelkezésére bocsátja a) az adatkezelő és - ha valamely adatkezelési műveletet adatfeldolgozó végez, az adatfeldolgozó - megnevezését és elérhetőségeit, b) az adatvédelmi tisztviselő nevét és elérhetőségeit, c) a tervezett adatkezelés célját és d) az érintettet e törvény alapján megillető jogok, valamint azok érvényesítése módjának ismertetését. (2) Az (1) bekezdésben foglaltakkal egyidejűleg, azzal azonos módon vagy az érintettnak címzetten az adatkezelő az érintett számára tájékoztatást nyújt	(b) the name and contact details of the Data Protection Officer, (c) the purpose of the intended processing; and d) a description of the rights of the data subject under this Act and the manner of exercising them. 2. Simultaneously with, in the same way as or addressed to the data subject, the controller shall provide the data subject with information a) the legal basis of the data processing, b) the period of retention of the processed personal data, the criteria for determining this period, (c) in the case of transfers or planned transfers of personal data processed, the recipients of the transfers, including third country recipients and international organizations; (d) the source of the collection of the personal data processed; and (e) any other relevant facts relating to the circumstances of the processing. 3. The controller may delay the execution of the information referred to in paragraph 2 in proportion to the aim pursued, limit the content of the information or refrain from providing the information if such action is strictly necessary. (a) the efficient and effective conduct of investigations or proceedings conducted by him or with his participation, in particular criminal proceedings, (b) the effective and efficient prevention and detection of criminal offenses,

a) az adatkezelés jogalapjáról, b) a kezelt személyes adatok megőrzésének időtartamáról, ezen időtartam meghatározásának szempontjairól, c) a kezelt személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek - ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket - köréről, d) a kezelt személyes adatok gyűjtésének forrásáról és e) az adatkezelés körülményeivel összefüggő minden további érdemi tényről. (3) A (2) bekezdésben foglaltak szerinti tájékoztatás teljesítését az elérni kívánt céllal arányosan az adatkezelő késleltetheti, a tájékoztatás tartalmát korlátozhatja vagy a tájékoztatást mellőzheti, ha ezen intézkedése elengedhetetlenül szükséges a) az általa vagy részvételével végzett vizsgálatok vagy eljárások - így különösen a büntetőeljárás - hatékony és eredményes lefolytatásának, b) a bűncselekmények hatékony és eredményes megelőzésének és felderítésének, c) a bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtásának, d) a közbiztonság hatékony és eredményes védelmének, e) az állam külső és belső biztonsága hatékony és eredményes védelmének, így különösen a honvédelem és a nemzetbiztonság vagy f) harmadik személyek alapvető jogai védelmének biztosításához.	(c) the enforcement of penalties and measures against perpetrators of criminal offenses, d) the effective and efficient protection of public security, (e) the effective and efficient protection of the external and internal security of the State, in particular national defense and national security; or (f) to ensure the protection of the fundamental rights of third parties. § 17. * (1) In order to enforce the right of access, the data controller shall, at the request of the data subject, inform whether his or her personal data are handled by the data controller himself or herself or by a data processor acting on his or her behalf or on his or her behalf. 2. Where the personal data of the data subject are processed by the controller or by a processor acting on his behalf or at his disposal, the controller shall make the personal data processed by him and by the processor acting on his behalf or at his disposal available to the data subject in addition to paragraph 1, and informs him a) the source of the personal data processed, b) the purpose and legal basis of the data processing, c) the scope of the personal data processed, (d) in the case of transfers of processed personal data, the recipients of the transfers, including third country recipients and international organizations; e) the period of retention of the personal data processed, the criteria for determining this period,

17. § * (1) A hozzáféréshez való jog érvényesülése érdekében az érintettet kérelmére az adatkezelő tájékoztatja arról, hogy személyes adatait maga az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó kezeli-e. (2) Ha az érintett személyes adatait az adatkezelő vagy a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó kezeli, az adatkezelő az (1) bekezdésben meghatározottakon túl az érintett rendelkezésére bocsátja az érintett általa és a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatait, és közli vele a) a kezelt személyes adatok forrását, b) az adatkezelés célját és jogalapját, c) a kezelt személyes adatok körét, d) a kezelt személyes adatok továbbítása esetén az adattovábbítás címzettjeinek - ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket - körét, e) a kezelt személyes adatok megőrzésének időtartamát, ezen időtartam meghatározásának szempontjait, f) az érintettet e törvény alapján megillető jogok, valamint azok érvényesítése módjának ismertetését, g) profilalkotás alkalmazásának esetén annak tényét és h) az érintett személyes adatainak kezelésével összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és az azok kezelésére tett intézkedéseket. (3) Az érintett hozzáféréshez való jogának érvényesítését az adatkezelő az elérni kívánt	f) a description of the rights of the data subject under this Act and the manner of exercising them, (g) if profiling is used, the fact of it; and (h) the circumstances of the occurrence of data protection incidents related to the processing of the personal data of the data subject, their effects and the measures taken to deal with them. (3) The data controller may restrict or refuse to exercise the right of access of the data subject in proportion to the purpose to be achieved, if this measure is strictly necessary to ensure one of the interests specified in Section 16 (3) a) -f). 4. If a measure pursuant to paragraph 3 is applied, the controller shall immediately inform the data subject in writing. a) the fact of restricting or refusing access, as well as the legal and factual reasons, if making them available to the data subject does not jeopardize the exercise of any of the interests specified in Section 16 (3) a) -f), and (b) the rights of the data subject under this Act and the manner in which they are to be exercised, in particular whether the data subject may exercise his or her right of access with the assistance of the Authority. 21-22. sections: § 21. * (1) If the data subject rejects the data subject's request for the rectification, erasure or restriction of the processing of personal data processed by the data controller or a data processor acting on his or her behalf or on his or her behalf, he or she shall inform the data subject in writing without delay.

céllal arányosan korlátozhatja vagy megtagadhatja, ha ezen intézkedés elengedhetetlenül szükséges a 16. § (3) bekezdés a)-f) pontjában meghatározott valamely érdek biztosításához. (4) A (3) bekezdésben foglaltak szerinti intézkedés alkalmazása esetén az adatkezelő írásban, haladéktalanul tájékoztatja az érintettet a) a hozzáférés korlátozásának vagy megtagadásának tényéről, továbbá jogi és ténybeli indokairól, ha ezeknek az érintett rendelkezésére bocsátása a 16. § (3) bekezdés a)-f) pontjában meghatározott valamely érdek érvényesülését nem veszélyezteti, valamint b) az érintettet e törvény alapján megillető jogokról, valamint azok érvényesítésének módjáról, így különösen arról, hogy az érintett a hozzáféréshez való jogát a Hatóság közreműködésével is gyakorolhatja. 21-22. szakaszok: 21. § * (1) Ha az érintett kérelmét az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatok helyesbítésére, törlésére vagy ezen adatok kezelésének korlátozására az adatkezelő elutasítja, az érintettet írásban, haladéktalanul tájékoztatja a) az elutasítás tényéről, annak jogi és ténybeli indokairól, valamint b) az érintettet e törvény alapján megillető jogokról, valamint azok érvényesítésének módjáról, így különösen arról, hogy az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatok helyesbítésére, törlésére vagy ezen adatok kezelésének korlátozására vonatkozó jogát a Hatóság közreműködésével is gyakorolhatja.	(a) the fact of the refusal, the legal and factual grounds for it; and (b) the data subject's rights under this Act and the manner in which they are enforced, in particular the right to rectify, erase or restrict the processing of personal data processed by the controller or the processor acting on his behalf or at his disposal, with the assistance of the Authority. . (2) The data controller may delay the fulfillment of the information pursuant to subsection (1) a) in proportion to the intended purpose, limit the content of the information or omit the information if this measure is absolutely necessary in accordance with Section 16 (3) (a) -f). 3. If the controller rectifies, deletes or restricts the processing of personal data processed by him or by a processor acting on his behalf or at his disposal, the controller shall notify the controllers and processors to whom the data are subject to this measure of the fact and content of this measure. in order for them to carry out the rectification, erasure or restriction on the processing of the data in respect of their own data processing. § 22. * In order to enforce his rights, the data subject shall As defined in Chapter a) the Authority may initiate an investigation in order to examine the lawfulness of the data controller's action if the data controller restricts the exercise of the rights specified in Section 14 or rejects its request for the enforcement of these rights, and (b) the Authority may request that data protection authority proceedings be instituted if it considers that the controller or the processor acting on its behalf or acting on its behalf infringes the rules on the processing of

(2) Az (1) bekezdés a) pontjában foglaltak szerinti tájékoztatás teljesítését az adatkezelő az elérni kívánt céllal arányosan késleltetheti, a tájékoztatás tartalmát korlátozhatja vagy a tájékoztatást mellőzheti, ha ezen intézkedése elengedhetetlenül szükséges a 16. § (3) bekezdés a)-f) pontjában meghatározott valamely érdek biztosításához. (3) Ha az adatkezelő az általa, illetve a megbízásából vagy rendelkezése szerint eljáró adatfeldolgozó által kezelt személyes adatokat helyesbíti, törli vagy ezen adatok kezelését korlátozza, az adatkezelő ezen intézkedés tényéről és annak tartalmáról értesíti azon adatkezelőket és adatfeldolgozókat, amelyek részére az adatot ezen intézkedését megelőzően továbbította, annak érdekében, hogy azok a helyesbítést, törlést vagy az adatok kezelésének korlátozását a saját adatkezelésük tekintetében végrehajtsák. 22. § * Jogainak érvényesítése érdekében az érintett a VI. Fejezetben meghatározottak szerint a) a Hatóság vizsgálatát kezdeményezheti az adatkezelő intézkedése jogszerűségének vizsgálata céljából, ha az adatkezelő a 14. §-ban meghatározott jogainak érvényesítését korlátozza vagy ezen jogainak érvényesítésére irányuló kérelmét elutasítja, valamint b) a Hatóság adatvédelmi hatósági eljárásának lefolytatását kérelmezheti, ha megítélése szerint személyes adatainak kezelése során az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó megsérti a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírásokat.	personal data laid down by law or a binding act of the European Union. Section 27: § 27. (1) Public data in the public interest or in the public interest shall not be disclosed if it is classified data in accordance with the Classified Data Protection Act. (2) The right to access public data in the public interest and in the public interest - by defining the types of data - (a) in the interests of national defense; (b) in the interests of national security; (c) for the purpose of prosecuting or preventing criminal offenses; (d) in the interests of the environment or nature; (e) for central financial or foreign exchange policy purposes; (f) foreign relations, with regard to relations with international organizations; (g) in the context of judicial or administrative proceedings; (h) with regard to intellectual property rights you can limit. (3) * In the public interest, the use of the central and local government budget or European Union support, budget-related benefits, discounts, management, possession, use, utilization and disposal of state and municipal property shall not be considered a business secret. information relating to its encumbrance, the acquisition of any right affecting such property, and information the

27. szakasz: 27. § (1) A közérdekű vagy közérdekből nyilvános adat nem ismerhető meg, ha az a minősített adat védelméről szóló törvény szerinti minősített adat. (2) A közérdekű és közérdekből nyilvános adatok megismeréséhez való jogot - az adatfajták meghatározásával - törvény a) honvédelmi érdekből; b) nemzetbiztonsági érdekből; c) bűncselekmények üldözése vagy megelőzése érdekében; d) környezet- vagy természetvédelmi érdekből; e) központi pénzügyi vagy devizapolitikai érdekből; f) külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra tekintettel; g) bírósági vagy közigazgatási hatósági eljárásra tekintettel; h) a szellemi tulajdonhoz fűződő jogra tekintettel korlátozhatja. (3) * Közérdekből nyilvános adatként nem minősül üzleti titoknak a központi és a helyi önkormányzati költségvetés, illetve az európai uniós támogatás felhasználásával, költségvetést érintő juttatással, kedvezményrel, az állami és önkormányzati vagyon kezelésével, birtoklásával, használatával, hasznosításával, az azzal való rendelkezéssel, annak megterhelésével, az ilyen vagyont érintő bármilyen jog megszerzésével kapcsolatos adat, valamint az az adat, amelynek megismerését vagy nyilvánosságra hozatalát külön törvény közérdekből elrendeli. A nyilvánosságra hozatal azonban nem eredményezheti az olyan adatokhoz - így	disclosure or disclosure of which is required by a separate law in the public interest. However, disclosure shall not give rise to access to data, in particular proprietary knowledge, the disclosure of which would be disproportionately prejudicial to the conduct of business, provided that this does not prevent access to public data in the public interest. 3a. * A natural or legal person, or an entity without legal personality, which establishes a financial or business relationship with a person belonging to a public finance subsystem shall be required to provide public information relating to that relationship and in the public interest pursuant to paragraph 3. provide information to anyone on request. The obligation to provide information may also be fulfilled by publishing public data in the public interest or by indicating a public source containing data previously published in electronic form. 3b. * If the information subject pursuant to paragraph 3a refuses the information, the body requesting the information may initiate proceedings against the body entitled to exercise legal supervision over the information subject. 4. Access to data of public interest may be restricted on the basis of a Union act in view of the significant financial or economic policy interests of the European Union, including monetary, budgetary and tax policy interests. (5) Data prepared or recorded in the course of the procedure for making a decision falling within the tasks and competence of a body performing public tasks, which is the basis for the decision, shall not be public for ten years

különösen a védett ismerethez - való hozzáférést, amelyek megismerése az üzleti tevékenység végzése szempontjából aránytalan sérelmet okozna, feltéve hogy ez nem akadályozza meg a közérdekből nyilvános adat megismerésének lehetőségét. (3a) * Az a természetes személy, jogi személy vagy jogi személyiséggel nem rendelkező szervezet, aki vagy amely az államháztartás alrendszerébe tartozó valamely személlyel pénzügyi vagy üzleti kapcsolatot létesít, köteles e jogviszonnyal összefüggő és a (3) bekezdés alapján közérdekből nyilvános adatra vonatkozóan - erre irányuló igény esetén - bárki számára tájékoztatást adni. A tájékoztatási kötelezettség a közérdekből nyilvános adatok nyilvánosságra hozatalával vagy a korábban már elektronikus formában nyilvánosságra hozott adatot tartalmazó nyilvános forrás megjelölésével is teljesíthető. (3b) * Ha a (3a) bekezdés alapján tájékoztatásra kötelezett a tájékoztatást megtagadja, a tájékoztatást igénylő a tájékoztatásra kötelezett felett törvényességi felügyelet gyakorlására jogosult szerv eljárását kezdeményezheti. (4) A közérdekű adatok megismerése korlátozható uniós jogi aktus alapján az Európai Unió jelentős pénzügy- vagy gazdaságpolitikai érdekére tekintettel, beleértve a monetáris, a költségvetési és az adópolitikai érdeket is. (5) A közfeladatot ellátó szerv feladat- és hatáskörébe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített, a döntés megalapozását szolgáló adat a keletkezésétől számított tíz évig nem nyilvános. Ezen adatok megismerését - az adat	from the time of its occurrence. Access to this data may be authorized by the head of the body managing the data, taking into account the weight of the public interest in accessing the data and excluding it. (6) * The request for access to the data on which the decision is based may be rejected after the decision has been made within the period specified in subsection (5) if the data also serves as a basis for further decision or the lawful operation of the public authority. would jeopardize the order or performance of its tasks and powers free from unauthorized external influences, in particular the free expression of the position of the originator in the preparation of decisions. (7) Legislation may set a shorter period than specified in subsection (5) in order to limit the disclosure of certain data used to substantiate the decision. (8) The provisions of this Chapter shall not apply to the provision of data from the public credit register, which is regulated by a separate law. Section 60: § 60 * (1) In order to enforce the right to the protection of personal data, the Authority shall initiate data protection authority proceedings at the request of the data subject and may initiate data protection authority proceedings ex officio. (2) An application for the initiation of a data protection official procedure may be submitted in the case specified in Article 77 (1) and

megismeréséhez és a megismerhetőség kizárásához fűződő közérdek súlyának mérlegelésével - az azt kezelő szerv vezetője engedélyezheti. (6) * A döntés megalapozását szolgáló adat megismerésére irányuló igény - az (5) bekezdésben meghatározott időtartamon belül - a döntés meghozatalát követően akkor utasítható el, ha az adat további jövőbeli döntés megalapozását is szolgálja, vagy az adat megismerése a közfeladatot ellátó szerv törvényes működési rendjét vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását, így különösen az adatot keletkeztető álláspontjának a döntések előkészítése során történő szabad kifejtését veszélyeztetné. (7) Jogszabály a döntés megalapozását szolgáló egyes adatok megismerhetőségének korlátozására az (5) bekezdésben meghatározottnál rövidebb időtartamot állapíthat meg. (8) E fejezet rendelkezései nem alkalmazhatók a közhitelű nyilvántartásból történő - külön törvényben szabályozott - adatszolgáltatásra. 60. szakasz: 60. § * (1) A személyes adatok védelméhez való jog érvényesülése érdekében a Hatóság az érintett erre irányuló kérelmére adatvédelmi hatósági eljárást indít és hivatalból adatvédelmi hatósági eljárást indíthat. (2) Az adatvédelmi hatósági eljárás megindítása iránti kérelem az általános adatvédelmi rendelet 77. cikk (1)	Section 22 (b) of the General Data Protection Regulation. The Authority shall initiate ex officio data protection authority proceedings if: a) establishes on the basis of its investigation that an infringement has occurred or is in imminent danger in connection with the processing of personal data, and no remedy has been remedied or an imminent threat has been eliminated within the time limit set by the Authority, (b) on the basis of its investigation, finds that there has been or is an imminent threat of an infringement of the processing of personal data and that a fine is appropriate under the provisions of the General Data Protection Regulation. (4) If the data protection authority procedure was preceded by an investigation of the Authority based on a notification, the notifier shall be notified by the Authority of the initiation or termination of the data protection authority procedure. (5) In the case specified in subsection (2), the application shall contain, in addition to those specified in the General Administrative Procedure Act: (a) an indication of the alleged infringement, (b) a description of the specific conduct or situation which led to the alleged infringement, (c) the data available to the applicant to identify the controller or processor committing the alleged infringement, (d) the facts and evidence supporting the allegations of an alleged infringement; and (e) a firm request for a decision to remedy the alleged infringement.

bekezdésében, valamint a 22. § b) pontjában meghatározott esetben nyújtható be. (3) A Hatóság hivatalból adatvédelmi hatósági eljárást indít, ha a) vizsgálata alapján megállapítja, hogy a személyes adatok kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye áll fenn, és az 56. § szerinti felszólítás vagy ajánlás alapján a jogsérelem orvoslására, illetve a jogsérelem közvetlen veszélyének megszüntetésére a Hatóság által meghatározott határidőben nem került sor, b) vizsgálata alapján megállapítja, hogy a személyes adatok kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye áll fenn és az általános adatvédelmi rendelet rendelkezései alapján bírság kiszabásának van helye. (4) Ha az adatvédelmi hatósági eljárást a Hatóság bejelentésen alapuló vizsgálata előzte meg, a bejelentőt az adatvédelmi hatósági eljárás megindításáról, illetve befejezéséről a Hatóság értesíti. (5) A (2) bekezdésben meghatározott esetben a kérelem az általános közigazgatási rendtartásról szóló törvényben meghatározottakon túl tartalmazza a) a feltételezett jogsértés megjelölését, b) a feltételezett jogsértést megvalósító konkrét magatartás vagy állapot leírását, c) a feltételezett jogsértést megvalósító adatkezelő, illetve adatfeldolgozó azonosításához szükséges, a kérelmező rendelkezésére álló adatokat,	6. In proceedings before the data protection authority, the applicant shall be entitled to legal aid; the Authority shall advance the costs of the proceedings, the advance payment of which would be borne by the applicant. Section 64: § 64. (1) If the data controller does not comply with the request contained in § 56 (1), the Authority shall, due to a breach of public interest data and public data in the public interest, within thirty days, request the court to order the controller to act as requested by the Authority. (2) * Section 31 (5) shall apply to determine the jurisdiction and jurisdiction of the court. (3) The data controller shall prove that the data processing complies with the provisions of law. (4) A party who does not otherwise have legal capacity to sue may also be a party to a lawsuit. (5) Upon request, the court may order the publication of its judgment - by publishing the identification data of the data controller - if required by the protection of data protection or the interests of freedom of information and the rights of a larger number of data subjects protected by this Act.

d) a feltételezett jogsértéssel kapcsolatos állításokat alátámasztó tényeket és azok bizonyítékait, továbbá e) a megjelölt jogsértés orvoslása iránti döntésre vonatkozó határozott kérelmet. (6) Az adatvédelmi hatósági eljárásban a kérelmezőt költségmentesség illeti meg, a Hatóság előlegezi az olyan eljárási költséget, amelynek előlegezése a kérelmezőt terhelné. 64. szakasz: 64. § (1) Ha az adatkezelő az 56. § (1) bekezdésében foglalt felszólításnak nem tesz eleget, a közérdekű adatok és a közérdekből nyilvános adatokkal kapcsolatos jogsértés miatt a Hatóság az 56. § (2) bekezdése szerinti tájékoztatásra vonatkozó határidő lejártát követő harminc napon belül keresettel kérheti a bíróságtól az adatkezelőnek a Hatóság felszólítása szerinti magatartásra való kötelezését. (2) * A bíróság hatáskörének és illetékességének megállapítására a 31. § (5) bekezdését kell alkalmazni. (3) Azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az adatkezelő köteles bizonyítani. (4) A perben fél lehet az is, akinek egyébként nincs perbeli jogképessége. (5) A bíróság kérelemre elrendelheti ítéletének - az adatkezelő azonosító adatainak közzétételével történő - nyilvánosságra hozatalát, ha azt az adatvédelem, illetve az	

információszabadság érdekeinek és nagyobb számú érintett e törvényben védett jogainak védelme megköveteli.	
2012. évi C. törvény a Büntető Törvénykönyvről 219-220. szakaszok: 219. § (1) * Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy b) az adatok biztonságát szolgáló intézkedést elmulasztja, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő. (2) * Az (1) bekezdés szerint büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével az érintett hozzáféréshez való jogának gyakorlása érdekében szükséges tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti. (3) * A büntetés két évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges adatra vagy bűnügyi személyes adatra követik el. (4) A büntetés büntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatus felhasználásával követik el.	Act C of 2012 on the Criminal Code 219-220. sections: § 219. (1) * Who, in violation of the provisions specified in the law on the protection or processing of personal data or in a binding legal act of the European Union, for the purpose of gaining profit or causing significant damage to interests (a) processes personal data without authorization or for any other purpose, or b) fails to take a data security measure, punishable by imprisonment for a term not exceeding one year. (2) * A person who fails to comply with his or her obligation to provide information in order to exercise the right of access of the data subject in breach of the provisions of the law on the protection or processing of personal data or a binding act of the European Union shall also be penalized in accordance with paragraph 1. significantly harms the interests of others or others. (3) * The penalty is imprisonment for up to two years if the misuse of personal data is committed on special data or criminal personal data. (4) The punishment shall be imprisonment for a term not exceeding three years if the misuse of personal data is committed as an official person or using a public mandate.

220. § (1) Aki a közérdekű adatok nyilvánosságáról szóló törvényi rendelkezések megszegésével a) közérdekű adatot az adatigénylő elől eltitkol, vagy azt követően, hogy a bíróság jogerősen a közérdekű adat közzétételére kötelezte, tájékoztatási kötelezettségének nem tesz eleget, b) közérdekű adatot hozzáférhetetlenné tesz vagy megsemmisít, illetve c) hamis vagy hamisított közérdekű adatot hozzáférhetővé vagy közzé tesz, vétség miatt két évig terjedő szabadságvesztéssel büntetendő. (2) A büntetés büntett miatt három évig terjedő szabadságvesztés, ha a közérdekű adattal visszaélést jogtalan hasznoszerzés végett követik el.	§ 220. (1) Who violates the legal provisions on the disclosure of data of public interest (a) withholds data of public interest from the person requesting the data or fails to comply with his or her obligation to provide information after the court has legally ordered the disclosure of data of public interest, (b) make information of public interest inaccessible or falsify it; or (c) make false or falsified information of public interest available or publish it, punishable by imprisonment for a term not exceeding two years. (2) The punishment shall be imprisonment for a term not exceeding three years if the misuse of public interest data is committed for the purpose of unlawful gain.
2013. évi V. törvény a Polgári Törvénykönyvről 2:43. szakasz: 2:43. § [Nevesített személyiségi jogok] A személyiségi jogok sérelmét jelenti különösen a) az élet, a testi épség és az egészség megsértése; b) a személyes szabadság, a magánélet, a magánlakás megsértése; c) a személy hátrányos megkülönböztetése; d) a becsület és a jóhírnév megsértése; e) a magántitokhoz és a személyes adatok védelméhez való jog megsértése; f) a névviseléshez való jog megsértése;	Act V of 2013 on the Civil Code 2:43. platoon: 2:43. § [Named rights of personality] It is a violation of individual rights in particular (a) infringements of life, limb and health; b) violation of personal liberty, privacy, private home; (c) discrimination against any person; (d) breach of honor and reputation; (e) violation of the right to privacy and the protection of personal data; (f) infringement of the right to a name; (g) infringement of the right to images and phonograms.

g) a képmáshoz és a hangfelvételhez való jog megsértése. 2:52-54. szakaszok: 2:52. § [Sérelemdíj] (1) Akit személyiségi jogában megsértenek, sérelemdíjat követelhet az őt ért nem vagyoni sérelemért. (2) A sérelemdíj fizetésére kötelezés feltételeire - különösen a sérelemdíjra köteles személy meghatározására és a kimentés módjára - a kártérítési felelősség szabályait kell alkalmazni, azzal, hogy a sérelemdíjra való jogosultsághoz a jogsértés tényén kívül további hátrány bekövetkeztének bizonyítása nem szükséges. (3) A sérelemdíj mértékét a bíróság az eset körülményeire - különösen a jogsértés súlyára, ismétlődő jellegére, a felróhatóság mértékére, a jogsértésnek a sértettre és környezetére gyakorolt hatására - tekintettel, egy összegben határozza meg. 2:53. § [Kártérítési felelősség] Aki személyiségi jogainak megsértéséből eredően kárt szenved, a jogellenesen okozott károkért való felelősség szabályai szerint követelheti a jogsértőtől kárának megtérítését. 2:54. § [A személyiségi jogok érvényesítése] (1) A személyiségi jogokat személyesen lehet érvényesíteni.	2: 52-54. sections: 2:52. § [Damage fee] 1. A person who is violated in his or her right to privacy may claim damages for non-pecuniary damage suffered by him or her. (2) The conditions for the obligation to pay damages, in particular the determination of the person liable for damages and the method of rescission, shall be subject to the rules on liability for damages, provided that proof of the occurrence of damage other than the infringement is not required. (3) The amount of the damages shall be determined by the court in a single amount, taking into account the circumstances of the case, in particular the gravity of the infringement, its repetitive nature, the degree of imputability, the impact of the infringement on the victim and its environment. 2:53. § [Liability for damages] Anyone who suffers damage as a result of a violation of his or her privacy rights may claim damages from the infringer in accordance with the rules of liability for unlawful damage. 2:54. § [Enforcement of privacy rights] (1) The rights of the individual may be exercised in person. (2) A minor with limited legal capacity and a person with partial legal capacity may act independently in the protection of his or her personal rights. A legal representative may act

(2) A korlátozottan cselekvőképes kiskorú és a cselekvőképességében részlegesen korlátozott személy a személyiségi jogai védelmében önállóan felléphet. A cselekvőképtelen személyiségi jogainak védelmében törvényes képviselője léphet fel. (3) Az ismeretlen helyen távollévő személyiségi jogának védelmében a hozzátartozója vagy gondnoka léphet fel. (4) Ha a személyiségi jog megsértése közérdekbe ütközik, a jogosult hozzájárulásával az ügyész keresetet indíthat, és érvényesítheti a jogsértés felróhatóságtól független szankcióit. Az ügyész keresete alapján a jogsértéssel elért vagyoni előnyt közérdekű célra kell átengedni. E bekezdést az (5) bekezdésben foglalt jogsértés esetén azzal az eltéréssel kell alkalmazni, hogy az ügyész a jogosult hozzájárulása nélkül is - az elévülési időn belül - keresetet indíthat. (5) A közösség bármely tagja jogosult a személyisége lényeges vonásának minősülő, a magyar nemzethez, illetve valamely nemzeti, etnikai, faji vagy vallási közösséghez tartozásával összefüggésben a közösséget nagy nyilvánosság előtt súlyosan sértő vagy kifejezőmódjában indokolatlanul bántó jogsérelem esetén a jogsértés megtörténtétől számított harmincnapos jogvesztő határidőn belül személyiségi jogát érvényesíteni. A közösség bármely tagja a jogsértéssel elért vagyoni előny átengedésének kivételével a személyiségi jogok megsértésének valamennyi szankcióját érvényesítheti. 5:14. szakasz (1): 5:14. § [A dolog]	to protect the personal rights of an incapacitated person. (3) A relative or guardian may intervene to protect the right to privacy in an unknown place. (4) If the violation of the right to privacy is in the public interest, the prosecutor may, with the consent of the right holder, bring an action and enforce sanctions for the violation, which are independent of the culpability. On the basis of the prosecutor's action, the property advantage obtained by the infringement must be transferred to a public interest purpose. This paragraph shall apply in the event of an infringement of paragraph 5, with the exception that the public prosecutor may bring an action within the limitation period without the consent of the right holder. (5) Any member of the community is entitled to a limitation period of thirty days from the occurrence of the violation in the event of a violation of the Hungarian nation or a national, ethnic, racial or religious community that is an essential feature of his personality. exercise his right to privacy within Any member of the community may enforce all sanctions for violation of the rights of the individual, except for the transfer of the property advantage obtained by the infringement. 5:14. Section (1): 5:14. § [The thing] (1) A physical object that can be taken possession of may be the subject of a right of ownership.

(1) A birtokba vehető testi tárgy tulajdonjog tárgya lehet.	
2016. évi CXXX. törvény a polgári perrendtartásról	Act CXXX of 2016 on the Civil procedure
2016. évi CL. törvény az általános közigazgatási rendtartásról	Act CL of 2016 on General Administrative Order
116. szakasz:	Section 116:
116. § [A fellebbezés általános szabályai]	§ 116 [General rules of appeal]
(1) Az ügyfél, vagy akire a döntés rendelkezést tartalmaz, az elsőfokú döntés ellen akkor fellebbezhet, ha azt törvény kifejezetten megengedi.	(1) The client, or to whom the decision contains a provision, may appeal against the decision of the first instance if this is expressly permitted by law.
(2) Fellebbezésnek van helye, ha a határozatot	(2) An appeal shall lie from the decision
a) * - a képviselő testület kivételével - helyi önkormányzat szerve, vagy	(a) * a body of local government other than a representative body, or
b) rendvédelmi szerv helyi szerve hozta.	(b) a local body of law enforcement brought.
(3) * Abban az ügyben, amelyben a határozat az (1) vagy (2) bekezdés alapján fellebbezéssel támadható, az önálló jogorvoslattal támadható végzés ellen fellebbezésnek van helye.	(3) * In a case where the decision may be appealed against under paragraph (1) or (2), an appeal may be lodged against the order which may be challenged on a stand-alone basis.
(4) Az (1) és (2) bekezdésben foglalt esetekben sincs helye fellebbezésnek	4. In the cases referred to in paragraphs 1 and 2, no appeal shall lie
a) ha az elsőfokú döntést - a központi hivatal kivételével - központi államigazgatási szerv vezetője hozta,	(a) if the decision at first instance was taken by the head of a central public administration body other than the central office,
b) ha a képviselő-testület önkormányzati hatósági ügyben hozott döntést,	b) if the representative body has made a decision in a municipal authority matter,
c) * a másodfokú hatóság által hozott önálló jogorvoslattal támadható végzés esetén,	c) * in the case of an order subject to an independent appeal by a second instance authority,
d) ha nincs kijelölt másodfokú hatóság,	

e) nemzetgazdasági szempontból kiemelt jelentőségűvé nyilvánított ügyben, f) ha a hatósági szerződés alapján végrehajtást rendeltek el. (5) * A (2) bekezdésben foglalt esetekben sincs helye fellebbezésnek, ha törvény a fellebbezést kizárja.	(d) in the absence of a designated second instance authority, e) in a matter declared to be of high importance from the point of view of national economy, (f) if enforcement has been ordered under an official contract. (5) * In the cases provided for in subsection (2), there is no place for an appeal if the appeal is excluded by law.
2017. évi I. törvény a közigazgatási perrendtartásról 115-119. szakaszok: 115. § [A felülvizsgálat alapja és eljárási szabályai] (1) * A jogerős ítélet, továbbá a keresetlevelet visszautasító vagy az eljárást megszüntető jogerős végzés ellen jogszabálysértésre, illetve a Kúria közzétett határozatától jogkérdésben való eltérésre hivatkozással felülvizsgálati kérelmet terjeszthet elő a fél, az érdekelt, valamint a rendelkezés rá vonatkozó része ellen az, akire a határozat rendelkezést tartalmaz. (2) A felülvizsgálatra a fellebbezésre vonatkozó szabályokat az e fejezetben foglalt eltérésekkel kell megfelelően alkalmazni. (3) * A Kúria közzétett határozatától jogkérdésben való eltéréssel összefüggésben jogegységi panasznak a bíróságok szervezetéről és igazgatásáról szóló törvényben foglaltak szerint van helye.	Act I of 2017 on the Code of Administrative Procedure 115-119. sections: Section 115 [Basis and Rules of Procedure for Review] (1) * An appeal against a final judgment or a final order rejecting an application or terminating proceedings may be brought against the party, the interested party and the part of the provision concerning him by reference to an infringement of the law or a deviation from the published decision of the Curia. the decision contains a provision. 2. The rules on appeal shall apply mutatis mutandis to the review, subject to the derogations provided for in this Chapter. (3) * In connection with the deviation from the published decision of the Curia in a matter of law, a complaint of legal unity shall be admissible in accordance with the provisions of the Act on the Organization and Administration of Courts.

116. § [A felülvizsgálatból kizárt határozatok] Nincs helye felülvizsgálatnak a) * az elsőfokon jogerőre emelkedett határozat ellen, kivéve, ha a fellebbezést törvény nem teszi lehetővé, vagy kizárja, b) * c) a jogerős határozatnak csupán a kamatfizetésre, a perköltségre, a teljesítési határidőre vagy a részletfizetésre vonatkozó rendelkezései ellen, d) a Kúria határozata ellen, e) ha azt törvény különösen indokolt esetben kizárja.	§ 116 [Decisions excluded from review] There is no room for review a) * against a decision which has become final at first instance, unless an appeal is not permitted or excluded by law, b) * (c) against the provisions of a final decision relating solely to the payment of interest, legal costs, time limits for payment or installments, d) against the decision of the Curia, e) if it is excluded by law in particularly justified cases.
117. § [Felülvizsgálati kérelem] (1) A felülvizsgálati kérelmet az elsőfokú határozatot hozó bíróságnál a jogerős határozat közlésétől számított harminc napon belül kell jogi képviselő útján benyújtani. A határidő elmulasztása miatt a határidő lejártát követő tizenöt napon belül van helye igazolásnak. (2) A felülvizsgálati kérelem visszautasításáról a Kúria tanácsban, indokolt végzésben határoz. (3) A felülvizsgálati kérelemben nem lehet hivatkozni új jogalapra és olyan új tényre, körülményre, amely nem volt sem az elsőfokú, sem a másodfokú eljárás tárgya. (4) * A felülvizsgálati kérelemben meg kell jelölni a kérelem befogadhatóságának okát,	§ 117. [Request for review] 1. An application for review shall be lodged with the court of first instance within 30 days of notification of the final decision. Failure to meet the deadline shall result in a certificate within fifteen days of the deadline. (2) The Curia shall decide on the rejection of the application for review by a reasoned order of the Council. (3) A request for review may not be based on a new plea in law or on a new fact or circumstance which was not the subject of the proceedings at first instance or second instance. (4) * The reason for the admissibility of the application shall be indicated in the application for review, however, its existence shall not be proved and justified, except for the reason

azonban annak fennállását bizonyítani és azt - a 118. § (1) bekezdés a) pont ad) alpontja szerinti ok kivételével - indokolni nem kell. A 118. § (1) bekezdés b) pontja szerinti ok esetében meg kell jelölni azt a közzétett kúriai határozatot és annak azt a részét, amelytől a felülvizsgálni kért határozat jogkérdésben eltér. A fél által megjelölt befogadhatósági okhoz a bíróság nincs kötve. (5) * A (4) bekezdésben foglaltak tekintetében hiánypótlásnak nincs helye. 118. § [Döntés a felülvizsgálati kérelem befogadhatóságáról] (1) * A Kúria a felülvizsgálati kérelmet akkor fogadja be, ha a) az ügy érdemére kiható jogszabálysértés vizsgálata aa) a joggyakorlat egységének vagy továbbfejlesztésének biztosítása, ab) a felvetett jogkérdés különleges súlya, illetve társadalmi jelentősége, ac) az Európai Unió Bírósága előzetes döntéshozatali eljárásának szükségessége, ad) a kérelmező alapvető eljárási jogának valószínűsíthető sérelme, vagy az ügy érdemére kiható egyéb eljárási szabályszegés, illetve b) a Kúria közzétett határozatától jogkérdésben való eltérés miatt indokolt. (2) A felülvizsgálati kérelem befogadásáról vagy a befogadás megtagadásáról a Kúria háromtagú tanácsban, tárgyaláson kívül, a felterjesztéstől számított harminc napon belül	pursuant to Section 118 (1) (a) (d). In the case of a reason pursuant to Section 118 (1) (b), the published curative decision and the part of it from which the decision requested to be reviewed differs in legal matters shall be indicated. The court is not bound by the admissibility reason given by the party. (5) * There is no need to fill in the gaps with regard to the provisions of paragraph (4). § 118. [Decision on the admissibility of the application for review] (1) * The Curia will accept the request for review if (a) the investigation of an infringement affecting the substance of the case (aa) ensuring the unity or development of case law, (ab) the special weight or social significance of the legal issue raised, (ac) the need for a preliminary ruling procedure before the Court of Justice of the European Union, (ad) a possible breach of the applicant's fundamental procedural rights or any other breach of procedure affecting the merits of the case; or b) a deviation in law from the published decision of the Curia justified. (2) The Curia shall decide on the admission or refusal of admission to the review in a tripartite council, outside the hearing, within thirty days from the submission. Reasons shall

határoz. A felülvizsgálati kérelem befogadását megtagadó végzést indokolni kell. (3) A befogadhatóság tárgyában hozott végzést a Kúria közli a felülvizsgálati kérelmet előterjesztő féllel. (4) A felülvizsgálati kérelem befogadásáról szóló végzést - a felülvizsgálati kérelem egyidejű megküldésével - közölni kell a kérelmet előterjesztő fél ellenfelével és az érdekelttel, akik annak közlésétől számított nyolc napon belül, abban a körben, amelyre nézve a kérelmet befogadták, felülvizsgálati ellenkérelmet vagy csatlakozó felülvizsgálati kérelmet terjeszthetnek elő. 119. § [A felülvizsgálati kérelem hatálya] (1) A felülvizsgálati kérelem benyújtásának a felülvizsgálni kért bírósági határozat és az annak alapjául szolgáló közigazgatási cselekmény hatályosulására nincs halasztó hatálya. (2) * A felülvizsgálati kérelemmel egyidejűleg azonnali jogvédelem iránti kérelem is előterjeszthető. Ha a felülvizsgálati kérelem azonnali jogvédelem iránti kérelmet tartalmaz, az elsőfokú bíróság haladéktalanul intézkedik az iratok Kúriára történő felterjesztéséről. A Kúria az azonnali jogvédelem iránti kérelemről legkésőbb a befogadás tárgyában hozott végzéssel egyidejűleg dönt. 121. szakasz: 121. § [Felülvizsgálati határozat]	be given for an order refusing to grant a request for review. 3. The admissibility order shall be communicated by the Curia to the party requesting the review. 4. The order accepting the request for review shall be notified, together with the request for review, to the opponent of the requesting party and to the interested party, who shall, within eight days of service thereof, they may submit an application. § 119 [Scope of the application for review] 1. The filing of an application for review shall not have suspensory effect on the entry into force of the judgment which is the subject of the review and of the administrative act on which it is based. (2) * An application for immediate legal protection may be filed at the same time as the application for review. If the application for review contains an application for immediate legal protection, the court of first instance shall immediately arrange for the documents to be served on the Mansion. The Curia decides on the application for immediate legal protection at the latest at the same time as the order on admission. Section 121: § 121 [Review decision]

(1) * Ha a felülvizsgálni kért határozat az ügy érdemére kiható módon jogszabálysértő, illetve a Kúria közzétett határozatától jogkérdésben eltér, a bíróság a jogerős határozatot a) egészben vagy részben hatályon kívül helyezi, és szükség esetén az ügyben eljáró bíróságot új eljárás lefolytatására és új határozat hozatalára utasítja, b) úgy változtatja meg, hogy a megtámadott közigazgatási cselekményt megsemmisíti, és a közigazgatási szervet új eljárás lefolytatására kötelezi. (2) * Ha a felülvizsgálni kért határozat a jogszabályoknak megfelel, vagy olyan eljárási szabálysértés történt, amely az ügy érdemi elbírálására nem hatott ki, illetve az a Kúria közzétett határozatától jogkérdésben nem tér el, a Kúria a megtámadott határozatot hatályában fenntartja. (3) Ha a legfőbb ügyész a perben szakmai véleményét kifejtette, a Kúria a felülvizsgálati határozatot megküldi a legfőbb ügyésznek. (4) Felülvizsgálati eljárásban egyszerűsített ítélet nem hozható.	(1) * If the decision requested for review is unlawful in law or differs in law from the published decision of the Curia, the court shall issue a final decision. (a) set aside, in whole or in part, and, if necessary, order the court seised to conduct new proceedings and give a new decision; (b) alter it by annulling the contested administrative act and ordering the administrative body to conduct a new procedure. (2) * If the decision requested to be reviewed complies with the law or a procedural violation has occurred which did not affect the substantive adjudication of the case or does not deviate in law from the published decision of the Curia, the Curia shall maintain the contested decision in force. (3) If the Attorney General has expressed a professional opinion in the lawsuit, the Curia shall send the review decision to the Attorney General. (4) A simplified judgment may not be given in a review procedure.
2017. évi XC. törvény a büntetőeljárásról 184. szakasz (2): (2) A személyazonosság megállapítása során a terheltnek nyilatkoznia kell a személyét azonosító és a vele való kapcsolattartást biztosító következő adatokról: a) neve, születési neve,	Act XC of 2017 on Criminal Proceedings Section 184 (2): 2. In establishing identity, the accused shall declare the following details identifying him or her and ensuring that he or she is in contact with him or her: a) name, birth name, b) place and date of birth,

b) születési helye és ideje, c) anyja neve, d) állampolgársága, e) személyazonosító okmányának száma, f) lakcíme, értesítési címe, tényleges tartózkodási helye, g) kézbesítési címe, telefonos elérhetősége. 244. szakasz (6): 244. § (6) Az elektronikus hírközlési szolgáltatást végző szervezetek, valamint a postai küldemények, vagy az egyéb zárt küldemények, továbbá az információs rendszerben tárolt adatok továbbítását, feldolgozását, kezelését végző szervezetek kötelesek a leplezett eszközök alkalmazását biztosítani és az alkalmazásra feljogosított szervekkel együttműködni. 261-262. szakaszok: 261. § (1) A büntetőeljárásban a bíróság, az ügyészség és a nyomozó hatóság, illetve - törvényben meghatározott esetben - az előkészítő eljárást folytató szerv bármely szervtől, jogi személytől vagy jogi személyiséggel nem rendelkező szervezettől adatszolgáltatást kérhet. (2) A vádemelés után az ügyészség a bizonyítási indítvány megtétele, bizonyítási eszköz felkutatása és biztosítása érdekében adatszolgáltatást kérhet. (3) Az adatkérés keretében a büntetőeljárással összefüggésbe hozható,	c) mother's name, d) nationality, e) the number of your identity document, f) address, address of notification, actual place of residence, g) delivery address, telephone contact. Section 244 (6): § 244. (6) Organizations providing electronic communications services, as well as postal items or other closed items, as well as organizations performing the transmission, processing and management of data stored in the information system are obliged to ensure the use of disguised devices and co-operate with authorized bodies. 261-262. sections: § 261. (1) In criminal proceedings, the court, the prosecutor's office and the investigating authority or, in cases specified by law, the body conducting the preparatory proceedings may request information from any body, legal person or organization without legal personality. (2) After the indictment, the public prosecutor's office may request the provision of information in order to make a motion of proof, search for and provide a means of proof. (3) In the context of a request for information, it may be linked to criminal proceedings, a) the transmission of data held by the organization,

a) a szervezet birtokában lévő adat továbbítása, b) a szervezet birtokában lévő elektronikus adat vagy irat továbbítása, vagy c) a szervezet által teljesíthető tájékoztatás adása kérhető. (4) Az adatkérés állami vagy helyi önkormányzati nyilvántartásban kezelt adat továbbítására, illetve átvételére is irányulhat. (5) Az adatkérésre vonatkozó kérelemben meg kell jelölni a) az adatkérés e törvény szerinti feltételeit, célját, b) az adatszolgáltatás teljesítéséhez szükséges, az adatszolgáltatás tárgyának azonosítására szolgáló adatokat, így különösen az érintett személy, tárgy vagy szolgáltatás adatait, c) a szolgáltatandó adatok körét és d) az adatszolgáltatás teljesítésének módját és határidejét. 262. § (1) A nyomozó hatóság és a rendőrség belső bűnmegelőzési és büntetőrendészeti feladatokat ellátó szerve, valamint a rendőrség terrorizmust elhárító szerve kizárólag az ügyészség engedélyével kérhet adatszolgáltatást a) * b) * c) az elektronikus hírközlési szolgáltatótól, d) a postai szolgáltatótól, illetve a postai közreműködői tevékenységet végző személytől vagy szervezettől,	(b) the transmission of electronic data or records held by the organization; or (c) providing information that the organization can provide on request. (4) A data request may also be aimed at the transmission or receipt of data managed in a state or local government register. (5) The request for data shall indicate a) the conditions and purpose of the data request pursuant to this Act, (b) data necessary to identify the subject of the supply, in particular the person, object or service concerned, (c) the scope of the data to be provided; and (d) the manner and deadline for completing the reporting. § 262. (1) The investigative authority and the body of the police performing internal crime prevention and detection functions, as well as the police counter-terrorism body may request data only with the permission of the prosecutor's office a) * b) * c) the electronic communications service provider, d) the postal service provider or the person or organization performing the activity of postal intermediary, (e) from an organization handling data which are bank secrets, payment secrets, securities secrets, treasury secrets or insurance secrets, in respect of such data,

e) a banktitoknak, fizetési titoknak, értékpapírtitoknak, pénztártitoknak vagy biztosítási titoknak minősülő adatot kezelő szervezettől, ilyen adatra vonatkozóan, f) az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló törvényben meghatározott egészségügyi és személyes adatot kezelő szervezettől, ilyen adatra vonatkozóan. (2) Az adatkéréshez szükséges engedély iránti indítványhoz csatolni kell az adatkérés indoklását alátámasztó ügyiratokat. (3) Ha az adatkérés engedélyezése olyan késedelemmel járna, amely az adatkéréssel elérni kívánt célt jelentősen veszélyeztetné, engedély nélkül is kérhető az adatszolgáltatás. Az adatszolgáltatás nem tagadható meg az ügyészi engedély hiánya miatt. Ilyen esetben az ügyészség engedélyét utólag haladéktalanul be kell szerezni. Ha az adatkérést az ügyészség nem engedélyezi, az így beszerzett adatok bizonyítékként nem használhatók fel és azokat haladéktalanul törölni kell. 264-265. szakaszok: 264. § (1) Az adatkérés keretében megkeresett szervezet - ha törvény másképp nem rendelkezik - köteles a kérelemben foglaltakat a megállapított határidő alatt teljesíteni vagy annak észlelését követően a teljesítés akadályát haladéktalanul közölni. Az adatszolgáltatást hiányos vagy töredékadatok esetén is teljesíteni kell. (2) Az adatkérés keretében megkeresett szervezet köteles a kérelemben foglaltakat - ideértve különösen az adat feldolgozását,	f) from an organization handling health and personal data as defined in the Act on the Processing and Protection of Health and Related Personal Data, in respect of such data. (2) The application for a permit required for a request for data shall be accompanied by the documents supporting the justification of the request for data. (3) If the authorization of a request for data would result in a delay which would significantly jeopardize the purpose to be achieved by the request for data, the provision of data may be requested without authorization. The provision of data cannot be refused due to the lack of prosecutor's permission. In such a case, the permission of the prosecutor's office must be obtained immediately afterwards. If the request for data is not authorized by the prosecution, the data thus obtained may not be used as evidence and must be deleted immediately. 264-265. sections: § 264. (1) The organization contacted within the framework of the data request shall, unless otherwise provided by law, be obliged to comply with the contents of the request within the established term or to notify the obstacle to the performance immediately upon its detection. The data must also be provided in case of incomplete or fragmentary data. 2. The requested authority shall comply with the request, including in particular the processing, recording or transmission of the data in writing or by electronic means, free of charge.

írásban vagy elektronikus úton való rögzítését és továbbítását - térítésmentesen teljesíteni. (3) A rejtjelezett vagy más módon megismerhetetlenné tett adatot az adatkérés keretében megkeresett szervezet köteles az átadás vagy a közlés előtt eredeti állapotába visszaállítani, illetve az adatszolgáltatást kérő szerv számára az adat tartalmát megismerhetővé tenni. (4) Az adatkérés keretében csak annyi és olyan személyes adat szolgáltatása kérhető, amely az adatkérés céljának megvalósításához elengedhetetlenül szükséges. (5) Ha az adatkérés eredményeként olyan személyes adat jut az adatszolgáltatást kérő szerv tudomására, amely az adatkérés céljával nem függ össze, az adatot haladéktalanul törölni kell. Ha a törlendő személyes adat eredeti iratban szerepel, az adatkérés céljával összefüggő személyes adatról kivonatot kell készíteni és ezzel egyidejűleg az eredeti iratot az adatkérés keretében megkeresett szervezetnek vissza kell küldeni. (6) Az adatkérés keretében az adatszolgáltatást kérő szerv birtokába került eredeti iratot legkésőbb az eljárás befejezésekor az adatkérés keretében megkeresett szervezetnek vissza kell küldeni. (7) Ha az adatkérésről történő tájékoztatás a büntetőeljárás eredményességét veszélyeztetné, az adatszolgáltatást kérő szerv erre vonatkozó kifejezett rendelkezése alapján az adatkérés keretében megkeresett szervezet a kérelem tényéről és a kérelemben foglaltakról, valamint az annak során teljesített adattovábbítás tartalmáról másnak nem adhat	(3) The organization requested in the framework of the data request shall restore the encrypted or otherwise unknown data to its original state prior to the transfer or communication, and shall make the content of the data available to the body requesting the provision of data. (4) Within the framework of a data request, only such personal data and such data as are strictly necessary for the realization of the purpose of the data request may be requested. (5) If, as a result of a request for data, personal data come to the knowledge of the body requesting the provision of data which are not related to the purpose of the request for data, the data shall be deleted immediately. If the personal data to be deleted are in an original document, an extract of the personal data related to the purpose of the data request must be prepared and at the same time the original document must be returned to the organization contacted in the data request. (6) The original document received by the requesting body in the framework of the request for data shall be returned to the requested organization at the latest at the end of the procedure. (7) If the provision of information on the request would jeopardize the effectiveness of criminal proceedings, the requested authority may not provide information on the fact of the request and the content of the request and the content of the transmission, to keep it all a secret. In the event of a request by the data subject for information on the processing of his or her personal data, information shall be provided which does not indicate that the transfer of his or her personal data has taken

tájékoztatást és köteles biztosítani, hogy mindezek titokban maradjanak. A kérelemmel érintett személynek a saját személyes adatai kezelésére vonatkozó tájékoztatás iránti kérelme esetén olyan tájékoztatást kell adni, amelyből nem derül ki, hogy a személyes adatainak továbbítására az adatkérés céljából sor került. Erre az adatkérés keretében megkeresett szervezetet az adatkérésre vonatkozó kérelemben figyelmeztetni kell. (8) A (7) bekezdés szerinti korlátozás az előkészítő eljárás befejezéséig, illetve a nyomozás befejezéséig tarthat, kivéve, ha a korlátozás megszüntetése az érintettel szemben folytatott más büntetőeljárás eredményességét veszélyeztetné. A korlátozás megszüntetéséről az adatkérés keretében megkeresett szervezetet tájékoztatni kell. 265. § (1) Ha az adatkérés keretében megkeresett szervezet a kérelemben foglaltakat a megállapított határidőn belül nem teljesíti, annak teljesítését alaptalanul megtagadja, vagy a 264. § (7) bekezdésében foglalt kötelezettségét megszegi, rendbírsággal sújtható. Ha annak feltételei fennállnak, a rendbírság kiszabása mellett az e törvényben meghatározott kényszerintézkedés is elrendelhető. (2) Ha az adatkérés keretében megkeresett szervezet a kérelemben foglaltakat azért nem teljesíti, mert azt törvény kizárja, a megkeresett szervezet birtokában lévő adat megszerzése érdekében a megkeresett szervezetet érintő további eljárási cselekmény nem végezhető. 267. szakasz: 267. § (1) Az ügyészség, a nyomozó hatóság, a rendőrség belső bűnmegelőzési és	place for the purpose of the request. The requested organization shall be notified of this in the request for data. 8. A restriction pursuant to paragraph 7 may last until the end of the preparatory proceedings or the investigation, unless the removal of the restriction would jeopardize the effectiveness of other criminal proceedings against the data subject. The requested organization shall be informed of the lifting of the restriction. § 265. (1) If the organization contacted within the framework of the data request fails to comply with the contents of the request within the established term, it unreasonably refuses to comply with it or violates its obligation set forth in § 264 (7), may be fined. If the conditions are met, in addition to the imposition of a fine, the coercive measure specified in this Act may also be ordered. (2) If the requested organization does not comply with the provisions of the request because it is excluded by law, no further procedural act concerning the requested organization may be performed in order to obtain the data in the possession of the requested organization. Section 267: § 267. (1) The prosecutor's office, the investigating authority, the police's internal crime prevention and detection body and the police's counter-terrorism body may collect data in order to establish a suspicion of a criminal offense and to clarify whether there are means of proof, and where are they located.

bűnfelderítési feladatokat ellátó szerve, valamint a rendőrség terrorizmust elhárító szerve adatgyűjtést végezhet a bűncselekmény gyanújának megállapítása céljából, illetve annak tisztázása érdekében, hogy vannak-e bizonyítási eszközök, és ezek hol találhatók. (2) * A vádemelés után az ügyészség a bizonyítási indítvány megtétele, bizonyítási eszköz felkutatása és biztosítása, továbbá az elkobozható vagy a vagyonelkobzás alá eső dolog vagy vagyon felderítése és biztosítása érdekében adatgyűjtést végezhet, ehhez a nyomozó hatóságot és a nyomozó hatóság vagyonvisszaszerzésért felelős szervét is igénybe veheti. (3) Az adatgyűjtés során a) az ügyészségről szóló törvényben, a rendőrségről szóló törvényben, illetve a Nemzeti Adó- és Vámhivatalról szóló törvényben meghatározott nyilvántartásokból adatok gyűjthetők, b) a nyilvánosságra hozatal céljából készített vagy jogszerűen nyilvánosságra hozott adatállományból, illetve forrásból adatok gyűjthetők, c) bárkitől felvilágosítás kérhető, d) kép-, hang- vagy kép- és hangfelvétel bemutatásával személy vagy tárgy kiválasztatása, illetve azonosítása kérhető, illetve e) a bűncselekmény helyszínét meg lehet vizsgálni. (4) Az adatgyűjtést végző hatóság tagja az adatgyűjtésről feljegyzést készít.	(2) * Following an indictment, the public prosecutor's office may collect data in order to make a request for evidence, locate and secure evidence, and to detect and secure confiscated or confiscated property or property, including the investigating authority and the investigating authority's asset recovery body. you can use. (3) During data collection a) data may be collected from the registers specified in the Act on the Prosecutor's Office, the Act on the Police and the Act on the National Tax and Customs Administration, (b) data may be collected from a file or source prepared or lawfully disclosed for the purpose of disclosure, c) information can be requested from anyone, (d) the selection or identification of a person or object may be requested through the presentation of an image, sound or image and sound recording; or (e) the location of the offense may be investigated. (4) The member of the data collection authority shall make a record of the data collection. 5. A communication contained in a record concerning the collection of data may be used as a testimony if it is maintained during the interrogation of the data subject as a defendant or witness.

(5) Az adatgyűjtésről készült feljegyzésbe foglalt közlés vallomásként akkor használható fel, ha azt az érintett terheltként vagy tanúként történő kihallgatása során fenntartja.	
2020. évi CXXVII. törvény egyes törvényeknek az egyenlő bánásmód követelménye hatékonyabb érvényesítését biztosító módosításáról 8. szakasz: 8. § Hatályát veszti a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény 1. § (4) bekezdés b) pontja.	Act CXXVII of 2020 on amending certain laws to ensure more effective enforcement of the requirement of equal treatment Section 8: § 8 Act XLIII of 2010 on the status of central state administration bodies and members of the Government and state secretaries is repealed. Section 1 (4) (b) of the Act.
180/2004. (V. 26.) Kormányrendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről	180/2004 (V. 26) Government Decree on the arrangements for the cooperation of organisations carrying out electronic communications tasks and organisations authorised to obtain secret information or secret data
46/2020. (III. 16.) Kormányrendelet az élet- és vagyonbiztonságot veszélyeztető tömeges megbetegedést okozó humánjárvány megelőzése, illetve következményeinek elhárítása, a magyar állampolgárok egészségének és életének megóvása érdekében elrendelt veszélyhelyzet során teendő intézkedésekről (III.)	46/2020 (III. 16) Government Decree on measures to be taken in the event of an emergency to prevent or avert the consequences of a human epidemic that threatens the safety of life and property and to protect the health and life of Hungarian citizens (III.)
179/2020. (V. 4.) Kormányrendelet a veszélyhelyzet idején az egyes adatvédelmi és adatigénylési rendelkezésektől való eltérésről	179/2020 (V. 4) Government decree on derogations from certain data protection and data request provisions in the event of an emergency

Bibliography

English titles

Legislation

EU Charter of Fundamental Rights.

General Data Protection Regulation.

Directive 2000/43 of 29 June 2000 on implementing the principle of equal treatment between persons irrespective of racial or ethnic origin.

Reports

Hungarian Civil Liberties Union and Privacy International, *The Right to Privacy in Hungary Stakeholder Report Universal Periodic Review 25th Session* (2015).

Monitoring Progress in National Initiatives on Digitising Industry, Country Report Hungary (European Commission 2020).

Deutsche Telekom, *Transparency Report: Hungary*
<https://www.telekom.com/en/corporateresponsibility/data-protection-data-security/news/hungary-363562>.

Google and Apple, *Report Jump in Requests for User Data* (BBC News, 2 October 2017)
<https://www.bbc.com/news/technology41442857>.

Stephen Nellis, *Apple Sees Steep Increase in US National Security-Related Data Requests* (Business Insider, 25 May 2018)
<http://www.businessinsider.com/apple-nsa-datarequest-transparency-report-2018-5>.

Report of COMEST on Robotics Ethics (UNESCO, 2017).

NAIH, *Resolution 2020/5533* (Hungarian National Authority for Data Protection and Freedom of Information).

European Commission, *Digital Transformation Scoreboard 2018: EU Businesses Go Digital: Opportunities, Outcomes and Uptake*
https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Digital%20Transformation%20Scoreboard%202018_0.pdf

Books

Ellenberger, Jürgen, 'Abschnitt 2. Sachen und Tiere' in *Palandt (hg.)* (ed), *Kommentar zum BGB* (Beck 2019).

Csink, Lóránt, Balázs Schanda, and András Zs. Varga (eds), *The Basic Law of Hungary – A First Commentary* (Clarus Press 2012).

Hacker, Philipp, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law' (2018) *Common Market Law Review* 55(4) 1166.

Koch, Bernard A, 'Product Liability 2.0 – Mere Update or New Version?' in Sebastian Lohsse, Reiner Schulze, and Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things* (Münster Colloquia on EU Law and the Digital Economy IV, Nomos 2019).

Periodicals

Hacker, Philipp, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law' (2018) *Common Market Law Review* 55(4) 1166.

In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World (International Network of Civil Liberties Organizations)
<https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf>.

Pujar, S M and Satyanarayana, K V, 'Internet of Things and Libraries' (2015) *Annals of Library & Information Studies* 62(3) 186
<http://op.niscair.res.in/index.php/ALIS/article/view/9800>.

European Data Protection Board, Thirtieth Plenary Session: EDPB Response to NGOs on Hungarian Decrees and Statement on Article 23 GDPR
https://edpb.europa.eu/edpb_workshop_en.

Aiden-Michel, *Uncharted: Big Data as a Lens on Human Culture*.

European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust COM (2020) 65 final, 14-22
https://www.ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

McCarthy, John, 'What Is AI? / Basic Questions' Jmc.Stanford.Edu
<http://jmc.stanford.edu/artificial-intelligence/what-isai/index.html>.

Chronowski, Nora, 'The New Hungarian Fundamental Law in the Light of the European Union's Normative Values' <https://poseidon01.ssrn.com>.

Lewis, Paul, 'I Was Shocked It Was So Easy: Meet the Professor Who Says Facial Recognition Can Tell If You're Gay,' *The Guardian* (7 July 2018).

Revolidis, Ioannis and Dahi, Alan, 'The Peculiar Case of the Mushroom Picking Robot: Extra-contractual Liability in Robotics' in Marcelo Corrales, Mark Fenwick, and Nikolaus Forgó (eds), *Robotics, AI and the Future of Law* (Springer, Singapore 2018) 59.

Digital resources

European Commission, *What is Personal Data?*
<https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hu>.

European Commission, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust* COM (2020) 65 final
<https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf>.

European Parliament, *Resolution of 16 July 2020 on Artificial Intelligence in the EU* (2020)
https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html.

European Parliament, *Resolution on Artificial Intelligence and Civil Rights* (2021)
https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html.

European Parliament, *Study on Artificial Intelligence in the EU* (2020)
[https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU\(2020\)621926_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf).

European Union Agency for Fundamental Rights, *Article 8: Protection of Personal Data*
<https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data>.

Human Rights Watch, *Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and the Use of AI in Weapon Systems* (10 August 2020)
<https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and>.

McCarthy, John, *What Is AI? / Basic Questions* (Jmc.Stanford.Edu)
<http://jmc.stanford.edu/artificial-intelligence/what-isai/index.html>.

On AI and Robotics (Policy@Manchester)
https://policyatmanchester.shorthandstories.com/on_ai_and_robotics/index.html.

Stop Killer Robots <https://www.stopkillerrobots.org/>.

United Nations, *Impact of Digital Technologies* (UN75)
<https://www.un.org/en/un75/impact-digital-technologies>.

World Intellectual Property Organization, *Artificial Intelligence and Intellectual Property Policy*
https://www.wipo.int/about-ip/en/artificial_intelligence/policy.html.

Case-law

According to the jurisprudence created in and after the case of *Flaminio Costa v E.N.E.L.* - Judgment of the Court of 15 July 1964.

Boyd and Crawford 2013.

Skilton and Hovsepian 2017.

CJEU, Case 109/88, Danfoss, EU:C:1989:383 cited by Hacker, 'Teaching Fairness to Artificial Intelligence'.

Hungarian titles

Legislation

Magyarország Alaptörvénye.

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

2003. évi C. törvény az elektronikus hírközlésről.

2009. évi CLV. törvény a minősített adat védelméről.

2011. évi CLI. törvény az Alkotmánybíróságról.

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

2012. évi C. törvény a Büntető Törvénykönyvről.

2013. évi V. törvény a Polgári Törvénykönyvről.

2016. évi CXXX. törvény a polgári perrendtartásról.

2016. évi CL. törvény az általános közigazgatási rendtartásról.

2017. évi I. törvény a közigazgatási perrendtartásról.

2017. évi XC. törvény a büntetőeljárásról.

2020. évi CXXVII. törvény egyes törvényeknek az egyenlő bánásmód követelménye hatékonyabb érvényesítését biztosító módosításáról.

180/2004. (V. 26.) Kormányrendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről.

46/2020. (III. 16.) Kormányrendelet az élet- és vagyonbiztonságot veszélyeztető tömeges megbetegedést okozó humánjárvány megelőzése, illetve következményeinek elhárítása, a magyar állampolgárok egészségének és életének megóvása érdekében elrendelt veszélyhelyzet során teendő intézkedésekről (III.).

179/2020. (V. 4.) Kormányrendelet a veszélyhelyzet idején az egyes adatvédelmi és adatigénylési rendelkezésektől való eltérésről.

Reports

Baji 2017, Dessewffy–Láng 2015, Giczi–Szőke 2017, Jakobi 2014, Kmetty 2018, Nagy–Veroszta 2018, Németh 2015, Ságvári 2017a, 2017b, 2017c, Székely 2015, Vukovich 2015, Jakobi–Lócsei 2016, Z. Karvalics 2018.

Mesterséges intelligencia: a Bizottság felvázolja a beruházás ösztönzésére és az etikai iránymutatások kidolgozására vonatkozó európai megközelítést.
https://ec.europa.eu/commission/presscorner/detail/hu/IP_18_3362.

Books

Menyhárd, Attila: Dologi jog.

Ságvári Bence: Diszkrimináció, átláthatóság és ellenőrizhetőség.

Bernadette Somody, Máté Daniel Szabo, Beatrix, Vissy, Dalma Dojcsák: Alapjogi tanok.

Periodicals

Csáji, Balázs Csanád: A mesterséges intelligencia filozófiai problémái. (kézirat), ELTE Filozófia szak, 2002, 4. http://old.sztaki.hu/~csaji/CsBCs_MI.pdf.

Csink, Lóránt – Mayer Annamária: Variációka szabályozásra In: <https://mek.oszk.hu/13500/13526/13526.pdf>.

Eszteri, Dániel: A mesterséges intelligencia magánjogi viselkedéséért való magánjogi felelősség az online játékokban. Pályamunka, Budapest, 2014.
<https://jogaszvilag.hu/a-jovo-jogasza/a-mesterseges-intelligenciaviselkedeseert-valo-maganjogi-felelosseg-az-online-jatekokban/>.

Gregor, Katalin; Dr. Varga Judit, Dr; Lukovics, Adél; Molnár, Veronika, 'Az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV. törvény alkalmazása'.

Menyhárd, Attila, 'Diszkrimináció-tilalom és polgári jog'.

Pásztor, Emese, '„Magánélet és bizonytalanság” – A jogi kontrollmechanizmusok szerepe a nemzetbiztonsági célú titkos információgyűjtés alapjogi kockázatainak mérséklésében' (2017) Információs Társadalom, XVII./ 1., 24-44.

(///H:/ELTE-%20JOG/8.%20szemeszter/munka/ELSA/Maganelet_es_bizonytalansag_-A_jogi_kontrollmecha%20(1).pdf).

Case-law

15/1991 (IV.13) Alkotmánybírósági határozat

61/1992. (XI. 20.) Alkotmánybírósági határozat

36/2005. (X. 5) Alkotmánybírósági határozat

42/2012. (XII. 20.) Alkotmánybírósági határozat

3086/2013. (III. 27.) Alkotmánybírósági határozat

32/2015. (XI. 19.) Alkotmánybírósági határozat

30/2017. (XI. 14.) Alkotmánybírósági határozat

Szabó and Vissy v. Hungary, judgment of 12 January 2016, no. 37138/14

ELSA ITALY

Contributors

National Coordinator

Francesca Mulliri

National Researchers

Arianna Crosera

Eugenio Ciliberti

Federica Paolucci

Leila Kentache

Maria Vittoria Voi

Martina Caslini

Nesrine Kraiem

Olena Barda

Pierfrancesco De Felice

Valeria Argento

Veronica Gallo

National Linguistic Editor

Enrica Bertoldi

Giulia Piccioni

National Technical Editor

Federico Quagliarini

Marika Francescapia Casula

National Academic Supervisor

Avvocata Enrica Priolo

Introduction

'It should be evident that the protection of privacy rights has become a daunting challenge when information can be easily collected, processed, and disseminated'³⁹⁷. The rise of Advanced Digital Technologies (ADT) put the legislators in front of new challenges regarding the protection of privacy's rights. The concept of privacy is strongly affected by social and cultural evolutions, which brought today to a greater awareness of new technologies' real scope and impact on privacy as a fundamental human right. Furthermore, the 4th industrial revolution and a preponderance of new rising technologies' rapid development have left a legislative lack that needs to be filled in many ways³⁹⁸. Nowadays, the importance of a data protection policy, and so the protection of the data itself, is largely recognised, although it becomes essential to allocate the liability for violation of that same data, especially considering the legislative loophole. The aim of this research is to present an accurate photograph of the Italian framework, also in light of the recent pandemic situation, and underline the new concerns about privacy protection related to the real controlling power in the hands of the involved parties.

1. Which human rights issues do Advanced Digital Technologies pose in your country?

1.1. ADTs implications on human rights

The transition from human rights offline to the virtual field has aroused several problems. Advanced digital technologies (ADTs) are a delicate instrument that puts at great peril fundamental rights, due to the congenital duality of the instruments itself. The Council of Europe's Recommendations on Human Rights Impact Assessment clearly emphasise that 'Member states should establish a legal framework that sets out a procedure for public authorities to carry out human rights impact assessments (HRIAs) on AI systems acquired, developed and/or deployed by those authorities'³⁹⁹. The European Convention on Human Rights represents a primary tool regulating the domestic HRIA. Since the ECHR has to be referred to Article 117 of the Italian Constitution⁴⁰⁰, a contrasting national disposition has

³⁹⁷ Spinello R., *The Right to Privacy in the Age of Digital Technology*, in *Privacy in a Digital, Networked World - Technologies, Implications and Solutions*, edited by Zeadally Sherali and Badra Mohamad (Springer International Publishing Switzerland, 2015), 291.

³⁹⁸ Nucera S., *Intelligenza artificiale ed intervento umano: tra lacune giuridiche ed opportunità per il XXI secolo*, in *Ratio Iuris*, 24 February 2021.

³⁹⁹ Council of Europe Commissioner for Human Rights, Recommendation, Unboxing Artificial Intelligence: 10 steps to protect human rights, 2019, <<https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64>> accessed 21 February 2021.

⁴⁰⁰ Italian Constitutional Court, judgments nos. 348-349/2007.

to be considered as non-existent by the judge *a quo*. The Italian Constitution represents itself as the most relevant document within the domestic system in which human rights are safeguarded. The National Strategy for Artificial Intelligence underlines that AI must be at the service of people: human supervision has to be guaranteed in order to prevent the risks of aggravating social and territorial imbalances.⁴⁰¹ The Strategy provides the establishment of a permanent consultation tool on ethical and social issues of advanced digital technologies and dedicates specific attention to the most fragile subjects of society.⁴⁰² Indeed, anthropocentrism has been identified as one of the main Strategy's guiding principles: it is a timely priority to adequately protect fundamental freedoms and essential rights. Nevertheless, individuals' prerogatives are exposed to unprecedented threats. For instance, the right to privacy is challenged by third parties who can easily access private data; freedom of expression as well as the right to peaceful assembly and association encounter new limitations;⁴⁰³ neuro-privacy threatens the freedom of thought; automated decision-making procedures menace individuals' ability to obtain an effective remedy;⁴⁰⁴ the 'filter bubbles' undermine the right to free elections;⁴⁰⁵ modern surveillance tools bring the right to be presumed innocent until proven guilty into question⁴⁰⁶; moreover, children rights are directly endangered as recently shown by the TikTok case.⁴⁰⁷ As more and more information about individuals is classified as 'Big Data', there is ample scope for discriminatory practices. This non-exhaustive list of fundamental rights and freedoms is related to a complex legal framework.

1.2. International, European and Italian standards

⁴⁰¹ Ministry of Economic Development, 'Italian National Strategy for Artificial Intelligence' (2020) <www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf> accessed 21 February 2021.

⁴⁰² *ibid*, paras 3.6-3.7.

⁴⁰³ European Parliament, Directorate-General for External Policies, 'Surveillance and Censorship: The impact of technologies on human rights' (2015) <[www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU\(2015\)549034_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf)> accessed 21 February 2021.

⁴⁰⁴ Committee of Experts on Internet Intermediaries, 'Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications' (2018) <<https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a>>, 24.

⁴⁰⁵ MSI-NET, 'Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications' (2018), 30-32.

⁴⁰⁶ Jacopo Coccoli, 'The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era' (2017) 1(2) *Peace Human Rights Governance*, 223-250 <http://phrg.padovauniversitypress.it/system/files/papers/2017_2_4.pdf> accessed 21 February 2021.

⁴⁰⁷ Garante per la Protezione dei Dati Personali, 'TikTok si adegnerà alle richieste del Garante privacy. Ma l'autorità vigilerà sull'effettiva efficacia delle misure che saranno adottate' (2021) <www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9533424> accessed 21 February 2021.

At an international level, standards are primarily set by the Universal Declaration of Human Rights⁴⁰⁸ and the International Covenant on Civil and Political Rights.⁴⁰⁹ In this regard, the Convention for the Protection of Individuals⁴¹⁰ and the Convention on Cybercrime⁴¹¹ play an important role. Moreover, the UN Guiding Principles on Business and Human Rights require private sector entities to comply with all applicable laws and to respect human rights;⁴¹² the Recommendation on a Guide to human rights for Internet users emphasizes the equal application of human rights online and offline;⁴¹³ the European Ethical Charter announces relevant ethical principles;⁴¹⁴ the Guidelines on Artificial Intelligence and Data Protection⁴¹⁵ underline that safeguarding human rights should represent an essential prerequisite. Furthermore, the Declaration on the manipulative capabilities of algorithmic processes calls 47 Member States to ‘address the significant impacts of the targeted use of data on societies and on the exercise of human rights more broadly’.⁴¹⁶ At European level, it has been recommended that all appropriate EU external financial instruments should be used to further protect and promote freedom of opinion and expression online as well as offline;⁴¹⁷ the White Paper on Artificial Intelligence affirms that European AI is grounded in values and fundamental rights such as human dignity and privacy protection⁴¹⁸; the EU Digital Single Market Strategy considers the impact of ADT

⁴⁰⁸ Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).

⁴⁰⁹ International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

⁴¹⁰ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), amended in 2014.

⁴¹¹ Council of Europe, ‘Convention on Cybercrime’ (2001), art 15.

⁴¹² OHCHR, ‘Guiding Principles on Business and Human Rights’ (2011)

<https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed 28 February 2021.

⁴¹³ Council of Europe Committee of Ministers, *Recommendations of the Committee of Ministers on a Guide to human rights for Internet users*, CM/Rec(2014)6.

⁴¹⁴ European Commission for the Efficiency of Justice, ‘European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment’ (2018)

<www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment> accessed 28 February 2021.

⁴¹⁵ Directorate General of Human Rights and Rule of Law, ‘Guidelines on Artificial Intelligence and Data Protection’ (2019)

<<https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/1680919d8>> accessed 28 February 2021.

⁴¹⁶ Council of Europe Committee of Ministers, ‘Declaration on the manipulative capabilities of algorithmic processes’ (2019) <https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b> accessed 28 February 2021.

⁴¹⁷ Foreign Affairs Council Meeting, ‘EU Human Rights Guidelines on Freedom of Expression Online and Offline’ (2014) <www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142549.pdf> accessed 28 February 2021.

⁴¹⁸ European Commission, ‘White Paper On Artificial Intelligence: A European approach to excellence and trust’ (2020)

<https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 28 February 2021.

on the most fundamental rights⁴¹⁹; the Charter of Fundamental Rights of the European Union provides a foundation for European positions on digital rights;⁴²⁰ the EU General Data Protection Regulation (GDPR) represents a primary document which aims to protect individuals' personal data and to unify the regulation within the EU⁴²¹. Moreover, the EU Cybersecurity Plan protects open internet and online freedom and it emphasises the need of fundamental rights' protection in cyberspace.⁴²² At national level, Article 2 of the Italian Constitution affirms that the Italian Republic recognises and guarantees the inviolable rights of the person, which are consecrated in its Part I, Title I. Pursuant to Article 10, the Italian legal system conforms to the generally recognised principle of international law with the following limits: the 'fundamental principles of the Constitutional system' and the 'inalienable rights of the person'.⁴²³ Finally, by virtue of the above mentioned Article 117, the European Convention on Human Rights has automatic effects in the domestic level and represents a relevant legal standard since 1950; in particular, Articles 6, 8, 9, 10, 11, 13, 14 ECHR are the ones directly involved in the challenges of the Information Age.

2. How is personal information protected in your national legislation?

2.1. The information society and its data

Information may be considered the heart of our era's concerns and delights: it is argued that we are submerged and embedded in what is called Infosphere, the 'whole system of services and documents, encoded in any semiotic and physical media, whose contents include any sort of data, information and knowledge with no limitations either in size, typology or logical structure'⁴²⁴ and that our lives are increasingly on-lives that annul boundaries between digital and physical.⁴²⁵ In this context, information is essentially described as data where data is well formed and meaningful,⁴²⁶ the management of which has become particularly important with the advent of ICTs. Since then, a rising importance

⁴¹⁹ European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe (2015)

<<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192>> accessed 28 February 2021.

⁴²⁰ Charter of Fundamental Rights of the European Union, OJ 2009 C 83/389.

⁴²¹ European Parliament and Council, Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016), OJ 2016 L 119/1.

⁴²² European Commission, EU Cybersecurity plan to protect open internet and online freedom and opportunity (2013)

<<https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>> accessed 28 February 2021.

⁴²³ Italian Constitutional Court, Judgment no. 238/2014.

⁴²⁴ Luciano Floridi, *Philosophy and computing: an introduction* (Routledge 1999) 8.

⁴²⁵ Luciano Floridi, *The Fourth Revolution: how the infosphere is reshaping human reality* (Oxford University Press 2014) 44.

⁴²⁶ Luciano Floridi, *Information: A Very Short Introduction* (Oxford University Press 2010) 20.

in the modalities used to manage what remains personal, what is well-formed and meaningful about each individual within this all-encompassing Infosphere, has been observed. And what is it that remains personal? Data can be described as personal if the well formed and meaningful information it conveys is ultimately related to a physical person and therefore, when it permits identification and individuation⁴²⁷. Personal data is in this sense defined by Article 4(1) of the General Data Protection Regulation of 2016 as ‘any information relating to an identified or identifiable natural person (‘data subject’) [...] directly or indirectly.’

2.2. Protection of personal information: at the highest level

It is no wonder that this information is, in virtue of the described identificatory function, worthy of particular protection and that its protection, due to the close relationship with personal identity, is entrusted to fundamental human rights’ law of the highest value. In this regard, the premises for national protection of personal information are extensively present in international law. In Italy, these mainly consist of the Universal Declaration of Human Rights and, at the regional level, of the European Convention on Human Rights (ECHR). The latter is particularly influential due to its judicial enforcement through the European Court of Human Rights (ECtHR), which makes it a ‘living instrument’⁴²⁸ and because of the peculiar status of international law under Article 117 of the Italian Constitution. It is also worth mentioning that when implementing European Law Member States are also bound by the Charter of Fundamental Rights of the European Union (CFREU), which provides for the protection of personal data in its Article 8. At this high level in the pyramid of sources of law, personal information is protected through the right to privacy, covered by Article 8 of the ECHR and by Article 2 of the Italian Constitution. In both cases, the Articles do not specifically refer to personal information but have been judicially interpreted to this end. Indeed, the Italian Court of Cassation with its judgment no. 2129 of the 27th of May 1975, confirmed the existence in the Italian legal system of a ‘general right to privacy of the person’ and the European Court of Human Rights repeatedly invoked Article 8 in cases regarding among others the access to personal data, the consent of the data subject and the processing of personal data by the police.⁴²⁹

2.3. The Italian framework on data processing

⁴²⁷ Camilla Bistolfi, Luca Bolognini, Enrico Pelino, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali* (Giuffrè 2016) 30.

⁴²⁸ George Letsas, *The ECHR as a living instrument: its meaning and legitimacy* in Andreas Follesdal, Birgit Peters and Geir Ulfstein (eds.) *Constituting Europe: The European Court of Human Rights in a National, European and Global Context* (Cambridge University Press 2013) 108.

⁴²⁹ See Data Protection Unit of the Council of Europe, ‘Case law of the European Court of Human Rights concerning the protection of personal data’ (2018).

The general human right to privacy potentially applies to personal information during its entire life-cycle⁴³⁰, the essence of which can be traced back to activities under the broadly defined term of processing (*trattamento*) of data. The main Italian legislation on the protection of personal information, namely Legislative Decree no. 196 of 2003, is indeed focussed on these activities, in accordance with the GDPR of 2016 therein integrated through Legislative Decree no. 101 of 2018. It may be stated that the underlying means of protection for personal information provided by the latter instruments essentially consist in making the processing activities conditional to a legitimate legal basis and/or consensus according to the modalities described in Article 6(1) of the GDPR⁴³¹ and subject to a cardinal supervising authority (*Garante per la protezione dei dati personali*), created in 1996 by Law no. 675. The conditions according to which the processing is allowed largely depend on the category this personal information belongs to and in particular on whether it is classified as special categories of data under Article 9(1) of the GDPR, which states that the processing of special categories of data is prohibited if one of the conditions under its second paragraph does not apply.

2.4. Concluding remarks

Therefore, summing up the current legislative structure as regards data protection, the will to eliminate incompatibilities with the latest European Regulation is evident: as already mentioned, the pre-existent Legislative Decree no. 196 of 2003 has been integrated with no. 101 of 2018 to guarantee compliance with the GDPR, even though the latter is a Regulation and directly binding in its entirety according to Article 288 of the Treaty on the Functioning of the European Union (TFEU). It is important to underline that in Legislative Decree no. 101/2018 the Legislator has in several cases provided for a higher protection than the one described by the GDPR itself, using ‘opening clauses [...] that leave discretionary powers in certain specific fields offered by the GDPR’.⁴³² A significant example consists in the introduction, through Article 2f(1) and 2f(2), of the further requirement of biannual guarantee measures introduced by the supervising authority to protect genetic, biometric and health data in case they are processed. The dissemination of these data is also prohibited by Article 2f(8).

⁴³⁰ Floridi (n 426) 5.

⁴³¹ Servizio Studi della Camera dei Deputati, ‘L’adeguamento della disciplina sulla protezione dei dati personali al Regolamento (UE) 2016/679, A.G. 22’ (2018) 13.

⁴³² Guisella Finocchiaro, ‘Italy: The Legislative Procedure for National Harmonisation with the GDPR’ (2018) 4 Eur Data Prot L Rev 496.

3. To which extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?

Privacy and data protection are considered the European First Amendments⁴³³. This is not something that States can achieve on their own needing the intermediation of who dominates the digital: platforms. The collaboration between private and public is indispensable when it comes to remove contents hosted by those ‘large digital incumbents’⁴³⁴ and to enforce the protection of fundamental rights online. States, in particular in Europe, are moving toward a legislation that makes them accountable for what happens in their realms⁴³⁵. Hence, by examining the legal rationale under the light of the Italian case studies while applying and interpreting the relevant legislation⁴³⁶ transposing the Directive 2000/31/EC⁴³⁷ into the national legal system, this paragraph is going to show at which extent the private sector is self-regulating the limits of its liability and how this has consequences on the data protection.

3.1. Diving into the Italian ISP liability’s opacity

The purpose of the E-Commerce Directive was in line with the original market-oriented shape of the Community⁴³⁸: to facilitate electronic commerce by establishing a safe harbour⁴³⁹. However, since the digital environment has become the space where individuals’ lives are exerted in their totality, regulating liability has become a priority⁴⁴⁰. In this regard, Italy developed a restrictive approach to the exemption laid down by the

⁴³³ Paraphrasing the thoughts of Bilyana Petkova in ‘Privacy as Europe’s First Amendment’, (*European Law Journal* 25, no. 2, 2019).

⁴³⁴ Massimiliano Nuccio and Marco Guerzoni, ‘Big Data: Hell or Heaven? Digital Platforms and Market Power in the Data-Driven Economy’, (*Competition and change*, vol. 23(3), 2019).

⁴³⁵ This strategy is the object of on-going innovation at Communitarian level falling under the umbrella of the European Digital Strategy, amending the Directive 2000/31/EC. On this regard and on the level of liability, the main innovation is going to be visible in the Digital Service Act (hereafter DSA) ‘Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services’.

⁴³⁶ Italy implemented the Directive through Legislative Decree no. 70/2003.

⁴³⁷ Hereinafter, E-Commerce Directive. European Parliament and of the Council Directive (EC) 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’ [2000] OJ L178/1).

⁴³⁸ This remark is visible not only in the Directive itself (this point of view is recalled also by Rec. 2) but also in the Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, COM (1998).

⁴³⁹ The core of this piece of legislation is represented by art. 12-15 establishing the mentioned safe harbour as a general exemption from the obligation of monitoring contents (art. 15) and making exceptions according to the activity conducted by the provider: “mere conduit”, “caching” and “hosting”.

⁴⁴⁰ Frank Pasquale pictures the primacy of the digital firms as writing that «they were private companies, but they controlled vital resources and enjoyed a power similar to that of a public authority». Frank Pasquale, *The Black Box Society* (Harvard University Press, 2015).

E-Commerce Directive. As scholars point out⁴⁴¹, on the basis of the Google France case⁴⁴², Italian courts⁴⁴³ started to develop a *tertium genus* of provider: namely, a category that is not excluded from the liability exemption, but is subject to a stricter standard⁴⁴⁴. This results in an allocation of liability that may arise even in absence of a formal notice from a competent authority. The whole issue is about the “actual knowledge” requirement in art. 14 of Directive 2000/31/EC, implemented in “a singular way”⁴⁴⁵ by art. 16 (1) Dlgs⁴⁴⁶ no. 70/2003. Under some circumstances, this provision goes beyond the strict liability regime and creates a grey zone⁴⁴⁷ where ISPs are demanded to take some measures in order to prevent the reiteration of illegal conducts. Even if it may appear reasonable⁴⁴⁸, this obligation has some consequences: on the business level, it may affect the firm and the idea beneath the Directive itself. On the other hand, it has effects on the level of enforcing fundamental rights.

3.2. Privatization of fundamental rights?

The activism of the Italian courts on this matter opened the door to a very debated and complicated matter, where the institutions, and not the courts, should be the real playmaker on shifting the paradigm. As long as there is uncertainty on allocating liability upon the removal of contents infringing fundamental rights, such as data protection under the light of art. 8 CFREU⁴⁴⁹ private actors will pivot the limits of their responsibility on taking down contents. The regulatory pressures reflect the increasing role of ISPs on appropriately balancing conflicting rights: a conduct that Bassini⁴⁵⁰ describes as “privatisation of fundamental rights”. The matter is not only the protection of personal

⁴⁴¹ *Inter alia*, Marco Bassini, ‘Mambo Italiano: The Perilous Italian Way to ISP Liability’, in *Fundamental Rights Protection Online*, (Elgar Online, 2020).

⁴⁴² Joint cases: Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C236-08) Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08).

⁴⁴³ One of the main judgments on which the issue of active and passive providers became relevant is Google v. Vividown, even if it is about criminal and not civil law. The legal saga comprehends: Court of Milan, 24 February 2010; Court of Appeals of Milan, 21 December 2012; Supreme Court, 17 December 2013.

Extensively on the topic: Ernesto Apa and Oreste Pollicino, *Modeling the Liability of Internet Service Providers: Google vs. Vividown: A Constitutional Perspective* (EGEA spa, 2013).

⁴⁴⁴ As long as they are active, some providers have more control, and they may have more knowledge of the illegal content: this is the assumption.

⁴⁴⁵ Bassini (n 441).

⁴⁴⁶ Dlgs is the shorthand for Legislative Decree.

⁴⁴⁷ As recent Italian case laws show, there is a general disagreement almost on everything. In particular, Italian Supreme Court, 19 March 2019, no. 7708, Yahoo! v. RTI; Rome Court of Appeal, 19 February 2018, no. 4312, Cesare Previti v. Wikimedia Foundation Inc.; Rome Tribunal, 1 February 2019, F.A. v. Google LLC, no. 81824.

⁴⁴⁸ Also considering some European Court case law such as Eva Glawischnig Piesczek v. Facebook, Case C-18/18 [2019] ECLI:EU:C:2019:821.

⁴⁴⁹ Charter of Fundamental Rights of the European Union, (2000/C 364/01).

⁴⁵⁰ Marco Bassini, ‘Fundamental Rights and Private Enforcement in the Digital Age’, (*European Law Journal*, 2019).

data and privacy, but the latter one, in the light of Rodotà's studies⁴⁵¹, shall be considered as the ensemble of the fundamental rights online. Fueling the private actors' involvement with opaque interpretation is not only a problem of liability but, once again, it concerns *de facto* the horizontal effects of fundamental rights enforced by private actors⁴⁵².

3.3. Conclusive remarks

Looking at the Italian experience in cases around the interpretation of the E-Commerce Directive, it was possible to observe the self-regulatory approach the private actors are demanded to undertake, becoming the "judges" of the contents hosted on their platforms⁴⁵³. This is not only a problem of data protection, but a matter of digital sovereignty and censorship: the more pressure and opacity to remove content is created, the more they will act accordingly creating a "collateral censorship".⁴⁵⁴ The hope is that the DSA will provide some clarification on this side and will build a new chapter of the "digital constitutionalism"⁴⁵⁵ rebalancing the allocation of powers between private and public.

4. What is the process of judicial review of cases data protection breaches?

4.1. The right to data privacy in the Italian legal system

With Law no. 675 of 31 December 1996⁴⁵⁶, the Legislator recognised, for the first time at a regulatory level, the existence of a right to privacy in the Italian legal system, aligning itself with the fundamental jurisprudential evolution on the subject which, after the initial analogical application of the *diritto all'immagine*⁴⁵⁷, raises the right of privacy to an inviolable human right guaranteed by Article 2 of the Italian Constitution⁴⁵⁸, recognising its autonomy⁴⁵⁹. The adherence to this anthropocentric vision highlights a deep evolution in the concept of privacy which, however, has not been grasped by the above-mentioned law,

⁴⁵¹ Stefano Rodotà and Paolo Conti, *Intervista Su Privacy e Libertà* (GLF Editori Laterza, 2005).

⁴⁵² Giorgio Giannone Codiglione and Marco Bassini, 'From Private Enforcement to Public Enforcement. Copyright Enforcement in the Digital Age: A Comparative Overview', (*Copyright and Fundamental Rights in the Digital Age*, 2020).

⁴⁵³ Marco Bellezza and Filippo Frigerio, 'A New Dawn for the ISP's Liability in Italy?', (*MediaLaws - Law and Policy of the Media in a Comparative Perspective*, 2018).

⁴⁵⁴ Jack Balkin, 'Free Speech and Hostile Environments', (*Columbia Law Review*, 1999).

⁴⁵⁵ Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union', (Rochester, NY: Social Science Research Network, 2019).

⁴⁵⁶ Art. 1 par. 1 of Law 31 December 1996, no. 675, *Protection of persons and other subjects regarding the processing of personal data*, in implementation of Directive 95/46/EC of the European Parliament and of the Council, <www.garanteprivacy.it>.

⁴⁵⁷ Court of Rome, judgment 14 September 1953, in *Foro Italiano*, Vol. 77, No 1 (1954), 115/116 – 133/134.

⁴⁵⁸ Constitutional Court, judgment on. 38/1973, which recalls Article 8 Charter of Fundamental Rights of the European Union and articles 8 and 10 ECHR; Court of Cassation, judgement of 20 April 1963, no. 990, in *Foro it*, 19963, I, 877.

⁴⁵⁹ Court of Cassation, judgement of 27 May 1975, no. 2129.

promulgated significantly later than the rest of Europe. Technological progress and liberalisation of telecommunications, in fact, leave the traditional American “right to be let alone” in the background⁴⁶⁰, focussing on the right to informative self-determination of the data subject⁴⁶¹ and on the need for data processing that is not detrimental to the rights and dignity of the individual⁴⁶². This passage is captured by Legislative Decree of 30 June 2003, no. 196⁴⁶³, the first codification on privacy in Europe, which, by repealing the previous legislation, recognises to anyone the independent⁴⁶⁴ right to the protection of personal data⁴⁶⁵, thus conforming to the EU regulatory framework⁴⁶⁶.

4.2. The balance between the right to data protection and other interests: the limitations to the rights of the data subject

The right to data protection becomes a legal prerogative of the exercise of other rights and freedoms⁴⁶⁷; this prerogative, however, cannot be understood in absolute terms, having to reconcile it with other fundamental rights in full compliance with the principle of proportionality⁴⁶⁸. In accordance with this approach, as far as is noted here, Article 23, paragraph 1, of the GDPR provides for the possibility for the Member State’s law to limite, by legislative measures, the scope of the obligations and rights referred to in the Articles from 12 to 21 and in Article 34 of the European Regulation, thus including the right of the data subject to limit the data processing (Article 18), the right to object to the data processing (Article 21), as well as the obligation of the data controller to communicate the data breach to the interested party (Article 34).

As regards the methods and occasions for exercising the rights of the data subject, the European Regulation is directly applicable in the Italian legal system from 25 May 2018, without the need for any national legislative adaptation: in fact, Title II of Part I of the Code regarding the Protection of Personal Data, entitled to Rights of the interested party, has been entirely repealed by Article 27 of the Legislative Decree no. 101 of 4 September

⁴⁶⁰ Samuel D. Warren – Louis D. Brandeis, *The Right to Privacy*, in Harvard Law Review, IV, 1890, No 5.

⁴⁶¹ Stefano Rodotà, *Tecnologie e diritti*, Il Mulino, Bologna, 1995.

⁴⁶² Recommendation No. R (99) 5 of the Committee of Ministers to Member States for the protection of privacy on the Internet, containing guidelines for the protection of individuals with regard to the collection and processing of personal data on the information highways, <www.garanteprivacy.it>.

⁴⁶³ Legislative Decree of 30 June 2003, n. 196, *Code regarding the Protection of Personal Data*, in force since 1° January 2004, <www.istat.it>. The Code was adopted in implementation of Directive 95/46/CE.

⁴⁶⁴ Francesca Naddeo, *The consent to the processing of the minor’s personal data*, in *Information and IT Law* (II), dossier 1, 1° February 2018, 27.

⁴⁶⁵ Art. 1 (repealed): ‘Anyone has the right to the protection of personal data concerning him’.

⁴⁶⁶ The right to the protection of personal data is part of the personality’s rights with constitutional coverage (Article 2 of the Italian Constitution), and is distinguished from the right to privacy, in accordance with the setting of the Charter of Fundamental Rights of the European Union (articles 7 and 8).

⁴⁶⁷ Giuseppe Santaniello, Vice President of the Guarantor for the protection of personal data, *The Italian Privacy Code from a European perspective*, 19 January 2004, in *InterLex, Law Technology Information*.

⁴⁶⁸ Whereas no. 4 GDPR in <www.eur-lex.europa.eu>.

2018, on ‘Provisions for the adaptation of national legislation to the provisions of EU Regulation 2016/679’⁴⁶⁹. The same decree introduces, within the revised code, a Chapter III containing ‘Provisions on the rights of the interested party’, providing for significant limitations on the exercise of rights pursuant to Articles 2-*undecies* and 2-*duodecies*. More precisely, it is emphasised that the Italian legal system, in order to protect the specific interests provided for by Article 2-*undecies*⁴⁷⁰ from an effective and concrete prejudice, establishes limitations on the exercise of only the rights and obligations set out in Articles 15 to 22 of the GDPR, effectively excluding any limitation on the obligation of the data controller to communicate the data breach, with the exception of ‘reasons of justice’⁴⁷¹, in accordance with art. 2-*duodecies*. In fact, in this case of personal data processing, the exercise of the interested party’s rights and the fulfilment of the obligation established by Article 34 can be delayed, limited or excluded to safeguard the independence of the judiciary and judicial proceedings, in compliance with the cardinal principles of necessity⁴⁷² and proportionality.

4.3. Procedural aspects of the judicial review of cases data protection breaches

The entry into force of the GDPR has made deep changes to the national data breach regulation, firstly by extending the obligation to notify the data subject of the violation of any personal data, originally provided exclusively for the suppliers of electronic communications services⁴⁷³. Furthermore, Chapter V of the Legislative Decree no. 101/2018, which consists of a single Article⁴⁷⁴, introduces the procedural provisions applicable to the data breach: more precisely, pursuant to the new Article 152 of the Code for the Protection of Personal Data, the judicial authority⁴⁷⁵ is mainly competent to decide on the appeals against the decisions of the guarantor authority, with full cognitive powers, confirming, in fact, a system based on the double protection track⁴⁷⁶. In particular, the

⁴⁶⁹ Legislative Decree n. 101 of 4 September 2018, in <www.gazzettaufficiale.it>.

⁴⁷⁰ These interests include those already contemplated in the previous art. 8 of the Personal Data Protection Code, now repealed, with the exception of the interest referred to in letter f-bis), introduced by art. 1 paragraph 681, Law 27 December 2019, no. 160.

⁴⁷¹ The ‘reasons for justice’ referred to in art. 2-*duodecies* refers to the limitation, provided for by Article 23 paragraph 1 letter. f) GDPR, to safeguard the independence of the judiciary and judicial proceedings.

⁴⁷² Pursuant to Article 5, paragraph 1, lett. c) of the GDPR, the processing must be limited to the use of data that are “adequate, relevant and limited to what is necessary with respect to the purposes for which they are processed”; the principle of necessity was already provided for by the previous art. 3 Code for the Protection of Personal Data, according to which “The information systems and computer programs are configured by minimising the use of personal data and identification data, so as to exclude their processing when the purposes pursued in individual cases can be achieved by, respectively, anonymous data or appropriate methods that allow the data subject to be identified only in case of need”.

⁴⁷³ Article 32-*bis* (repealed) of the Code regarding the Protection of Personal Data.

⁴⁷⁴ Article 17 amends the Article 10 of Legislative Decree 1 September 2011.

⁴⁷⁵ With the entry into force of the European Regulation, the forum becomes alternative: the jurisdiction is attributed to the court of the place where the data controller or the data subject resides.

⁴⁷⁶ With the exception of compensation for damage, which is the exclusive competence of the judge.

appeal is filed – under penalty of inadmissibility – within thirty days from the date of communication of the Guarantor for the Protection of Personal Data's⁴⁷⁷ provision; or, in the event of inaction by the guarantor, within thirty days of the expiry of the nine months deadline⁴⁷⁸ for deciding the complaint. The judgement that defines the trial is final.

5. Does the review constitute effective protection of data privacy?

In the European Union legal system, the protection of natural persons in relation to the processing of personal data is a fundamental right⁴⁷⁹. In May 2018, the new EU Data Protection Regulation 2016/679, the General Data Protection Regulation, entered into force. Also, data protection in Italy is governed by Legislative Decree 30 June 2003 no. 196, known as the Personal Data Protection Code (hereinafter PDPC), amended by Legislative Decree 10 August 2018 no. 101 to harmonize national legislation with the GDPR. The main purpose of data protection law is to provide effective remedies for ensuring extensive personal data rights protection.

5.1. Data breach remedies in the Italian legal system

The GDPR and the PDPC set out the framework of remedies in case of unlawful processing of personal data. Under Article 140-a of the PDPC, the data subject has the right to lodge a complaint with the data protection authority and with the ordinary judicial authority. In the first place, the data subject may complain to the Italian DPA⁴⁸⁰ and should provide an illustration of the facts and circumstances on which the request is based, provisions allegedly infringed and measures required, the identification details of the controller or processor, and the documentation⁴⁸¹. The DPA could reject a manifestly unfounded complaint, otherwise shall decide within nine months from the date of submission and, in any case, shall inform the data subject about the status of proceedings within three months. In certain circumstances, the DPA shall decide within twelve months, in presence of justified preliminary investigation requirements⁴⁸². Moreover, Articles 78 and 79 of the GDPR state that every data subject whose rights have been infringed shall have access to an effective judicial remedy. Such remedies typically consist of procedural tools to achieve correction, erasure, and also damages. Following Article 152, paragraph 1 of the PDPC, all disputes concerning the matters covered by the judicial appeals referred to Articles 78 and 79 of the GDPR are attributed to the ordinary judicial authority. Moreover,

⁴⁷⁷ Independent administrative authority established by the Law of 31 December 1996, no. 675, and then confirmed as the supervisory authority pursuant to Article 51 of the GDPR.

⁴⁷⁸ Art. 143, paragraph 3, Legislative Decree no. 196/2003.

⁴⁷⁹ Regulation EU 2016/679 of 27 April 2016 on the protection of the natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Recital 1.

⁴⁸⁰ Legislative Decree 30 June 2003 n 196 the Personal Data Protection Code, art 141.

⁴⁸¹ *ibid*, art 142, paras 1 and 3.

⁴⁸² *ibid*, art 143 para 3.

based on paragraph 1-*bis* of Article 152, the juridical process is regulated by Article 10 of Legislative Decree 1st September of 2011 no. 150. According to this provision, the data breach litigation process is governed by the rules of the labour proceedings, in which the main idea is to ensure the parties' equality of arms.

5.2. The framework of fines and penalties

The GDPR sets out a system of penalties and administrative fines to ensure compliance with the requirements of EU and national data protection law. The two measures with the largest economic impact are Article 82 on damages and Article 83 on administrative fines of the GDPR. Under Article 82, a data subject who has suffered harm as a result of the unlawful processing of personal data has the right to receive compensation from the controller or processor for the harm suffered. In the context of data protection law, the administrative fine is an important part of the remedy system, whose goal is to protect persons with respect to the processing of data. The Italian Legislator maintained the system of fines provided by Article 83 of the GDPR and simultaneously amended the list of criteria for their application, namely in Article 166 of the PDPC. According to the provision of the GDPR, it is up to the national DPA to decide whether to issue such a fine and, if so, to determine its amount. Besides, the authority shall ensure to impose penalties in a manner that is effective, proportionate, and dissuasive⁴⁸³. Furthermore, it can be noted that Article 83 provides for a two-tiered system, in order to ensure that fines are applied on a broadly consistent and proportionate scale. The first tier may result in a fine of up to 10 million euros, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. The second tier could result in a fine of up to 20 million euros, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. However, administrative fines are not the only option; Article 58 of the GDPR offers a number of different other measures. The DPA can indeed issue warnings, reprimands, or orders, or withdraw certifications⁴⁸⁴. Moreover, it is a common practice for Italian DPA to impose fines accompanied by a corrective measure and the Cavauto s.r.l. case⁴⁸⁵ could be a good example. The DPA held that Cavauto s.r.l. accessed and processed personal data of its employee saved on the employee's business computer and failed to comply with the established principles of personal data protection. The employer dismissed the employee on the basis of the personal data found on the computer

⁴⁸³ Article 29 Data Protection Working Party, 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679' (2017) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237> accessed 2 March 2021.

⁴⁸⁴ Johanna Chamberlain, Jane Reichel, 'The relationship between damages and administrative fines in the EU General Data Protection Regulation' (SSRN, 7 September 2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3447854> accessed 20 February 2021.

⁴⁸⁵ Garante per la protezione dei dati personali, Order injunction against Cavauto s.r.l. of 26 March 2020 n 9446730 <<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9446730>> accessed 2 March 2021.

and refused to recognise the right of access to personal data. Applying Articles 57 and 58 of the GDPR, the DPA ordered the controller to comply with the employees request to access to the personal data and to bring its processing operations into compliance with Article 32. Moreover, a fine of 10.000 euros was imposed. Additionally, the PDPC provides for both administrative fines and criminal penalties. It lists causes of criminal offences provided by Articles 167, 167 – a, 167 – b, 168, 170, 171. Depending on the breach, the sanction is imprisonment in a range from six months to six years.

5.3 Concluding remarks

Finally, based on analysis of the system of remedies and penalties, it is evident the intention of the Italian and European Legislators to ensure effective protection to the data subject. Moreover, in the Italian legal framework, the principle of effectiveness is strengthened by Article 1 of Legislative Decree 2 July 2010 no. 104, which requires the legal system to provide a whole group of procedural safeguards to guarantee full protection to the person harmed by acts of public authorities. Nevertheless, the set of remedies and sanctions shall not be seen as the main and only instrument to guarantee the respect of the fundamental right to personal data protection, as the GDPR and the PDPC define a whole series of preventive measures for the safety of the processing and minimisation of risks⁴⁸⁶. Undoubtedly, EU and national law set out a strong system of remedies and unprecedented administrative fines, fundamentally changing the potential financial consequences of breaching data protection law⁴⁸⁷. However, it is complicated to ensure the universal effectiveness of these instruments in all cases and for all scenarios. For this reason, their effectiveness should be assessed on a case-by-case basis.

6. What is the process of judicial review of anti-discrimination cases?

Italian anti-discrimination law consists in a complex legislative framework, resulting from a stratification of national and supranational rules. Its nature is relative: it depends on and should be conformed to the present historical and social context. Indeed, the legal debate on solutions in cases in which discrimination originates in technology is still developing; present issues reflect the lack of legislative innovation in the IT area, giving rise to errors in the systems that may amount to direct or indirect discrimination⁴⁸⁸.

⁴⁸⁶ Marco Orofino, *Ne bis in idem e sistema sanzionatorio nella disciplina della protezione dei dati personali dopo l'adozione del GDPR*, (2019) 4 Public Comparative and European Law 1139.

⁴⁸⁷ Detlev Gabel, Tim Hickman, 'Chapter 16: Remedies and sanctions – Unlocking the EU General Data Protection Regulation (*White & Case*, 5 April 2019) <<https://www.whitecase.com/publications/article/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection>> accessed 25 February 2021.

⁴⁸⁸ M. R. Carbone, *Se l'algoritmo è razzista: quali misure e norme a tutela dei soggetti deboli*, available at <<https://www.agendadigitale.eu/cultura-digitale/se-lalgoritmo-e-razzista-quali-misure-e-norme-a-tutela-dei-soggetti-deboli/>> accessed 25 February 2021.

6.1. The evolution of Italian Anti-discrimination Law and the boost of the available Legal Solutions

Until the end of the '90s, Italian discrimination cases were included almost exclusively within criminal law; only the most striking discriminations were punished, thus discouraging victims from bringing their cases before justice⁴⁸⁹. In this background of ineffectiveness, the role of civil law in anti-discrimination law was enhanced. Any discrimination case is resolved in the light of art. 3 of the Italian Constitution. Yet, in the latest decades, anti-discrimination law in general has experienced a progressive growth in its substance, especially from the perspective of the tools through which violations are contrasted. Commencing from the European framework, art. 14 of the European Convention of Human Rights (ECHR) guarantees equal treatment, while as to EU law, Directive 2000/43/EC, Directive 2000/78/EC and Recast Directive 2006/54/EC should be considered⁴⁹⁰. The first two were given execution respectively through Legislative Decree no. 215 and 216/2003⁴⁹¹, that contributed to the completion of the Italian anti-discrimination law by allocating it a general character, while the transposal of Recast Directive complemented the gender equality provisions⁴⁹².

As to judicial solutions, the reaction of the Italian Legislator to the lack of an effective protection lies in Arts. 43 and 44 of the Legislative Decree no. 286/1998⁴⁹³, as the Italian tool to comply with Directives 2000/43 and 2000/78, Arts. 7 and 9. Indeed, art. 44 enshrines the civil action against discrimination: when the behaviour of a private or public subject produces a discrimination on the ruled grounds, the appellant can resort to the ordinary judicial authority, to ask for the cessation of the harmful behaviour and the removal of its effects. To these controversies, the fast-track procedure ruled in art. 28 of Legislative Decree no. 150/2011 applies⁴⁹⁴. The remedies may involve non-pecuniary damages, the order for a removal plan of the verified discriminations, the order for the

⁴⁸⁹ B. Troisi, *Atti di discriminazione e mediazione*, in *Quaderni di conciliazione*, edited by Carlo Pilia, Cagliari, 2011, 23-41.

⁴⁹⁰ Council Directive 2000/43/EC; Council Directive 2000/78/EC; Directive 2006/54/EC (recast).

⁴⁹¹ Through Legislative Decree 9 July 2003, n. 215, transposing Directive 2000/43/EC and Legislative Decree 9 July 2003, n. 216, transposing Directive 2000/78/EC, specific procedural tools were addressed to cases involving discrimination on grounds of race, ethnic origin, religion, personal beliefs, disability, age and sexual orientation.

⁴⁹² Legislative Decree 25 January 2010, no. 5, transposing Directive 2006/54/EC (recast).

⁴⁹³ Legislative Decree of 25 July 1998, no. 286, Consolidated Act of Provisions concerning immigration, Arts. 43 and 44.

⁴⁹⁴ Legislative Decree of 1 September 2011, no. 150. This procedure is regulated by art. 702-bis, 702-ter and 702-quarter of the Italian Code of Civil Procedure. M. Minardi, *Il processo sommario di cognizione*, in *Procedura Civile*, Altalex, 2010. Available at:

<<https://www.altalex.com/documents/news/2010/03/25/il-processo-sommario-di-cognizione>> S.

Menchini, *L'ultima "idea" del legislatore per accelerare i tempi della tutela dichiarativa dei diritti: il processo sommario di cognizione*, in *Corr. Giur.*, 2009. M. Bove, *Il procedimento sommario di cognizione di cui agli articoli 702-bis ss. c.p.c., in Judicium. Il processo civile in Italia e in Europa*.

publication of the judgment on a daily national newspaper at the expense of the discriminating subject. Disputes on grounds of gender discrimination are also challengeable before the civil court under the ordinary procedure. art. 15 of Law 903/77 defines any discriminatory act as null and void⁴⁹⁵. In this realm, an urgency procedure was introduced for the employee before the Labour Court of the place where the discrimination occurred⁴⁹⁶. In cases in the workplace, victims can resort to conciliation procedures (art. 410 Code of Civil Procedure) or opt for an individual action before the Labour or Administrative Tribunal having jurisdiction on that territory.

6.2. Some remarks on the functioning of the Judicial Solutions

As to the effectiveness of the judicial review, critics to Italian anti-discrimination law focus on its complexity: the stratification among domestic and community rules has been defined as a “cold merger”, often ending up in legal uncertainty and therefore ineffectiveness of the rules in force⁴⁹⁷. Such procedures encounter the traditional shortcomings of anti-discrimination cases, such as the infrequency of litigation. Another gap is the distinct protection provided for in cases of gender discrimination and that for all the other grounds, with the risk of building a ranking among discriminations: the fast-track procedure differs from the urgency procedure allowed in cases of gender discrimination, which is effective for the tempestive removal of discriminations⁴⁹⁸.

6.3. The legal challenges in Anti-discrimination Law arising from IT Innovation

The impact that the IT systems may have on the enjoyment of the principle of equality is still under persistent observance. Since the engine enhancing the development of such systems consists in the huge amount of data at their disposal, the debate is focussed on the protection of personal data provided for in EU law. The GDPR, in recital 71, touches the principles to be followed in the data processing: in the realm of the data ‘profiling’, personal data should be secured “in a manner (...) that prevents, inter alia, discriminatory effects on natural persons (...)”⁴⁹⁹. The discriminatory effect is thus expected; wrong assumptions may lead to algorithmic biases: yet, the principle of non-discrimination is not envisaged in this Regulation. An algorithm may be built on already discriminatory data, that is the GIGO (‘garbage in garbage out’) principle: the developed algorithm will reflect the

⁴⁹⁵ Law of 9 December 1977, no. 903, Equal treatment between men and women in the workplace, Arts. 1 to 5 and 15.

⁴⁹⁶ Legislative Decree of 11 April 2006, no. 198, “Code of equal opportunities between man and woman, pursuant to Article 6 of the Law of 28 November 2005, no. 246”, art. 38.

⁴⁹⁷ M. Capponi, *Diritto antidiscriminatorio, fattore di rischio “nazionalità” e bandi di concorso nella pubblica amministrazione: l’ultimo approdo del giudice di merito*, in *Lavoro, Diritti, Europa. Rivista nuova di Diritto del Lavoro*, 2018, 10-12.

⁴⁹⁸ *ibid.*

⁴⁹⁹ Regulation (EU) 2016/679 (General Data Protection Regulation), recital 71.

quality of its data⁵⁰⁰. Jurists enclose the issue under the feature of “cognitive uncertainty” to underline the difficulties in regulating this field: technology supersedes the general comprehension, even the one of the Legislators⁵⁰¹. Solutions, which are developing, may be categorized in *a priori* and *ex post* solutions; as to those preceding the development of an algorithm, emphasis is put on private policies by companies producing software, with the final aim of a socially and legally sustainable governance of the net⁵⁰². The Guarantor Authorities hold a considerable role in this development. As to *ex post* solutions, they are generally deemed to be less effective: the inexistence of guidelines for developers constitutes a great lack in the system, which has risen, along years, the necessity for governments to trace a set of standards and preventive measures to guide the developers in the building of IT systems. Among such measures, education of the developers is relevant to instruct them on the legal issues that may arise⁵⁰³. Technologic development constitutes a challenge for the legal world, for which legal and IT experts shall cooperate in the view to set common standards and, in the case those standards are breached, an effective, upgraded and suitable judicial protection.

7. Does your country have any specific regulations on Advanced Digital Technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?

To comply with the General Data Protection Regulation (GDPR) the national legislator changed Legislative Decree no. 196/2003 (the Italian law on privacy) thorough Legislative Decree no. 101/2018: these are currently the main legislative reference texts on data protection to identify rules that can regulate the impact of some new emerging technologies on the right to privacy.

In the field of Artificial Intelligence⁵⁰⁴, there are two provisions that seek to regulate the effects of this new technology on people’s rights: Article 22 of the GDPR and Article 130 of Legislative Decree no. 196/2003. From the analysis of Article 22, it can be deduced the right of the data subject not to be subjected to a decision based solely on the automated processing of the data, and the right to obtain human intervention aimed at a new evaluation of the automated decision⁵⁰⁵. Under paragraph 4 of Article 22, the prohibition is

⁵⁰⁰ A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, n. 1/2019, 63-89.

⁵⁰¹ *ibid*, 86.

⁵⁰² Carbone (n 488).

⁵⁰³ *ibid*.

⁵⁰⁴ AI can be defined as a set of systems that show intelligent behaviour by analysing their environment and performing actions with a certain degree of autonomy to achieve specific objectives. F. Sarzana Di S. Ippolito and M. Nicotra, *Diritto della blockchain, intelligenza artificiale e IoT* (Milan, Wolters Kluwer Italy, 2018).

⁵⁰⁵ This second residual protection is also without prejudice to cases in which the data controller submits the data subject to an automated decision based on one of the exceptions provided for in the same Article 22, in cases where the fully automated processing is necessary for the conclusion or the execution of a contract, or

not derogable in the case of the processing of personal data⁵⁰⁶, unless they have been made public by the interested party or there is a significant public interest of the EU or of the States to which these have been subjected to automated processing. The rationale of this rule resides in the concern of the European legislator towards decisions having a strong impact on people's lives, and therefore potentially harmful, which are determined without the mediation of the reflective activity of man, but rather by the calculation of a machine. This reinforced protection of data subjects' rights is the result of the fear produced by the lack of absolute trust in 'dehumanised' decisions. Inevitably, this rule can be criticised considering that it is difficult to configure the hypothesis in which the human operator does not trust the computational capacity of the machine and assumes the responsibility of opting for a different or opposite decision: the result is the frustration of the protection abstractly guaranteed by Article 22 in its effective application⁵⁰⁷. The only provision of national law that follows this logic can be found in Article 130 of the Legislative Decree no. 196/2003: it provides for the need for the consent of the data subject for the use of totally automated call systems aimed at sending commercial communication⁵⁰⁸. In this case, the guarantee given by human intervention in automated personal data processing mechanisms is represented by the consent of the data subject. Also, in this case it is not difficult to criticise the rule due to an apparent protection considering that the consent of the data subject could hardly be configured as actually informed. Ultimately, now neither the European nor the national legislature seem to have issued rules capable of effectively protecting the rights of data subjects where the data is processed through automated systems.

7.1. Critical issues in GDPR compliance in Italy

The influence of European and international legislation has always represented a driving force towards national privacy legislation, starting with the Directive 95/46/EC based on which Legislative Decree 196/2003 was adopted, replacing the first Italian Privacy Law no. 675/1996⁵⁰⁹. Despite this tradition on the subject, it must be considered how the activity of adapting Italian legislation to the GDPR has been influenced by delays. The result was a very confusing legislation with various coordination problems that still exist: from the elimination of rules without their adequate replacement, to the presence of rules relating to

required by the laws of the Union or of a Member State (which also contain adequate measures to protect the rights, freedoms and legitimate interests of the person), or legally legitimised by the explicit consent of the interested party (founded on specific and detailed information according to the GDPR).

⁵⁰⁶ Personal Data are defined in Article 9 of GDPR.

⁵⁰⁷ F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Turin, G. Giappichelli Editore, 2018.

⁵⁰⁸ The only exception is provided for in paragraph 4 of Article 130 of Legislative Decree no. 196/2003, which provides for the possibility of sending commercial communications to users, who have purchased a specific good or service, containing information on similar products or services. to those previously purchased (soft-spam practice).

⁵⁰⁹ This law established the Italian National Authority for the Protection of Personal Data. Its first President was Professor Stefano Rodotà.

the areas in which the GDPR leaves decision-making autonomy to States that seem to be poorly integrated with the its general principles, passing through a general delegation to interpreters and the National Authority to assess the compatibility with the GDPR of the previous provisions. Another missed opportunity is represented by the figure of the DPO (Data Protection Officer)⁵¹⁰. With the GDPR this figure has become mandatory, but its actual implementation failed for the moment, considering the amount of appointments of subjects not suitable for this function by the data controllers. This phenomenon suggests that the figure of the DPO is considered more as a further bureaucratic fulfilment for the subjects obliged to its designation than as an opportunity to implement data protection measures and strategies.

7.2. The future EU regulation on AI and ePrivacy

Undoubtedly, the regulatory framework is destined to be more defined with further regulatory interventions aimed at regulating these technologies and impacting the right to data protection of European citizens. Among these interventions are of particular interest: resolutions no. A9-0186/2020 and A9-0178/2020⁵¹¹ by European Parliament, which are draft regulations for AI proposed to the EU Commission in October 2020, and the ePrivacy Regulation⁵¹², the European regulation on the processing of personal data and the protection of privacy in the electronic communications sector.

Regarding the proposed regulations on AI, the first regulation scheme affirms the need to build trust at all levels of society towards AI, robotics, and related technologies, particularly where these are considered high risk: the subjects who develop these technologies should be required to adopt an ethically oriented approach in this activity as it is focussed on respect for fundamental rights and human dignity, as well as to provide adequate transparency to citizens about the use of AI. An approach that would put the EU at the forefront of AI regulation⁵¹³.

⁵¹⁰ The most important GDPR Articles on DPO are arts 37 to 39.

⁵¹¹ The resolutions no. A9-0186/2020 is available here:

<https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html>The resolutions no. A9-0176/2020 is available here:

<https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_EN.html>.

⁵¹² The ePrivacy Draft Regulation is available here:

<<https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf>>.

⁵¹³ The second draft regulation is focussed on the civil liability regime in cases of damage caused using AI, and the third on its implications on intellectual property.

Regarding the so-called ePrivacy Regulation⁵¹⁴, this is going to have an important impact on technologies such as the IoT⁵¹⁵, and consequently on the Italian legislation. It aims to guarantee confidentiality in electronic communications and to define the cases in which service providers are authorised to process electronic communications data or to have access to data stored on users' devices. The ePrivacy Regulation tends to repeat the same approach as the GDPR where principles such as Privacy by Design, Privacy by Default and Accountability are central.

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?

The main feature of the "hacking by law enforcement" is to perform extensive surveillance, enabling investigators to "bypass physical barriers traditionally aimed to protect individuals and their privacy"⁵¹⁶. In particular, the indirect acquisition of data implies an online surveillance and raises more doubts about its compatibility with human fundamental rights⁵¹⁷.

The installation of a malware, a malicious software, on target electronic devices without the knowledge of the users permits to monitor their activity through the device. The Italian Legislator has chosen to allow only one of its possible uses: the recording of conversations between present people. According to the second paragraph of Article 266 of the Italian Criminal Procedure Code "wiretapping among present people may also take place by inserting a malware on a portable electronic device"⁵¹⁸.

As a result of the intrusive character of this investigative technique and the possible breaches of fundamental rights, the public prosecutor - in charge of the investigations - needs a special authorisation by the judge to use the malware tool, which is subjected to a forty-days length⁵¹⁹. In the request the prosecutor shall indicate the existence of two

⁵¹⁴ It is intended to replace the current Directive 2002/58/EC, which Italy has implemented in the Legislative Decree no. 196/2003. On 10 February, the EU Council approved its final draft to be presented to the EU Parliament as part of the approval process through negotiation between the EU Council and the EU Parliament, which can be found here:

<<https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf>>.

⁵¹⁵ Internet of Things (IoT) can be defined as the set of Internet connections managed by objects and places without the intervention of human operators, according to F. Sarzana Di S. Ippolito and M. Nicotra, *Diritto della blockchain, intelligenza artificiale e IoT*, Milan, Wolters Kluwer Italy, 2018.

⁵¹⁶ Michele Simonato, 'Defence rights and the use of information technology in criminal procedure' (2014), *Revue internationale de droit penal* 85 (1), 265.

⁵¹⁷ Most challenges are posed, but not limited, during pre-trial investigations.

⁵¹⁸ Art. 266, para 2-bis, c.p.p. The new regulation has been provided by Legislative Decree no. 216/2017 as amended by Legislative Decree 161/2019, converted in law no. 7/2020. And it shall apply to criminal proceedings registered after 31 August 2020.

⁵¹⁹ In urgent cases, indicated by Article 266 (2-bis) c.p.p., the prosecutor may order himself, with a motivated decree, the use of a malware; the compulsory validation of the investigating judge must occur within 48 hours.

conditions: serious clues of crime (the indication of liability is not required) and the indispensability of the measure for the prosecution of the investigations. The judge must indicate the reason that makes the use of a malware necessary⁵²⁰.

If such communications take place in domestic places, the use of the malware is allowed only if “there are good reasons to believe that the criminal activity is taking place there”⁵²¹.

The judge must also indicate the places and time of activation of the microphone through the malware.

Less restrictive requirements to the use of malware are provided for some specific crimes⁵²².

In order to guarantee the originality and integrity of the recordings, the operations are expected to be carried out exclusively by means of installed systems in the Public Prosecutor's Office. However, there is no legislative indication regarding the concrete ways of installing the malware in the target device.

The law provides that the malware shall be deactivated and made permanently unusable on recommendation of the judicial police at the end of the operations.

8.1. Hacking activities and software design

A malicious software “concentrates a plurality of tools in a single investigative act”, given a powerful mean to the public authority⁵²³. In this sense a relevant case is the Exodus malware. In March 2019, Security Without Borders published a test report on Exodus, a malware sold to the Ministry of the Interior and the Italian secret services to be used as spyware⁵²⁴. This malware used by the public authority showed several problems related to fundamental rights and the use of IT in criminal proceedings⁵²⁵. First and foremost, the Exodus case stressed the lack of regulation regarding the specific admissible installation's procedures of the malware⁵²⁶.

⁵²⁰ Art. 267 c.p.p.

⁵²¹ Art. 266, para 2 *bis* c.p.p.

⁵²² I.e. organised and terrorism crimes; specific crimes against the public administration.

⁵²³ Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico, 30 aprile 2019, available in <www.garanteprivacy.it> accessed 23 February 2021.

⁵²⁴ See Security Without Borders, Exodus: Nuovo Spyware per Android Made in Italy, available in <<https://securitywithoutborders.org/blog/2019/03/29/exodus-ita.html>, 29.3.2019> accessed 26 February 2021.

⁵²⁵ Francesca Palmiotto, ‘Captatori informatici e diritto alla difesa. Il caso Exodus.’ (2020) Giustizia Penale e Nuove tecnologie

<<http://www.la-legislazionepenale.eu/wp-content/uploads/2020/10/Palmiotto-Revisione-Finale.pdf>> accessed 21 February 2021, 6-10.

⁵²⁶ The law provides that only programs that comply with the technical requirements established by decree by the Ministry of Justice must be used for installation purposes. Exodus was being installed without a target validation procedure and it was hidden in popular applications available in the Google Store.

As mentioned, besides the recording of conversations between present people, the capability of such malware to decrypt the encrypted data, thus having access also to particularly sensitive data, is not regulated by Italian law. Some scholars consider the malware's activities comparable to evidence-seeking tools already governed by the law, stressing as essential whether the investigation is aimed at the acquisition of exchanged messages which have been stored locally or whether it is aimed at capturing messages in real time during their dispatch⁵²⁷. In the latter case, the wiretapping regulation shall apply.

According to others, non-regulated malware's activities could be lawful since the Italian criminal procedural system does not provide a principle of mandatory proof: the judge is expressly authorised to accept "proofs not regulated by law"⁵²⁸. Other scholars argue that, since the activities carried out by the malware can violate individual rights protected by Arts. 13 to 15 of the Italian Constitution (in particular, home intimacy and secrecy of communications), these are not allowed unless they are not strictly provided by the law⁵²⁹. This intent was shown by the Legislator, stating that a malware permits the execution of a "set of operations that technology allows to carry out, that the Legislator did not intend to regulate, limiting the scope of the regulatory intervention to regulate the aspects relating to audio-wiretapping"⁵³⁰.

The focus in this matter should be the design of the malware, as the Exodus case has shown. The lack of adequate technical specifications by the ministerial decrees, which should indicate in detail the technical characteristics of the malware, permits this tool to be designed, in practice, against the law. Thus, the potential illegality of its design could affect the legitimacy of the proof.

Finally, the use of malwares changed the relation between prosecution powers and defence rights⁵³¹. In order to exercise the right to be heard, the legal defence should be able to

⁵²⁷ Pierluigi Di Stefano, 'I Trojan horse nel processo penale' (2020) Giustizia insieme <<https://www.giustiziainsieme.it/it/diritto-processo-penale/1364-il-trojan-horse-nel-processo-penale?hitcount=0>> accessed 26 February 2021; Andrea Nocera, 'L'acquisizione delle chat whatsapp e messenger: intercettazione, perquisizione o sequestro?' (2018) Il Penalista <<https://ilpenalista.it/articoli/focus/lacquisizione-delle-chat-whatsapp-e-messenger-intercettazione-perquisizione-o>> accessed 25 February 2021; Roberto O. Valli, 'la perquisizione informatica e la perquisizione da remoto' (2018) Il Penalista <<https://ilpenalista.it/articoli/focus/la-perquisizione-informatica-e-la-perquisizione-da-remoto>> accessed 26 February 2021.

⁵²⁸ Art. 189 c.p.p.

⁵²⁹ In those matters the Italian law does not admit 'atypical' evidence and investigations. See Francesco Caprioli, "Il 'captatore informatico' come strumento di ricerca della prova in Italia" (2017), *Rev. brasileira dir. proc. pen.* 3 (2), 487-488.

⁵³⁰ 'Relazione Illustrativa al d.lgs. 216/2017', available at <http://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0472bis_F001.pdf&leg=XVII> accessed 26 February 2021.

⁵³¹ Palmiotto (n 525) 17-22.

know the software and how it was actually used, since potential errors in the software design and its use will directly affect the “output”.

8.2. Procedural Safeguards

The investigative procedures take place under the supervision of the public prosecutor, also aiming to protect the privacy and reputation of the intercepted subjects, especially third parties unrelated to the proceeding.

The new Law no. 7/2020, aiming to better discipline the preventive selection of data and the omission of the transcripts of the acquired communications considered irrelevant, assigns a dual function to the public prosecutor, consisting in providing indications to what conversations should not be transcribed as well as to ensure that this happens (“surveil and ensure”)⁵³². Not only conversations relating to sensitive data should not be transcribed, but not even those containing expressions capable of damaging the reputation of the subjects involved⁵³³. Although, the lack of a procedural sanction and the breadth of the selection standard could make the provision useless to avoid a potential violation of the rights of third parties involved⁵³⁴. The judge can eventually dispose a hearing aimed to the removal of the material regarding some personal data or unlawfully acquired, to which the public prosecutor and the legal defence have the right to participate⁵³⁵.

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?

9.1. The issue of digital divide in the Italian legislative debate

The COVID-19 pandemic has stressed the issues related to digital innovation Italy has been facing in the past few years and showed the gaps of the country’s legislation in this area. Among others, the digital divide has proved to be one of the aspects in need of a solid State intervention, especially in consideration of the role that internet access played during the recent lockdown.

According to the findings of the Italian National Institute of Statistics (ISTAT) Annual Report 2020, in terms of digital divide Italy is still in a position of disadvantage in relation

⁵³² See Corte Suprema Di Cassazione, Ufficio Del Massimario e del Ruolo, ‘Relazione su novità normativa. La legge 28 febbraio 2020, n. 7, conversione in legge con modificazioni del Decreto Legge 30 dicembre 2019, n. 161, Modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni’, available in <https://www.sistemapenale.it/pdf_contenuti/1585594882_rel3520-ufficio-massimario-relazione-riforma-in-tercettazioni-decreto-161-2019-legge-7-2020.pdf> accessed 26 February 2021, 16-22.

⁵³³ Art. 268 (2-bis) c.p.p.

⁵³⁴ Corte Suprema Di Cassazione, Ufficio Del Massimario e del Ruolo (n 532).

⁵³⁵ Art. 268 (6) c.p.p.

to other advanced countries⁵³⁶. This clearly shows the lack of adequate public policies dealing with this theme, despite Article 2 of the Declaration of Internet Rights, issued by a Special Parliamentary Committee established by the Chamber of Deputies in 2014, states that internet access is “a fundamental right of all persons and a condition for their individual and social development”.⁵³⁷ This provision seems to have remained dead letter on the legislative level, although a bill was presented to the Senate in order to introduce measures aimed at expanding the presence of broadband services throughout the national territory⁵³⁸.

Except for this attempt, the Legislator strived to bridge this gap only in the occasion of the aforementioned COVID-19 emergency, by means of the *Cura Italia* Decree, introducing temporary measures “in order to increase the consumption of services on electronic communication networks”.⁵³⁹

9.2. The strategies adopted by the Italian Government to enhance the right to internet access

In the absence of a stable regulation, the efforts to strengthen the right to internet access need to be part of a wider digital agenda, whose implementation demands to be carried out by the government: under this perspective, in 2019 the Italian government established the Minister for Technological Innovation. Within its mandate, the Minister has outlined a strategy for the innovation and digital transformation of the country, based on three main challenges: the digitalisation of society, the innovation of the country, the sustainable and ethical development of society as a whole, according to the United Nations’ Sustainable Development Goals.⁵⁴⁰ Although well structured, the plan seems not to provide the population with efficient solutions in relation to the country’s digital divide, as it lacks a pattern of dialogue with regional and local institutions, in charge of enforcing the actions taken by the central government.

⁵³⁶ Italian National Institute of Statistics (ISTAT), Summary of the Annual Report 2020, presented on 3 July 2020, p. 15, available online at <https://www.istat.it/it/files//2020/09/Annual-Report-2020_Summary.pdf> accessed 9 February 2021.

⁵³⁷ Chamber of Deputies, Declaration of Internet Rights, adopted by the Committee for the Rights and Duties of the Internet on 28 July 2015, available online at <https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf> accessed 9 February 2021.

⁵³⁸ Senate of the Republic, XVII Legislature, Draft Law no. 1722, presented on 19 December 2014, available online at <<http://www.senato.it/service/PDF/PDFServer/BGT/00902175.pdf>> accessed 10 February 2021 [Italian].

⁵³⁹ Decree-Law no. 18 of 17 March 2020 (Measures to strengthen the National Health Service and economic support for families, workers and businesses related to the COVID-19 epidemiological emergency), art 82.

⁵⁴⁰ Italian Minister for Technological Innovation, Italy 2025. Strategy for the technological innovation and digitalization of the country, available online at <<https://assets.innovazione.gov.it/1610546390-midbook2025.pdf>> accessed 10 February 2021 [Italian].

Nonetheless, in this direction goes the National Strategy for Digital Skills, leading to a cooperative approach upon four areas of intervention: education, active workforce, ICT specialist skills and citizenship, aiming to reduce the gaps both on the domestic and European levels⁵⁴¹. One of the main problems connected to the digital divide is to be found in the lack of infrastructures, which marks the greatest difference between Northern and Southern Italy, where most families struggle to access the internet.

This situation leads to a widespread digital illiteracy, representing a severe obstacle to the country's economic development. This is the reason behind the choice to invest approximately 50 billion Euros of the NextGenerationEU funds in the areas of digitalisation, innovation, competitiveness and culture⁵⁴². Nonetheless, the focus of the plan only goes to the digitalisation of the public administration and the productive systems, despite the fact that a full digital transition is deemed to be one of its staples.

9.3. The search for a constitutional perspective in the wider protection of human rights online

Overall, the criticism of these policies concerns their method rather than their contents: the need for clear and detailed guidelines seemed not to be relevant in the political discourse and the only indications in terms of objectives to be achieved came from the European Union. Nevertheless, in the past few years progress has been slow: this is why Italy ranked 25th out of 28 EU Member States in the 2020 edition of the Digital Economy and Society Index (DESI), showing a consistent deficiency in terms of basic and advanced digital skills⁵⁴³. This proves the width of the revolution the country necessitates to overcome its "digital dark age": in this sense, a legislative framework is essential, as well as a significant involvement of the private sector.

Once again, it must be highlighted that it is not a matter of quantity, but quality of investments: resources must be allocated in an efficient, reasonable and proportionate manner, in full compliance with the principle of substantial equality expressed by Article 3, paragraph 2, of the Italian Constitution. Even though there have been several proposals of constitutional amendments aimed at introducing the right to internet access within the

⁵⁴¹ Italian Minister for Technological Innovation, National Strategy for Digital Skills, adopted on 21 July 2020, available online at <<https://assets.innovazione.gov.it/1610029655-dtd-1277-a-all1.pdf>> accessed 12 February 2021 [Italian].

⁵⁴² Italian Minister of Economy and Finance, National Recovery and Resilience Plan, latest draft presented on 12 January 2021, available online at <https://www.ansa.it/documents/1610403841219_Bozza_Recovery_01_Cover.pdf> accessed 15 February 2021 [Italian].

⁵⁴³ European Commission, Digital Economy and Society Index (DESI) 2020 Italy, published on 11 June 2020, available online at <https://ec.europa.eu/newsroom/dac/document.cfm?doc_id=66918> accessed 21 February 2021.

Fundamental Charter⁵⁴⁴, the provision that “it is the duty of the Republic to remove those obstacles of an economic or social nature which constrain the freedom and equality of citizens, thereby impeding the full development of the human person and the effective participation of all workers in the political, economic and social organization of the country”, combined with the rule stated in Article 2, under which “the Republic recognises and guarantees the inviolable rights of the person, both as an individual and in the social groups where human personality is expressed”, is by itself sufficient to consider the right aforementioned, as well as human rights online as a whole, fundamental in the Italian legal system, urging the Legislator to adopt at least the guidelines to be followed in the public institutions’ actions to reduce the country’s digital divide.

However, it currently seems that over this theme there still is a much bigger and more complex dispute, requiring a radical change in the national climate for political debate rather than just a deep perception of this particular situation.

10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the upcoming five years?

The brief overview carried out so far highlighted data of enormous importance from the perspective of the impact of Artificial Intelligence (hereinafter also “AI”) on human rights.

The convergence of AI and the Internet has a strong impact on fundamental rights in such a radical way, as to impose a revising of the entire *corpus* of human rights elaborated by modern constitutionalism⁵⁴⁵.

Since the General Data Protection Regulation (GDPR) came into force, automated decision-making that has a legal or equally significant effect on individuals shall be subjected to some form of human supervision. This requirement stems from the concern that AI systems can take decisions without adequate checks and balances⁵⁴⁶.

10.1. Human rights and technological challenges

⁵⁴⁴ The most popular proposal is to be ascribed to Stefano Rodotà, who suggested introducing within the Constitution the Article 21-*bis*, worded as follows: ‘Everyone shall have the same right to access the Internet on equal terms, using appropriate technologies that remove all economic and social barriers. The law shall establish the appropriate measures to prevent the violations of the rights referred to in the First Title of the First Part’. This formulation later formed part of the provision of Article 2 of the Declaration of Internet Rights, which it has been considered above.

⁵⁴⁵ Rodotà S., *Il mondo nella rete. Quali diritti, quali vincoli*, Laterza, Roma-Bari, 2014, 69.

⁵⁴⁶ See in this sense the EC, White Paper On Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020 available here <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0065&from=EN> .

Technological evolution is leading to the creation of an era in which the use of algorithms is increasingly invasive in our society.

The priority should be focusing on how to safeguard human rights and human dignity in this technological context. The right to life, the right to a fair trial and the presumption of innocence,⁵⁴⁷ the right to privacy and freedom of expression, the right to equality and non-discrimination and mass surveillance, are all affected by the intrusiveness of AI. Responding to the challenges associated with the algorithms used, especially on Internet platforms, is therefore one of the most important issues, which is why regulation is needed⁵⁴⁸. In the first place, given the changing nature of the Internet and its regulatory framework, it is unclear whether it is possible to extend the legal concepts or the existing frameworks to the use of new technologies or whether an *ad hoc* regulation of human rights able to adequately capture the ethical challenges posed by algorithms, is necessary.⁵⁴⁹

This is the issue that the Legislator, when thinking of common legislation on AI, should primarily consider.

Secondly, different roles and responsibilities should be identified whenever there is a human rights violation due to algorithmic decisions. Specifically, a sort of pyramid of responsibility should be envisaged in order to understand whether the person who programmed the algorithm, the operator of the algorithm or the human being who implemented the decision can be held responsible. And again, it should be considered, in a context aimed at mitigating risks, what are the effects of these automated decisions on human rights.⁵⁵⁰

10.2. AI regulations: hypothesis of protection

Looking ahead, there will be increasing attention on an appropriate legal framework to regulate the implementation of AI solutions as this is increasingly seen as a key

⁵⁴⁷ For the potential influences AI may have on the right to a fair trial when it is used in the courtroom see Ulenaers J., *The Impact of Artificial Intelligence on the Right to a Fair Trial: Towards a Robot Judge?*, Asian J Law Econ 2020, July 21, 2020; <<https://doi.org/10.1515/ajle-2020-0008>> and also Senden L., *EU non-discrimination law in the era of artificial intelligence : mapping the challenges of algorithmic discrimination*, in Bernitz U., Groussot X., Paju J. and De Vries S. (eds), *General principles of EU law and the EU digital order*, Alphen aan den Rijn, Kluwer Law International, 2020, 151-182.

⁵⁴⁸ An analysis on the ethical implications of AI technologies can be found here: The ethics of artificial intelligence: Issues and initiatives, Panel for the Future of Science and Technology, EPRS | European Parliamentary Research Service, March 2020; <[https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU\(2020\)634452_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf)>.

⁵⁴⁹ For a critical approach to regulation, see MacCarthy M., *AI needs more regulation, not less*, Center for Technology Innovation, 9 March 2020; <www.brookings.edu/research/ai-needs-more-regulation-not-less/>.

⁵⁵⁰ For an analysis on the study on the human rights dimensions of automated data processing techniques and possible regulatory implications please see Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, Committee of Experts on Internet Intermediaries (MSI-NET), Council of Europe, March 2018

requirement. The Council of Europe recognises the need for legislation and will propose a strategic agenda that will include regulation of AI.⁵⁵¹

This is the starting point. In order to assess and understand the human rights risks involved in the operation of automated decision-making systems, companies should implement a human rights due diligence.⁵⁵² This can represent a kind of Data Protection Impact Assessment⁵⁵³ on human rights, investigating the actual and potential impacts on individuals that the use of these systems may have, directly or indirectly, and preventing or mitigating the harms identified in these assessments.

One cogent solution would also be to implement a robust relationship between law and technologies with a strong connection to the design or engineering of technology, as well as how we specifically use that technology and the capabilities in our lives.

This means that national and European Legislators must take into account AI technologies, providing for the inclusion of technological assessments, rules and values useful to guarantee the respect for human rights and social orders.⁵⁵⁴ Furthermore, it is necessary to examine the pros and cons of the technology used, whether it will transform or breach these rules and values, which will require the involvement of different stakeholders.

The future goal will therefore be to ensure that AI technologies develop in such a way as to guarantee social principles based on the protection of the individual, as well as the ability to challenge the rules and adapt to the social context.⁵⁵⁵

10.3. Closing remarks: a future perspective

In the coming five years, there will be a wide range of legislative instruments applicable to AI. In fact, on European level, the Commission is promoting a robust European legal framework to regulate AI as a way forward to developing sound and trustworthy AI

⁵⁵¹ The Council of Europe recognises the need for legislation and will propose by 2028, a strategic agenda which will include AI regulation as one of the major challenges
<www.coe.int/en/web/artificial-intelligence/director-jan-kleijssen>.

⁵⁵² Working Group on the issue of human rights and transnational corporations and other business enterprises, United Nations General Assembly, 16 July 2018
<<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/224/87/PDF/N1822487.pdf?OpenElement>>.

⁵⁵³ See art. 35 GDPR.

⁵⁵⁴ EC, Liability for artificial intelligence and other emerging digital technologies, Expert Group on Liability and New Technologies, 2019
<<https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>>.

⁵⁵⁵ EC, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM 64 Feb. 19, 2020,
<https://ec.europa.eu/info/files/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics_en>.

technologies, by promoting a clear definition for AI to determine the scope of its application and accommodate technical progress.⁵⁵⁶

The complex relationship between AI and human rights reveals, in fact, important issues and specifically these concerns how to prevent technological innovation, increasingly frequent and accelerated, from translating into rights violations. Precisely, because of the existence of this risk, and in line with a risk-based approach, forms of preventive assessment on the impact of AI on human rights could be developed. Hence the regulation of AI, converging with the development of the Internet and affecting various spheres of law, shall be developed starting from a European level, through reflective legislation, capable of adapting promptly to technological innovations.⁵⁵⁷

Conclusion

At the end of this analysis, it blatantly emerges how the important issues concerning the protection of privacy could be related to the absence of adequate regulation and, in some cases, to a complete legislative void.

This inevitably leads to several problems, aroused also due to the pandemic situation, which underline how far the legal framework is from a full and conscious protection of digital data in this era of Advanced Digital Technologies.

The formal European Legislator's intention to protect the right to privacy is also endorsed by the fact that, having become "disembodied entities", people need protection referring to their "digital body"⁵⁵⁸. The digital body's concept involves in a certain way a vision that shall be maintained when it comes to the concept of privacy and its protection as a fundamental right. A vision that turns into an inevitable precondition for data protection's activity and no longer a secondary purpose to pursue respecting the formal requirements. Nonetheless, the Legislator's intention is also to have a major impact, especially from a sanctioning point of view, on the leading figures who hold the individual's data: multinational companies⁵⁵⁹. The huge impact that multinationals have when it comes to privacy introduces the debate on what type of protection is the best guarantee from the point of view of the persons concerned: an *ex ante* or an *ex post* protection. At this point, a

⁵⁵⁶ EC, Artificial intelligence – ethical and legal requirements, COM June 2020, <<https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Requirements-for-Artificial-Intelligence>>.

⁵⁵⁷ Mark Lyon H., Gearing Up For The EU's Next Regulatory Push: AI, LA & SF Daily Journal Oct. 11, 2019 <<https://www.gibsondunn.com/wp-content/uploads/2019/10/Lyon-Gearing-up-for-the-EUs-next-regulatory-push-AI-Daily-Journal-10-11-2019.pdf>>.

⁵⁵⁸ Rodotà S., *Il diritto di avere diritti*, Roma-Bari, 2012, 395.

⁵⁵⁹ Borrillo B., *La tutela della "privacy" e le nuove tecnologie: il principio di "accountability" e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, in *dirittifondamentali.it*, 2020, 2, 326-356.

reminder about the rights of the personality and the instruments that the legal system provides for its protection is needed. The reparation of damages concerning the rights of the personality arises in quite different terms from other subjective situations since the injury suffered is not likely to be replenished in a specific form by restoring the situation before the injury: the previous situation cannot be restored only with an equivalent in monetary terms. Additionally, the inadequacy of the protection following the injuries, especially the ones without economic connotation, is evident.

All of this taken into consideration, the *ex post* protection appears to be the most common one, both because in some cases it is not possible to provide preventive protection and because the sector's technicians guidelines to refer to when it comes to data treatment regulation remain ambiguous. The accountability principle was introduced in order to prevent ambiguous situations and it ensured a possible perspective of prevention of the damage. This principle is the expression of the transition from a reparatory approach, which is the center of Directive 95/46/CE, to a preventive approach, based on the new Regulation ⁵⁶⁰. Keeping in mind all said above, the data protection's concept could appear as evanescent, necessarily leading to a compromise between the individual, whose data must be protected, and the services offered, for which that same data is required.

A striking parallelism can be made with Hobbes's *Leviathan*. In his book, Hobbes argued that the state of nature - the situation of war of all against all - could be avoided only by the presence of a strong government holding all the power over the citizens. People would have stripped themselves of their freedom in exchange for their security: a compromise⁵⁶¹. The parallelism with present days lies in the fact that personal data needs to be given for access to certain services, inevitable for the survival of the human being, seen as a 'social' being, but the knowledge of how data is treated is overshadowed.

Therefore, it is crucial to focus on how to improve this law's deficiencies. The legal framework is called to evolve, since especially ADT requires legal regulation to play an effective preventive role, thus it avoids the emergence of conflicts and consequent litigation.

The aim of the doctrine is to understand how the law can and shall regulate this new era, guiding and directing emerging technologies towards fundamental values, freedoms and rights of subjects, however keeping in mind that beyond ADT there is a human-based idea of innovation and a human contribution. It is crucial to maintain the role of individuals as a guide to avoid the realisation of disturbing techno-determinist visions where the machine replaces the human decision. Thus, the law of technology needs to be incorporated into

⁵⁶⁰ *ibid.*

⁵⁶¹ For more details, *Leviathan*. Revised Edition, eds. *A.P. Martinich and Brian Battiste*. Peterborough, on: *Broadview Press*, 2010. ISBN 978-1-55481-003-1.

the technique to provide a suitable direction to ensure the effectiveness of the principles and rules which guide the legal framework in order to create a synergy between the legal world and the technical world⁵⁶². Moreover, a model of law in technology is inherent in the proactive and preventive approach present in the European legislation on the protection of personal data: the data protection by design and by default's principles in which the law uses technology to ensure the protection of the dignity and development of the person. In this regard, together with technology, which implemented the law, it is necessary to rely on transparency until reaching the rights of knowability, comprehensibility and unionability. 'In this way technology can maintain and respect its function as a 'servant' instrument concerning the human being and his decisions, especially where they affect rights and freedoms'.⁵⁶³ In conclusion, in order to achieve these goals, the incorporation of law into technology, so for the former to be the means to obtain the comprehensibility and contestability of the latter and to empower human rights, has become of primary importance.

⁵⁶² Faini F, *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in *federalismi.it*, 2020, 16, 79-117.

⁵⁶³ *ibid.*

Table of legislation

Provision in Italian	Corresponding translation in English
Codice di Procedura Penale, Articolo 266, Comma 2 e 2-bis. Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa. 2-bis. L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater, e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4.	Italian Criminal Procedure Code, Article 266, Paragraphs 2 and 2-bis. In the same cases (of paragraph 1), the wiretapping of communications between those present is allowed, and can also be performed by inserting a malware on a portable electronic device. However, if these take place in the places indicated by article 614 of the criminal code, wiretapping is allowed only if there is a well-founded reason to believe that the criminal activity is taking place there. 2-bis. The wiretapping of communications between those present by inserting a malware on a portable electronic device is always permitted in the proceedings for the crimes referred to in Article 51, paragraphs 3-bis and 3-quater, and, subject to the indication of the reasons justifying the use also in the places indicated in Article 614 of the Criminal Code, for the crimes of public officials or persons in charge of public service against the public administration for which the penalty of imprisonment of not less than five years, determined in accordance with Article 4.
Costituzione Italiana, Articolo 2. La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale.	Italian Constitution, Article 2. The Republic recognises and guarantees the inviolable human rights, be it as individuals or as social groups which express their personality, and it requests the performance of the unalterable duty to social, economic, and political solidarity.

Costituzione Italiana, Articolo 3. Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla distinzione di sesso, razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese.	Italian Constitution, Article 3. All citizens have equal social dignity and are equal before the law, without distinction of gender, race, language, religion, political opinion, personal and social conditions. It is the duty of the Republic to remove those obstacles of an economic or social nature which constrain the freedom and equality of citizens, thereby impeding the full development of the human person and the effective participation of all workers in the political, economic and social organisation of the country.
Costituzione Italiana, Articolo 14. Il domicilio è inviolabile. Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale. Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali.	Italian Constitution, Article 14. The domicile is inviolable. Inspections, searches or seizures may not be carried out except in the cases and in the manner set out by law and in accordance with the guarantees prescribed for the safeguard of personal freedom. Controls and inspections for reasons of public health and safety or for economic and taxation purposes are regulated by special laws.
Costituzione Italiana, Articolo 15. La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.	Italian Constitution, Article 15. The freedom and confidentiality of correspondence and of every other form of communication is inviolable. Restrictions thereto may be imposed only by a reasoned warrant issued by a judicial authority with the guarantees established by law.
Costituzione Italiana, Articolo 117, Comma I.	Italian Constitution, Article 117, Paragraph I.

La potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali.	Legislative powers shall be vested in the State and the Regions in compliance with the Constitution and with the constraints deriving from EU legislation and international obligations.
Decreto-Legge 17 marzo 2020, n. 18 (Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19), Articolo 82: 1. Dalla data di entrata in vigore del presente decreto e fino al 30 giugno 2020, al fine di far fronte alla crescita dei consumi dei servizi e del traffico sulle reti di comunicazioni elettroniche è stabilito quanto segue. 2. Le imprese che svolgono attività di fornitura di reti e servizi di comunicazioni elettroniche, autorizzate ai sensi del Capo II del D.Lgs n. 259/2003 e s.m.i., intraprendono misure e svolgono ogni utile iniziativa atta a potenziare le infrastrutture e a garantire il funzionamento delle reti e l'operatività e continuità dei servizi. 3. Le imprese fornitrici di servizi di comunicazioni elettroniche accessibili al pubblico adottano tutte le misure necessarie per potenziare e garantire l'accesso ininterrotto ai servizi di emergenza. 4. Le imprese fornitrici di reti e servizi di comunicazioni elettroniche soddisfano qualsiasi richiesta ragionevole di miglioramento della capacità di rete e della qualità del servizio da parte degli utenti, dando priorità alle richieste provenienti dalle strutture e dai settori ritenuti “prioritari” dall'unità di emergenza della PdC o dalle unità di crisi regionali. 5. Le imprese fornitrici di reti e servizi di comunicazioni elettroniche accessibili al pubblico sono imprese di pubblica utilità e assicurano interventi di potenziamento e	Decree-Law no. 18 of 17 March 2020 (Measures to strengthen the National Health Service and economic support for families, workers and businesses related to the COVID-19 epidemiological emergency), Article 82: 1. Starting from the effective date of entering into force of this Decree up to 30 June 2020, in order to increase the consumption of services on electronic communication networks, the following provisions are laid down. 2. Companies providing electronic communications networks and services, authorized under Chapter II of the Legislative Decree No. 259/2003, as subsequently amended and supplemented, shall take measures and shall carry out any useful initiative aimed at strengthening the infrastructure and ensuring the functioning of networks and the operation and continuity of services. 3. Companies providing electronic communications services available to the public shall take all necessary measures to enhance and ensure uninterrupted access to emergency services. 4. Companies providing electronic communications networks and services shall satisfy any reasonable request by users for the improvement of network capacity and service quality, giving priority to requests from the structures and areas regarded as having “priority” by the PdC emergency unit or by regional crisis units. 5. Companies providing electronic communications networks and services

manutenzione della rete nel rispetto delle norme igienico-sanitarie e dei protocolli di sicurezza anti-contagio. 6. Le misure straordinarie, di cui ai commi 2, 3 e 4 sono comunicate all'Autorità per le garanzie nelle comunicazioni che, laddove necessario al perseguimento delle finalità di cui al presente articolo e nel rispetto delle proprie competenze, provvede a modificare o integrare il quadro regolamentare vigente. Dal presente articolo non derivano nuovi o maggiori oneri per la finanza pubblica.	available to the public are considered as public utilities companies and they shall ensure network upgrade and maintenance works in compliance with health and hygiene standards and anti-accounting security protocols. 6. The extraordinary measures referred to in paragraphs 2, 3 and 4 shall be communicated to the Italian Communications Authority which, where necessary to achieving the purposes referred to in this Article and in compliance with its powers, shall amend or supplement the existing regulatory framework. No new or increased public finance burden shall arise from this Article.
Decreto Legislativo n. 101 del 10 agosto 2018, Articolo 17: L'articolo 10 del decreto legislativo 1° settembre 2011, n. 150, è sostituito dal seguente: «art. 10 (Delle controversie in materia di applicazione delle disposizioni in materia di protezione dei dati personali). 1. Le controversie previste dall'articolo 152 del decreto legislativo 30 giugno 2003, n. 196, sono regolate dal rito del lavoro, ove non diversamente disposto dal presente articolo. 2. Sono competenti, in via alternativa, il tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero il tribunale del luogo di residenza dell'interessato. 3. Il ricorso avverso i provvedimenti del Garante per la protezione dei dati personali, ivi compresi quelli emessi a seguito di un reclamo dell'interessato, è proposto, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento ovvero entro sessanta giorni se il ricorrente risiede all'estero.	Legislative Decree no. 101 of 10 August 2018, Article 17: Article 10 of the legislative decree 1 September 2011, n. 150, is replaced by the following: «art. 10 (Of disputes concerning the application of provisions on the protection of personal data). 1. The disputes provided for by Article 152 of legislative decree no. 196, are governed by the rite of labour, unless otherwise provided for in this article. 2. Alternatively, the court of the place where the data controller resides or has its headquarters or the court of the place of residence of the interested party are competent. 3. The appeal against the provisions of the Guarantor for the protection of personal data, including those issued following a complaint by the interested party, is proposed, under penalty of inadmissibility, within thirty days from the date of communication of the provision or within sixty days if the applicant resides abroad. 4. Once the deadline foreseen for the decision of the complaint by Article 143, paragraph 3,

4. Decorso il termine previsto per la decisione del reclamo dall'articolo 143, comma 3, del decreto legislativo n. 196 del 2003, chi vi ha interesse può, entro trenta giorni dalla scadenza del predetto termine, ricorrere al Tribunale competente ai sensi del presente articolo. La disposizione di cui al primo periodo si applica anche qualora sia scaduto il termine trimestrale di cui all'articolo 143, comma 3, del decreto legislativo n. 196 del 2003 senza che l'interessato sia stato informato dello stato del procedimento. 5. L'interessato può dare mandato a un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di esercitare per suo conto l'azione, ferme le disposizioni in materia di patrocinio previste dal codice di procedura civile. 6. Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni. 7. L'efficacia esecutiva del provvedimento impugnato può essere sospesa secondo quanto previsto dall'articolo 5. 8. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio. 9. Nei casi in cui non sia parte in giudizio, il Garante può presentare osservazioni, da rendere per iscritto o in udienza, sulla controversia in corso con riferimento ai	of the legislative decree no. 196 of 2003, whoever has an interest in it may, within thirty days of the expiry of the aforementioned term, appeal to the competent Court pursuant to this Article. The provision referred to in the first period also applies if the quarterly term referred to in the Article 143, paragraph 3, of the legislative decree no. 196 of 2003 has expired without the interested party having been informed of the state of the procedure. 5. The interested party can give a mandate to a third sector body subject to the discipline of the legislative decree 3 July 2017, no. 117, which is active in the field of protection of the rights and freedoms of the interested parties with regard to the protection of personal data, to exercise the action on its behalf, without prejudice to the provisions on legal aid provided for by the code of civil procedure. 6. The judge sets the hearing for the parties to appear with a decree which assigns the appellant the peremptory term within which to notify the other parties and the Guarantor. No less than thirty days elapse between the day of notification and the appearance hearing. 7. The enforceability of the contested provision may be suspended in accordance with the provisions of Article 5. 8. If the appellant does not appear at the first hearing without alleging any legitimate impediment, the judge orders the cancellation of the case from the register and declares the termination of the trial, charging the appellant with the court costs. 9. In cases where he is not a party to the trial, the Guarantor may submit observations, to be made in writing or at a hearing, on the ongoing dispute with reference to the profiles relating to the protection of personal data. The judge orders that the Guarantor be notified about the pending dispute, by sending a copy of the introductory documents, in

profili relativi alla protezione dei dati personali. Il giudice dispone che sia data comunicazione al Garante circa la pendenza della controversia, trasmettendo copia degli atti introduttivi, al fine di consentire l'eventuale presentazione delle osservazioni. 10. La sentenza che definisce il giudizio non e' appellabile e può prescrivere le misure necessarie anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile dei dati, nonché il risarcimento del danno.”	order to allow the possible submission of observations. 10. The sentence defining the judgment cannot be appealed and may prescribe the necessary measures even in derogation of the prohibition referred to in article 4 of the law of 20 March 1865, no. 2248, attachment E), also in relation to any act of the public entity controller or responsible for the data, as well as compensation for damage.
Decreto legislativo n. 150 del 2 luglio 2011, Articolo 10: 1. Le controversie previste dall'articolo 152 del decreto legislativo 30 giugno 2003, n. 196, sono regolate dal rito del lavoro, ove non diversamente disposto dal presente articolo. 2. E' competente il tribunale del luogo in cui ha la residenza il titolare del trattamento dei dati, come definito dall'articolo 4 del decreto legislativo 30 giugno 2003, n. 196. 3. Il ricorso avverso i provvedimenti del Garante per la protezione dei dati personali è proposto, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito, ovvero entro sessanta giorni se il ricorrente risiede all'estero. 4. L'efficacia esecutiva del provvedimento impugnato può essere sospesa secondo quanto previsto dall'articolo 5. 5. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.	Legislative Decree no. 150 of 2 July 2011, Article 10: 1. Any disputes as per Article 152 of legislative decree no. 196 dated 30 June 2003 shall be regulated in accordance with the procedural arrangements applying to cases on employer-employee relationships except where provided otherwise in this Article. 2. Jurisdiction shall lie with the court of the place where the data controller is resident pursuant to the definitions contained in Article 4 of legislative decree no. 196 dated 30 June 2003. 3. Under penalty of inadmissibility, any provision by the Italian data protection authority shall be challenged by filing a petition within thirty days as from the date on which the said provision was notified or the relevant complaint was tacitly dismissed; the deadline shall be sixty days if the petition is filed by an entity residing abroad. 4. Enforcement of a provision that has been challenged may be staid in accordance with Article 5. 5. Should the petitioner fail to appear on the first day in court without alleging any legitimate impediment, the judge shall order

6. La sentenza che definisce il giudizio non è appellabile e può prescrivere le misure necessarie anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile dei dati, nonché il risarcimento del danno.	that the case be struck off the list and declare that the relevant proceeding is extinguished, and also award legal costs to the petitioner. 6. The judgment issued by the court may not be appealed and may order that the necessary measures be taken partly by derogating from the prohibition set forth in Article 4 of Law no. 2248 dated 20 March 1865, Annex E, as also related to any acts by public bodies in their capacity as either data controllers or data processors, and may award damages.
Decreto Legislativo n. 104 del 2 luglio 2010, Articolo 1: 1. La giurisdizione amministrativa assicura una tutela piena ed effettiva secondo i principi della Costituzione e del diritto europeo.	Legislative Decree no. 104 of 2 July 2010, Article 1: 1. Administrative jurisdiction ensures full and effective protection according to the principles of the Constitution and European law.
Decreto Legislativo n. 198 dell'11 aprile 2006, art. 38 Provvedimento avverso le discriminazioni, paragrafo 1: 1. Qualora vengano posti in essere comportamenti diretti a violare le disposizioni di cui all'articolo 27, commi 1, 2, 3 e 4, e di cui all'articolo 5 della legge 9 dicembre 1977, n. 903, su ricorso del lavoratore o per sua delega delle organizzazioni sindacali o della consigliera o del consigliere di parità provinciale o regionale territorialmente competente, il tribunale in funzione di giudice del lavoro del luogo ove è avvenuto il comportamento denunciato, nei due giorni successivi, convoca le parti e assume sommarie informazioni, se ritenga sussistente la violazione di cui al ricorso, oltre a provvedere, se richiesto, al risarcimento del danno anche non patrimoniale, nei limiti della prova fornita, ordina all'autore del comportamento denunciato, con decreto motivato ed immediatamente esecutivo, la cessazione del comportamento illegittimo e la rimozione degli effetti.	Legislative Decree no. 198, 11 April 2006, Article 38, para. 1: 1. In case behaviours directed at violating the provisions of art. 27, commas 1, 2, 3 and 4, and of art. 5 of the Law of 9 December 1977, no. 903, on the complaint by the worker or on its proxy to trade unions or the municipal or regional councilor for equality territorially competent, the tribunal acting as labour tribunal of the place in which the denounced behaviour occurred, in the two subsequent days, once the parties have been summoned and hearings are carried out, if he/she considers that the denounced violation occurred, apart from foreseeing, if required, also the non-pecuniary compensation, in the limits of the provided proof, he/she orders to the perpetrator of the denounced behaviour, with motivated and immediately executive decree, the cessation of the illegal behaviour and the removal of its effects.
Decreto Legislativo n. 70 del 9 aprile 2003, articolo 16:	Legislative Decree no. 70 of 9 April 2003, Article 16:

1. Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.	1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the provider is not liable for the information stored at the request of the recipient of the service, on condition that: a) has no actual knowledge of the illegal activity or information, and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; b) once made aware of the illegal nature of the activity or information, upon notice of the competent authorities, acts expeditiously to remove or disable access to the illegal material.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 1: Chiunque ha diritto alla protezione dei dati personali che lo riguardano.	Legislative Decree no. 196 of 30 June 2003, Article 1: Anyone has the right to the protection of personal data concerning him.
Decreto Legislativo 196/2003, Articolo 2-septies. Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute 1. In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo. 2. Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 è adottato con cadenza almeno biennale e tenendo conto: a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;	Legislative Decree 196/2003, Article 2-septies. Safeguards applying to the processing of genetic data, biometric data, and data relating to health 1. Pursuant to Article 9(4) of the Regulation, genetic data, biometric data and data relating to health may be processed if one of the conditions mentioned in paragraph 2 of the said Article is fulfilled and in compliance with the safeguards set out by the Guarantor in accordance with this Article. 2. The provision setting out the safeguards referred to in paragraph 1 shall be adopted at least every other year by taking account of the following: a. The guidelines, recommendations and best practices published by the European data protection board and the best practices concerning the processing of personal data; b. The scientific and technological developments in the sector addressed by the safeguards;

b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure; c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea. 3. Lo schema di provvedimento e' sottoposto a consultazione pubblica per un periodo non inferiore a sessanta giorni. 4. Le misure di garanzia sono adottate nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, del Regolamento, e riguardano anche le cautele da adottare relativamente a: a) contrassegni sui veicoli e accessi a zone a traffico limitato; b) profili organizzativi e gestionali in ambito sanitario; c) modalità per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute; d) prescrizioni di medicinali. 5. Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle specifiche finalità del trattamento e possono individuare, in conformità a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento di tali dati e' consentito. In particolare, le misure di garanzia individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonimizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati. 6. Le misure di garanzia che riguardano i dati genetici e il trattamento dei dati relativi alla salute per finalità di prevenzione, diagnosi e cura nonché quelle di cui al comma 4, lettere b), c) e d), sono adottate sentito il Ministro della salute che, a tal fine, acquisisce il parere del Consiglio superiore di sanità. Limitatamente ai dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il	c. The interest in the free movement of personal data in the EU. 3. The draft of the aforementioned provision shall be subjected to a public consultation for a period of at least sixty days. 4. The safeguards shall be adopted in compliance with Article 9(2) of the Regulation and also concern the precautions to be taken with regard to the following: a. Vehicle permit stickers and accesses to restricted access areas; b. Organisational and management issues in healthcare; c. Arrangements to directly inform data subjects of diagnoses and data relating to their health; d. Drug prescriptions. 5. The safeguards shall be adopted in respect of each category of personal data as per paragraph 1 by having regard to the specific purposes of the processing and may lay down, pursuant to paragraph 2, additional conditions to be fulfilled for the processing of the said data to be allowed. In particular, the safeguards in question shall set out the security measures including encryption and pseudonymisation techniques, minimisation measures, the specific arrangements to enable selective access to the data and provide information to data subjects, and such additional measures as may be necessary to safeguard data subjects' rights. 6. The safeguards concerning genetic data and the processing of data relating to health for prevention, diagnosis and treatment purposes as well as the safeguards referred to in paragraph 4, letters b) and c) above shall be adopted after hearing the Ministry of Health, which shall obtain, for that purpose, an opinion from the Consiglio Superiore di Sanità (Higher Council for Health Care). As regards genetic data, the safeguards may provide for relying on the data subject's consent as an additional measure to protect the data subject's rights in case a particular high risk

consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'articolo 9, paragrafo 4, del regolamento, o altre cautele specifiche. 7. Nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, e' ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia di cui al presente articolo. 8. I dati personali di cui al comma 1 non possono essere diffusi.	exists, pursuant to Article 9(4) of the Regulation, or set out any additional specific precautions. 7. Biometric data may be used with regard to the procedures enabling physical or logical access to data by authorised entities, by having regard to the obligations mentioned in Article 32 of the Regulation, in accordance with personal data protection principles and providing the safeguards referred to in this Article are complied with. 8. The personal data mentioned in paragraph 1 may not be disseminated.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 2-undecies: 1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto: a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio; b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive; c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione; d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità; e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria; f) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre	Legislative Decree no. 196 of 30 June 2003, Article 2-undecies: 1. The rights referred to in Articles 15 to 22 of the Regulations cannot be exercised with a request to the data controller or with a complaint pursuant to Article 77 of the Regulations if the exercise of these rights could result in an effective and concrete prejudice: a) interests protected under the provisions on money laundering; b) interests protected under the provisions on support for victims of extortion requests; c) the activity of parliamentary committees of inquiry established pursuant to Article 82 of the Constitution; d) activities carried out by a public entity, other than public economic entities, on the basis of an express provision of the law, for exclusive purposes relating to monetary and currency policy, the payment system, the control of intermediaries and credit and financial markets, as well as the protection of their stability; e) to carry out defensive investigations or to exercise a right in court; f) the confidentiality of the identity of the employee who reports pursuant to law no.

2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio. 2. Nei casi di cui al comma 1, lettera c), si applica quanto previsto dai regolamenti parlamentari ovvero dalla legge o dalle norme istitutive della Commissione d'inchiesta. 3. Nei casi di cui al comma 1, lettere a), b), d), e) ed f) i diritti di cui al medesimo comma sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del Regolamento. L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere a), b), d), e) ed f). In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'articolo 160. In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. Il titolare del trattamento informa l'interessato delle facoltà di cui al presente comma.	179, the offense of which he became aware by reason of his office. 2. In the cases referred to in paragraph 1, letter c), the provisions of parliamentary regulations or the law or the rules establishing the Commission of Inquiry apply. 3. In the cases referred to in paragraph 1, letters a), b), d), e) and f), the rights referred to in the same paragraph are exercised in accordance with the provisions of law or regulations governing the sector, which must at least bring measures aimed at regulating the areas referred to in Article 23, paragraph 2, of the Regulation. The exercise of the same rights may, in any case, be delayed, limited or excluded with motivated communication and made without delay to the interested party, unless the communication could compromise the purpose of the limitation, for the time and within the limits in which constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the data subject, in order to safeguard the interests referred to in paragraph 1, letters a), b), d), e) and f). In such cases, the rights of the interested party can also be exercised through the Guarantor in the manner referred to in Article 160. In this case, the Guarantor informs the interested party that it has carried out all the necessary checks or has carried out a review, as well as the right of the interested party to lodge a judicial appeal. The data controller informs the interested party of the faculties referred to in this paragraph.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 2-<i>duodecies</i>: 1. In applicazione dell'articolo 23, paragrafo 1, lettera f), del Regolamento, in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonché dinanzi al Consiglio superiore della magistratura e agli	Legislative Decree no. 196 of 30 June 2003, Article 2-<i>duodecies</i>: 1. In application of Article 23, paragraph 1, letter f), of the Regulation, in relation to the processing of personal data carried out for reasons of justice in the context of proceedings before the judicial offices of all levels and levels as well as before the Superior Council of the judiciary and other

altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalità previste dalle disposizioni di legge o di Regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento. 2. Fermo quanto previsto dal comma 1, l'esercizio dei diritti e l'adempimento degli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento possono, in ogni caso, essere ritardati, limitati o esclusi, con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, per salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari. 3. Si applica l'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo. 4. Ai fini del presente articolo si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonché i trattamenti svolti nell'ambito delle attività ispettive su uffici giudiziari. Le ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti.	self-governing bodies of the special judiciary or at the Ministry of Justice, the rights and obligations referred to in Articles 12 to 22 and 34 of the Regulation are governed within the limits and in the manner provided for by the provisions of law or Regulations governing such proceedings, in compliance with the provisions of Article 23, paragraph 2, of the Regulation. 2. Without prejudice to the provisions of paragraph 1, the exercise of the rights and the fulfillment of the obligations referred to in Articles 12 to 22 and 34 of the Regulation may, in any case, be delayed, limited or excluded, with motivated communication and made without delay to the interested party, unless the communication could compromise the purpose of the limitation, to the extent and for the time in which this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the interested party, to safeguard the independence of the judiciary and judicial proceedings. 3. Article 2-undecies, paragraph 3, third, fourth and fifth sentence applies. 4. For the purposes of this Article, the processing of personal data related to the judicial treatment of business and disputes, the treatments carried out in the field of legal and economic treatment of the judiciary staff, as well as the treatments carried out in the 'scope of inspection activities on judicial offices. The reasons of justice do not apply to the ordinary administrative-management activity of personnel, means or structures, when the secrecy of acts directly related to the judicial treatment of proceedings is not compromised.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 2- terdecies:	Legislative Decree no. 196 of 30 June 2003, Article 2-terdecies:

1. I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione. 2. L'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata. 3. La volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma. 4. L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3. 5. In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.	1. The rights referred to in Articles 15 to 22 of the Regulation referring to personal data concerning deceased persons can be exercised by those who have an interest of their own, or act to protect the interested party, as his agent, or for family reasons deserving of protection. 2. The exercise of the rights referred to in paragraph 1 is not permitted in the cases provided for by law or when, limited to the direct offer of information society services, the interested party has expressly prohibited it with a written declaration presented to the owner of the treatment or to the latter communicated. 3. The will of the interested party to prohibit the exercise of the rights referred to in paragraph 1 must be unequivocal and must be specific, free and informed; the prohibition may concern the exercise of only some of the rights referred to in the aforementioned paragraph. 4. The interested party has at any time the right to revoke or modify the prohibition referred to in paragraphs 2 and 3. 5. In any case, the prohibition cannot produce adverse effects for the exercise by third parties of the property rights arising from the death of the interested party as well as the right to defend their interests in court.
Decreto Legislativo n. 196 del 30 giugno 2003 Articolo 130.1: Fermo restando quanto stabilito dagli articoli 8 e 21 del decreto legislativo 9 aprile 2003, n. 70, l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso del contraente o utente. Resta in ogni caso fermo quanto previsto dall'articolo 1, comma 14, della legge 11 gennaio 2018, n. 5.	Legislative Decree no. 196 of 30 June 2003 Article 130.1: Without prejudice to the provisions of Articles 8 and 21 of the legislative decree 9 April 2003, no. 70, the use of automated call or call communication systems without the intervention of an operator for sending advertising or direct sales material or for carrying out market research or commercial communication is allowed with the consent of the contractor or user. In any case, the provisions of Article 1, paragraph 14, of the law of 11 January 2018, no. 5 remains valid

Articolo 130.4: Fatto salvo quanto previsto nel comma 1 , se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.	Article 130.4: Without prejudice to the provisions of paragraph 1, if the data controller uses the email coordinates provided by the interested party in the context of the sale of a product or service for the purposes of direct sales of their products or services, they may not request the consent of the interested party, provided that the services are similar to those being sold and the interested party, adequately informed, does not refuse such use, initially or on the occasion of subsequent communications. The interested party, at the time of collection and at the time of sending any communication made for the purposes referred to in this paragraph, is informed of the possibility of opposing the processing at any time, easily and free of charge.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 140 - bis: 1. Qualora ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati, l'interessato puo' proporre reclamo al Garante o ricorso dinanzi all'autorità giudiziaria. 2. Il reclamo al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, e' stata già adita l'autorità giudiziaria. 3. La presentazione del reclamo al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto, salvo quanto previsto dall'articolo 10, comma 4, del decreto legislativo 1° settembre 2011, n. 150.	Legislative Decree no. 196 of 30 June 2003, Article 140 - bis: 1. A data subject may lodge a complaint with the Guarantor or bring a proceeding before a judicial authority where he or she believes that any of the rights afforded by the legislation on personal data protection have been infringed. 2. A complaint with the Guarantor may not be lodged if a proceeding has already been brought before a judicial authority by the same parties and with regard to the same subject matter. 3. Lodging a complaint with the Guarantor shall prevent bringing an additional proceeding before a judicial authority by the same parties and with regard to the same subject matter, except as provided for in Article 10(4) of legislative decree no. 150 of 1 September 2011.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 141:	Legislative Decree no. 196 of 30 June 2003, Article 141:

1. L'interessato può rivolgersi al Garante mediante reclamo ai sensi dell'articolo 77 del Regolamento.	1. A data subject may lodge a complaint with the Guarantor in accordance with Article 77 of the Regulation.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 142: 1. Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare o del responsabile del trattamento, ove conosciuto. 2. Il reclamo è sottoscritto dall'interessato o, su mandato di questo, da un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati, con riguardo alla protezione dei dati personali. 3. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale mandato, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono. 4. Il Garante predispone un modello per il reclamo, da pubblicare nel proprio sito istituzionale, di cui favorisce la disponibilità con strumenti elettronici. 5. Il Garante disciplina con proprio regolamento il procedimento relativo all'esame dei reclami, nonché modalità semplificate e termini abbreviati per la trattazione di reclami che abbiano ad oggetto la violazione degli articoli da 15 a 22 del Regolamento.	Legislative Decree no. 196 of 30 June 2003, Article 142: 1. The complaint shall specify, in as detailed a manner as possible, the underlying facts and circumstances, the allegedly infringed provisions and the remedies sought and shall contain the identification data concerning the controller and the processor, if known. 2. The complaint shall be undersigned either by the data subject or by a non-profit body regulated by legislative decree No. 117 of 3 July 2017, acting under the data subject's mandate, which must be active in the field of the protection of data subjects' rights and freedoms with regard to the protection of personal data. 3. Such documents as may be helpful for assessment purposes shall be attached to the complaint along with the mandate given by the data subject, if any; an address for sending any communications, including via emails, facsimile or telephone, shall be also specified. 4. The Guarantor shall make available a complaint form and publish it on its institutional website; dissemination of the form in electronic format shall be promoted. 5. The Guarantor shall set out the procedure for handling complaints in its own rules of procedure and may provide for simplified arrangements and shorter deadlines in respect of the handling of complaints concerning alleged infringements of Articles 15 to 22 of the Regulation.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 143: 1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della	Legislative Decree no. 196 of 30 June 2003, Article 143: 1. Having concluded the preparatory phase, the Guarantor may take the measures referred to in Article 58 of the Regulation in

definizione del procedimento può adottare i provvedimenti di cui all'articolo 58 del Regolamento nel rispetto delle disposizioni di cui all'articolo 56 dello stesso. 2. I provvedimenti di cui al comma 1 sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti. 3. Il Garante decide il reclamo entro nove mesi dalla data di presentazione e, in ogni caso, entro tre mesi dalla predetta data informa l'interessato sullo stato del procedimento. In presenza di motivate esigenze istruttorie, che il Garante comunica all'interessato, il reclamo è deciso entro dodici mesi. In caso di attivazione del procedimento di cooperazione di cui all'articolo 60 del Regolamento, il termine rimane sospeso per la durata del predetto procedimento. 4. Avverso la decisione è ammesso ricorso giurisdizionale ai sensi dell'articolo 152.	accordance with the provisions made in Article 56 thereof if the complaint is found not to be clearly unsubstantiated and the prerequisites for a decision on the complaint are fulfilled, also prior to finalising the relevant proceeding. 2. The measures referred to in paragraph 1 shall be published in the Official Journal of the Italian Republic if the respective addressees cannot be identified easily because of their number or else on account of the complex investigations carried out. 3. The Guarantor shall decide on a complaint within nine months of the date the complaint was lodged and shall inform the data subject on the progress of the complaint within three months of the said date. Where there are reasons related to the preparatory activities, which the Guarantor shall communicate to the data subject, the decision on a complaint shall be made within twelve months of the aforementioned date. If the cooperation procedure envisaged in Article 60 of the Regulation is initiated, the running of time shall be stopped for as long as the said procedure is in progress. 4. The decision may be challenged before a judicial authority pursuant to Article 152.

Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 167:	Legislative Decree no. 196 of 30 June 2003, Article 167:
1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.	1. Any person who, with a view to gain for themselves or another or with intent to cause harm to the data subject, causes harm to the data subject by acting in breach of Article 123, 126 and 130 or else of the measures taken further to Article 129, shall be punished by imprisonment for between six months and one year unless the offence is more serious.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-<i>sexies</i> e 2-<i>octies</i>, o delle misure di garanzia di cui all'articolo 2-<i>septies</i> ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-<i>quinqüesdecies</i> arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.	2. Any person who, with a view to gain for themselves or another or with intent to cause harm to the data subject, causes harm to the data subject by processing the personal data mentioned in Articles 9 and 10 of the Regulation in breach of the provisions set out in Articles 2-<i>sexies</i> and 2-<i>octives</i> or the safeguards referred to in Article 2-<i>septies</i>, or else by acting in breach of the measures adopted further to Article 2-<i>quinqüesdecies</i>, shall be punished by imprisonment for one to three years unless the offence is more serious.
3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.	3. The penalty referred to in paragraph 2 shall also apply to any person who, with a view to gain for themselves or another or with intent to cause harm to the data subject, causes harm to the data subject by transferring the personal data to a third country or a international organisation in cases other than those permitted under Articles 45, 46 or 49 of the Regulation, unless the offence is more serious.
4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.	4. Where any of the offences mentioned in paragraphs 1 to 3 are reported to the public prosecutor, the latter shall inform the Guarantor thereof without delay.
5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle	5. The Guarantor shall transfer the records and findings gathered in the course of controls to the public prosecutor along with a reasoned report if there are grounds to believe that a criminal offence has been committed. Such records and findings shall be transferred to the public prosecutor no later than when the activities aimed at establishing the

violazioni delle disposizioni di cui al presente decreto. 6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.	infringements of the provisions mentioned in this decree are concluded. 6. The penalty shall be reduced if the offender or the organisation has been the subject of an administrative fine imposed by the Guarantor in accordance with this Code or the Regulation on account of the same facts and such fine has been levied.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 167-bis: 1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione. 3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.	Legislative Decree no. 196 of 30 June 2003, Article 167-bis: 1. Any person who, with a view to gain for themselves or another or with intent to cause harm, communicates or disseminates an automated filing system or a substantial part thereof containing personal data that are processed on a large scale, in breach of the provisions set out in Articles 2-ter, 2-sexies and 2-octies, shall be punished by imprisonment for one to six years unless the offence is more serious. 2. Any person who, with a view to gain for themselves or another or with intent to cause harm, communicates or disseminates an automated filing system or a substantial part thereof containing personal data that are processed on a large scale shall be punished by imprisonment for one to six years if the data subject's consent is required with a view to any communication or dissemination and such consent has not been obtained, unless the offence is more serious. 3. Paragraphs 4 to 6 of Article 167 shall apply to the offences mentioned in paragraphs 1 and 2 hereof.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 167 - ter: 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala	Legislative Decree no. 196 of 30 June 2003, Article 167 - ter: 1. Any person who, with a view to gain for themselves or another or with intent to cause harm, acquires, in a fraudulent manner, an automated filing system or a substantial part thereof containing personal data that are processed on a large scale shall be punished by

è punito con la reclusione da uno a quattro anni. 2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.	imprisonment for one to four years, unless the offence is more serious. 2. Paragraphs 4 to 6 of Article 167 shall apply to the offence mentioned in paragraph 1 hereof.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 168: 1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni. 2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.	Legislative Decree no. 196 of 30 June 2003, Article 168: 1. Whoever declares or certifies untrue information or circumstances, or else submits forged records or documents in the course of a proceeding or a fact-finding activity by the Guarantor shall be punished by imprisonment for between six months and three years, unless the offence is more serious. 2. Except for the cases under paragraph 1, whoever intentionally obstructs or disrupts a proceeding before the Guarantor or the fact-finding activities carried out by the Guarantor shall be punished by imprisonment for up to one year.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 170: 1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 è punito con la reclusione da tre mesi a due anni.	Legislative Decree no. 196 of 30 June 2003, Article 170: 1. Whoever fails to comply with a measure adopted by the Guarantor pursuant to Article 58(2), letter f), of the Regulation, Article 2-septies, paragraph 1, hereof and with the orders of general application mentioned in Article 21(1) of the legislative decree implementing Article 13 of Law no. 163 of 25 October 2017 shall be punished by imprisonment for between three months and two years, where such measure is binding on them.
Decreto Legislativo n. 196 del 30 giugno 2003, Articolo 171: 1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge.	Legislative Decree no. 196 of 30 June 2003, Article 171: 1. Any violation of the provisions referred to in Articles (4)1 and 8 of Law no. 300 of 20 May 1970 shall be punished as provided for by Article 38 of that Law.

Legge n. 675 del 31 dicembre 1996, Articolo 1, Paragrafo 1: 1. La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione.”	Law no. 675 of 31 December 1996, Article 1, Paragraph 1: This law guarantees that the personal data processing is carried out in compliance with the rights, fundamental freedoms, as well as the dignity of individuals, with particular reference to confidentiality and personal identity; it also guarantees the rights of legal persons and any other body or association.”

Bibliography

English titles

Legislation

Charter of Fundamental Rights of the European Union, OJ 2009 C 83/389.

Constitution of the Italian Republic 1947 (IT).

Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin.

Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation.

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (1950).

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

Council of Europe, Convention on Cybercrime (2001).

Declaration on Internet Rights, adopted by the Chamber of Deputies Special Parliamentary Committee for the Rights and Duties of the Internet on 28 July 2015.

Decree-Law no. 18 of 17 March 2020 (Measures to strengthen the National Health Service and economic support for families, workers and businesses related to the COVID-19 epidemiological emergency).

Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

European Convention on Human Rights, 1950.

International Covenant on Civil and Political Rights, 16 December 1966, entered into force in Italy on 23 March 1976.

Italian Code of Civil Procedure.

Italian Code of Criminal Procedure.

Law no. 7 of 28 February 2020, Conversion into law, with amendments, of the Legislative Decree no. 161 of 30 December 2019, containing urgent changes to the discipline of interception of conversations or communications.

Law n. 103 of 23 June 2017, Amendments to the Criminal Code, the Criminal Procedure Code and the Penitentiary System.

Law no. 675 of 31 December 1996, Protection of persons and other subjects regarding the processing of personal data.

Law no. 903 of 9 December 1977, Equal Treatment between men and women on the workplace.

Legislative Decree 29 December 2017, no. 216, Provisions on the wiretapping of conversations or communications, in implementation of the delegation referred to in Article 1, paragraphs 82, 83 and 84, letters a), b), c), d) and e), of the Law of 23 June 2017, no. 103.

Legislative Decree no. 150 of 1st September 2011.

Legislative Decree no. 150 of 1 September 2011, on complementary measures to the Code of Civil Procedure in the realm of reduction and simplification of the civil procedures of knowledge, pursuant to art. 54 of the Law of 18 June 2009, no. 69.

Legislative Decree 25 January 2010, no. 5, transposing Directive 2006/54/EC on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast).

Legislative Decree no. 104 of 2 July 2010, Implementation of Article 44 of Law no. 69 of 18 June 2009, delegating the Government for the reorganization of the administrative process.

Legislative Decree no. 198 of 11 April 2006, Code of equal opportunities between man and woman, pursuant to Article 6 of the Law of 28 November 2005, no. 246.

Legislative Decree, 9 April 2003, no. 70, Transposing the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce.

Legislative Decree no. 196 of 30 June 2003, Code regarding the protection of personal data, integrated with Legislative Decree no. 101 of 4 September 2018 on Provisions for the adaptation of national legislation to the provisions of EU Regulation 2016/679.

Legislative Decree 9 July 2003, no. 215, transposing Directive 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin.

Legislative Decree of 25 July 1998, no. 286, Consolidated Act of Provisions concerning immigration.

Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, COM (1998).

Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services, Digital Service Act (DSA) (2020).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)).

Reports

Article 29 Data Protection Working Party, ‘Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679’ (2017) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237> accessed 2 March 2021.

Council of Europe, Ad Hoc Committee on Artificial Intelligence (CAHAI), Strasbourg, 17 December 2020; <<https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da>>.

Council of Europe, Discrimination, artificial intelligence, and algorithmic decision-making, Study by Prof. Frederik Zuiderveen Borgesius, <www.coe.int/en/web/artificial-intelligence/director-jan-kleijssen>.

Council of Europe, Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, Committee of Experts on Internet Intermediaries (MSI-NET), March 2018.

Data Protection Unit of the Council of Europe, ‘Case law of the European Court of Human Rights concerning the protection of personal data’ (2018).

European Commission, Artificial intelligence – ethical and legal requirements, COM June 2020, available at <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Requirements-for-Artificial-Intelligence>.

European Commission, Digital Economy and Society Index (DESI) 2020 Italy, published on 11 June 2020, available online at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66918.

European Commission, Liability for artificial intelligence and other emerging digital technologies, Expert Group on Liability and New Technologies, 2019, <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>.

European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM 64 Feb. 19, 2020, available at https://ec.europa.eu/info/files/commission-report-safety-and-liability-implications-ai-in-ternet-things-and-robotics_en.

European Commission, White Paper On Artificial Intelligence - A European approach to excellence and trust, European Commission, Brussels, 19.2.2020 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0065&from=EN>.

European Parliament, Report with recommendations to the Commission on a civil liability regime for artificial intelligence, https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_EN.html.

European Parliament, Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html.

European Parliament, The ethics of artificial intelligence: Issues and initiatives, Panel for the Future of Science and Technology, EPRS | European Parliamentary Research Service, March 2020 [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU\(20\)634452_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(20)634452_EN.pdf).

Italian National Institute of Statistics (ISTAT), Summary of the Annual Report 2020, presented on 3 July 2020, available online at https://www.istat.it/it/files//2020/09/Annual-Report-2020_Summary.pdf.

Italian Minister for Technological Innovation, Italy 2025. Strategy for the technological innovation and digitalization of the country, available online at <<https://assets.innovazione.gov.it/1610546390-midbook2025.pdf>> accessed 10 February 2021 [Italian].

Italian Minister for Technological Innovation, National Strategy for Digital Skills, adopted on 21 July 2020, available online at <<https://assets.innovazione.gov.it/1610029655-dtd-1277-a-all1.pdf>> accessed 12 February 2021 [Italian].

Italian Minister of Economy and Finance, National Recovery and Resilience Plan, latest draft presented on 12 January 2021, available online at <https://www.ansa.it/documents/1610403841219_Bozza_Recovery_01_Cover.pdf> accessed 15 February 2021 [Italian].

Sellier E., Weyembergh A., Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation, Study Requested by the LIBE committee, August 2018.

Study Service of the Italian House of Representatives, The adaptation of the discipline on the protection of personal data to Regulation (UE) 2016/679, A.G. 22 (2018).

United Nations General Assembly , Working Group on the issue of human rights and transnational corporations and other business enterprises, 16 July 2018 <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/224/87/PDF/N1822487.pdf?OpenElement>>.

Books

Apa E. and Pollicino O., Modeling the Liability of Internet Service Providers: Google vs. Vivi Down: A Constitutional Perspective, (Egea, 2013).

Bistolfi Camilla, Bolognini Luca, Pelino Enrico, The European Privacy Regulation. Commentary to the new discipline on personal data protection (Giuffrè 2016).

Bolognini L., Pelino E., The code of the privacy discipline, Giuffrè, Milano, 2019.

Codiglione G. and Bassini M., From Private Enforcement to Public Enforcement. Copyright Enforcement in the Digital Age: A Comparative Overview, in Copyright and Fundamental Rights in the Digital Age, (Elgar, 2020).

Comandé G., Responsibility and accountability in the era of Artificial Intelligence, in Jurisprudence and independent Authorities in the era of liquid law. Studies in honor of Roberto Pardolesi, Di Ciommo F., Troiano O. (eds.), Piacenza, LaTribuna, 2018.

D'Acquisto G., Naldi M., Big data and privacy by design. Anonymization, pseudonymization, security, Giappichelli Editore, Turin, 2017.

Delmastro M., Nicita A., Big Data: how they are changing our world, Bologna, Il Mulino, 2019.

Faini F., Data Society. Data governance and protection of rights in the digital age, Milano, Giuffrè, 2019.

Finocchiaro G., The new European regulation on privacy and data protection, Zanichelli, Torino, 2017.

Floridi Luciano, Philosophy and computing: an introduction (Routledge 1999).

ID., Information: A Very Short Introduction (Oxford University Press 2010).

ID., The Fourth Revolution: how the infosphere is reshaping human reality (Oxford University Press 2014).

Frank M., Roehrig P., Pring B., What To Do When Machines Do Everything: How to Get Ahead in a World of AI, Algorithms, Bots, and Big Data, Wiley, Hoboken, 2017.

González-Fuster G., Van Brakel R., De Hert P., Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, Cheltenham (UK), 2019.

Harari Y. H., Homo Deus. A brief history of tomorrow, Bompiani, Milan, 2018.

Iaselli M., Internet of Things, drones and robotics: legal problems and possible solutions, Wolters Kluwer Italy, Milan, 2016.

Jankin Mikhaylov S., Esteve M., Champion A., Artificial intelligence for the public sector: opportunities and challenges of cross-sector collaboration, Philos Trans A Math Phys Eng Sci. 2018 Sep 13.

Letsas G., The ECHR as a living instrument: its meaning and legitimacy in Andreas Føllesdal, Birgit Peters and Geir Ulfstein (eds.) Constituting Europe: The European Court of Human Rights in a National, European and Global Context (Cambridge University Press 2013).

Menchini S., 'The ultimate "idea" of the legislator to speed up the duration of the declarative protection of rights: the fast-track procedure, in *Corr. Giur.*, 2009.

Orefice M., *Big Data and the effects on privacy, transparency and economic initiative*, Aracne Editrice, Rome, 2018.

Panetta R. (eds.), *Circulation and protection of personal data, between freedom and market rules*, Milano, Giuffrè, 2019.

Pasquale F., *The Black Box Society*, (Harvard University Press, 2015).

Pizzetti F., *Privacy and the European right to the protection of personal data. From Directive 95/46 to the new European Regulation*, Giappichelli Editore, Turin, 2016.

Privacy and the European right to the protection of personal data. The European Regulation 2016/679, Giappichelli Editore, Turin, 2016.

Artificial intelligence, personal data protection and regulation, Giappichelli Editore, Turin, 2018.

Protection of personal data in Italy between the GDPR and the revised code, Giappichelli Editore, Turin, 2021.

Rodotà S., *Electronic processors and social control*, Società Editrice Il Mulino, Bologna, 1973

Technologies and Rights (Il Mulino, 1995).

The world in the network. Which rights, which constraints, Laterza, Roma-Bari, 2014.

Conti P., *Interview on Privacy and Freedom*, (GLF Editori Laterza, 2005).

Sartor G., *Artificial intelligence and law. An introduction*, Giuffrè Editore, Milan, 1996.

Sarzana Di S. Ippolito F., Nicotra M., *Law of the blockchain, artificial intelligence and IoT*, Wolters Kluwer Italy, Milan, 2018.

Senden L., *EU non-discrimination law in the era of artificial intelligence: mapping the challenges of algorithmic discrimination*, in Bernitz U., Groussot X., Paju J. and De Vries S. (eds), *General principles of EU law and the EU digital order*, Alphen aan den Rijn: Kluwer Law International, 2020.

Spinello R., *The Right to Privacy in the Age of Digital Technology*, in *Privacy in a Digital, Networked World - Technologies, Implications and Solutions*, edited by Zeadally Sherali and Badra Mohamad (Springer International Publishing Switzerland, 2015).

Troisi B., Acts of discrimination and mediation, in Quaderni di conciliazione, edited by Carlo Pilia, Cagliari, 2011.

Periodicals

K. Ashton, That “Internet of Things” Thing, in RFID Journal, 2009.

Balkin J., Free Speech and Hostile Environments, (Columbia Law Review, 1999), accessed 10 February 2021 <https://digitalcommons.law.yale.edu/fss_papers/253>.

Bassini, M., Fundamental Rights and Private Enforcement in the Digital Age, (European Law Journal 25, no. 2 2019): 182–97, accessed 10 February 2021 <<https://doi.org/10.1111/eulj.12310>>.

ID., Mambo Italiano: The Perilous Italian Way to ISP Liability, (Fundamental Rights Protection Online, 2020), accessed 10 February 2021, <<https://www.elgaronline.com/view/edcoll/9781788976671/9797817889766.00014.xml>> ;

Bellezza M. and Frigerio F., A New Dawn for the ISP’s Liability in Italy?, (MediaLaws, 2018), accessed 20 February 2021, <<http://www.medialaws.eu/a-new-dawn-for-the-isps-liability-in-italy/>>.

Borrillo B., The protection of “privacy” and new technologies: the principle of “accountability” and sanctions imposed by the EU Supervisory Authorities after the entry into force of the GDPR, in *dirittifondamentali.it*, 2020, 2.

Bowyer K. W., Face recognition technology: Security versus Privacy, in *Technology and Society Magazine*, Vol. 4, 2004.

Capponi M., Anti-discrimination Law, risk factor “nationality” and competition notice in the public administration: the ultimate landing of the l’ultimo approdo of the judge, in *Lavoro, Diritti, Europa. Rivista nuova di Diritto del Lavoro*, 2018.

Caprioli F., The spyware as evidence tool in Italy (2017) 3 (2) *Rev. brasileira dir. proc. pen.*

Coccoli, J. The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era (2017) 1(2) *Peace Human Rights Governance*.

De Mauro A., M. Greco, and M. Grimaldi, “A Formal definition of Big Data based on its essential features”, in *Library Review*, vol. 65, 2016.

De Gregorio G. , *The Rise of Digital Constitutionalism in the European Union*, (SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 2019), accessed 15 February 2021, <<https://papers.ssrn.com/abstract=3506692>>.

De Pamphilis M., *Compensation for damages for unlawful processing of personal data after EU Reg. 2016/679 (2019) GC.com* accessed 1 February 2021 <<http://giustiziacyivile.com/danno-e-responsabilita/approfondimenti/il-risarcimento-del-danno-illegittimo-trattamento-dei-dati>>.

Fabiano N., *The Internet of Things ecosystem: the blockchain and privacy issues. The challenge for a global privacy standard*, *Advances in Science, in Technology and Engineering Systems Journal*, 2018.

Faini F., *Law in technology: emerging technologies and new forms of regulation*, in *federalismi.it*, 2020, 16.

Germani E., Ferola L., *Wearable computing and the future horizons of privacy*, in *Information and IT law*, 2014.

Guisella Finocchiaro, *Italy: The Legislative Procedure for National Harmonisation with the GDPR* (2018) 4 *Eur Data Prot L Rev* 496.

Minardi M., *The fast-track procedure*, in *Procedura Civile*, *Altalex*, 2010. Available at: <<https://www.altalex.com/documents/news/2010/03/25/il-processo-sommario-di-cognizione>>.

Lyon M. H., *Gearing Up For The EU’s Next Regulatory Push: AI, LA & SF Daily Journal* Oct. 11, 2019, <<https://www.gibsondunn.com/wp-content/uploads/2019/10/Lyon-Gearing-up-for-the-EUs-next-regulatory-push-AI-Daily-Journal-10-11-2019.pdf>>.

Naddeo F., *‘The Consent to the Processing of the Minor’s Personal Data’* (2018) II *Information and IT Law*, dossier 1, 1 February.

Nuccio M and Guerzoni M, *‘Big Data: Hell or Heaven? Digital Platforms and Market Power in the Data-Driven Economy’* (2019) 23(3) *Competition and Change*.

Orofino, *Ne bis in idem and penalty system in the discipline of personal data protection after the adoption of the GDPR*, (2019) 4 *Public comparative and European law* 1139.

Pallone EC, “‘Internet of Things’ and the Importance of the Right to Privacy Between Opportunities and Risks’ (2016) 1 *Cyberspace and Law*.

Petkova B, ‘Privacy as Europe’s First Amendment’ (2019) 25(2) *European Law Journal* 140.

Purtova N, ‘Do Property Rights in Personal Data Make Sense After the Big Data Turn?’ (Tilburg Law School Legal Studies Research Paper Series, no. 21/2017).

Santaniello G, ‘The Italian Privacy Code from a European Perspective’ (InterLex, Law Technology Information, 19 January 2004).

Simonato M, ‘Defence Rights and the Use of Information Technology in Criminal Procedure’ (2014) 85(1) *Revue Internationale de Droit Pénal*.

Simoncini A, ‘The Unconstitutional Algorithm: Artificial Intelligence and the Future of Freedoms’ (2019) 1 *BioLaw Journal*.

Solum LB, ‘Legal Personhood for Artificial Intelligences’ (Illinois Public Law and Legal Theory Research Papers, no. 09/13, 2008).

Stazi A, ‘Big Data and Comparative Law’ (2019) *Comparazione e Diritto Civile*.

Valerini F, ‘The Procedural News Regarding Privacy After Regulation 679/2016 (GDPR) and the Legislative Decree 101/2018’ (*Judicium*, Pacini Giuridica, 23 October 2018).

Warren SD and Brandeis LD, ‘The Right to Privacy’ (1890) IV(5) *Harvard Law Review*.

Ziccardi G, ‘Electronic Surveillance, Data Mining and Indiscriminate Processing of Citizens' Information Between Security Needs and Freedom Rights’ (2018) *Ragion Pratica*.

Zuddas P, ‘Covid-19 and Digital Divide: Digital Technologies and Social Rights Tested by the Health Emergency’ (2020) 3 *Osservatorio AIC*
https://www.osservatorioaic.it/images/rivista/pdf/2020_3_17_Zuddas.pdf accessed 20 February 2021.

Digital resources

Alù A and Longo A, ‘What is it digital divide: a new social (and cultural) discrimination’ (AgendaDigitale.eu, 13 March 2020)
<https://www.agendadigitale.eu/infrastrutture/il-digital-divide-culturale-e-una-nuova-discriminazione-sociale/>.

Bove M, 'The fast-track procedure pursuant to art. 702-bis and followings. c.p.c.' (Judicium. The civil procedure in Italy and Europe) <https://www.judicium.it/wp-content/uploads/saggi/36/bove%20%20procedimento%20sommario%20cognizione.pdf>.

Carbone MR, 'If the algorithm is racist: measures and norms protecting the weak subjects' (Agenda Digitale) <https://www.agendadigitale.eu/cultura-digitale/se-lalgoritmo-e-razzista-quali-misure-e-norme-a-tutela-dei-soggetti-deboli/> accessed [date not provided].

Cavallari G, 'The "digital dark age": the DESI 2020 and the ranking of Italy in the digitalization index' (Ius in Itinere, 13 June 2020) <https://www.iusinitinere.it/il-medioevo-digitale-il-desi-2020-e-la-posizione-dellitalia-nella-classifica-sulla-digitalizzazione-28850>.

Cerquozzi F, 'Right to internet access and Constitution' (Ius in Itinere, 24 October 2020) <https://www.iusinitinere.it/diritto-di-accesso-ad-internet-e-costituzione-31496>.

Committee of Experts on Internet Intermediaries, Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications (Council of Europe 2018) <https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a>.

Committee of Ministers of the Council of Europe, Declaration on the manipulative capabilities of algorithmic processes (2019) https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b.

Committee of Ministers of the Council of Europe, Recommendations and Declarations of the Committee of Ministers of the Council of Europe in the field of media and information society (2015) <https://rm.coe.int/1680645b44>.

Committee of Ministers of the Council of Europe, Recommendations of the Committee of Ministers to member states on a Guide to human rights for Internet users, CM/Rec(2014)6.

Committee of Ministers of the Council of Europe, Recommendation to Member States for the protection of privacy on the Internet, containing guidelines for the protection of individuals with regard to the collection and processing of personal data on the information highways <www.garanteprivacy.it>.

Council of Europe Commissioner for Human Rights, Recommendation, Unboxing Artificial Intelligence: 10 steps to protect human rights (2019) <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64>.

Davlet Gabel and Tim Hickman, 'Chapter 16: Remedies and sanctions – Unlocking the EU General Data Protection Regulation' (White&Case, 5 April 2019)

<https://www.whitecase.com/publications/article/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection>.

De Marco L, 'Origin and characters of the labor proceedings' (Diritto.it, 1 May 2004) <https://www.diritto.it/origine-e-caratteri-del-processo-del-lavoro/>.

Di Stefano S, 'Trojan horse in criminal trial' (Giustizia insieme, 2020) <https://www.giustiziainsieme.it/it/diritto-processo-penale/1364-il-trojan-horse-nel-processo-penale?hitcount=0>.

Directorate-General for External Policies, 'Surveillance and censorship: The impact of technologies on human rights' (European Parliament 2015) <[www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU\(2015\)549034_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf)>.

Directorate General of Human Rights and Rule of Law, 'Guidelines on Artificial Intelligence and Data Protection' (Council of Europe 2019) <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>.

European Commission, 'EU Cybersecurity plan to protect open internet and online freedom and opportunity' (2013) <https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>.

European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe' (2015) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192>.

European Commission, White Paper On Artificial Intelligence: A European approach to excellence and trust (2020) https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Commission for the Efficiency of Justice, 'European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment' (2018) <www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>.

European Parliament, Directorate-General for External Policies, 'Surveillance and Censorship: The impact of technologies on human rights' (2015) <[www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU\(2015\)549034_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf)>.

Evgeni Moyakine, 'Rights concerning complaints and judicial remedies' (Future Learn) <https://www.futurelearn.com/info/courses/general-data-protection-regulation/0/steps/32422>.

Forastiere A, 'Principle of effectiveness of judicial protection and uptake of reasons' (Justowin, 4 December 2017)

<https://www.justowin.it/new/2017/12/04/principio-di-effettivita-della-tutela-giurisdizionale-ed-assorbimento-dei-motivi/#:~:text=Nel%20sistema%20processuale%20amministrativo%2C%20il,Costituzione%20e%20del%20diritto%20europeo.>

Foreign Affairs Council Meeting, 'EU Human Rights Guidelines on Freedom of Expression Online and Offline' (2014) <www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142549.pdf>.

Garante per la protezione dei dati personali, Order injunction against Cavauto s.r.l. of 26 March 2020 n. 9446730 <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9446730>.

Garante per la Protezione dei Dati Personali, 'TikTok will comply with the requests of the Guarantor. But the authority will monitor the effectiveness of the adopted measures' (2021) <www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9533424>.

Goretta R, 'GDPR, the guide for complaints, appeals and reports to the Authority' (AgendaDigitale.eu, 2 July 2019) <www.agendadigitale.eu/sicurezza/privacy/gdpr-la>.

Italian Minister of Economy and Finance, National Recovery and Resilience Plan, latest draft presented on 12 January 2021, available online at https://www.ansa.it/documents/1610403841219_Bozza_Recovery_01_Cover.pdf.

Italian Minister for Technological Innovation, Italy 2025. Strategy for the technological innovation and digitalization of the country, available online at <https://assets.innovazione.gov.it/1610546390-midbook2025.pdf>.

Italian Minister for Technological Innovation, National Strategy for Digital Skills, adopted on 21 July 2020, available online at <https://assets.innovazione.gov.it/1610029655-dtd-1277-a-all1.pdf>.

Johanna Chamberlain and Jane Reichel, 'The relationship between damages and administrative fines in the EU General Data Protection Regulation' (SSRN, 7 September 2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3447854.

JPMorgan Chase & Co, Technology, globalization and the future of work in Europe: Essays on employment in a digitized economy (2015) <www.ippr.org/files/publications/pdf/technology-globalisation-future-of-work_Mar2015.pdf?noredirect=1>.

Lasagni G, 'The Use of trojans in the interception of communications between "presents"' (Diritto Penale contemporaneo, 2016) https://www.penalecontemporaneo.it/upload/LASAGNI_2016b.pdf.

MacCarthy M, AI needs more regulation, not less, Center for Technology Innovation, 9 March 2020 <www.brookings.edu/research/ai-needs-more-regulation-not-less/>.

Meta F, Recovery Plan: for digital Italy about 50 billion Euros for the pot, published on CorriereComunicazioni.it on 7 December 2020, available online at

<https://www.corrierecomunicazioni.it/digital-economy/recovery-plan-per-litalia-digitale-quasi-50-miliardi-sul-piatto/> .

Minadeo M, 'Labor proceeding: discipline and peculiarities of this special proceeding' (Ius in itinere, 11 July 2017) <https://www.iusinitinere.it/rito-del-lavoro-disciplina-di-tale-processo-3987>.

Ministry of Economic Development, Strategia Nazionale Italiana per l'intelligenza artificiale (2020) http://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf.

Nicotra G, 'Two challenges for Italy: digital divide and single network', published on Awarepec.com on 3 November 2020, available online at <https://awarepec.com/europa/due-sfide-per-litalia-digital-divide-e-rete-unica/> .

Nocera A, 'Acquisition of whatsapp and messenger chats: wiretap, search or seizure?' (Il Penalista, 2018) <https://ilpenalista.it/articoli/focus/lacquisizione-delle-chat-whatsapp-e-messenger-intercezione-perquisizione-o>.

Nucera S, 'Artificial intelligence and human intervention: between legal gaps and opportunities for the 21st century', in Ratio Iuris, available at <https://www.ratioiuris.it/intelligenza-artificiale-ed-intervento-umano-tra-lacune-giuridiche-ed-opportunita-per-il-xxi-secolo/>.

OHCHR, Guiding Principles on Business and Human Rights (2011) https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

Palmiotto F, 'Malwares and the right of defence. Exodus case' (Giustizia Penale e Nuove tecnologie, 2020) <http://www.la legislazione penale.eu/wp-content/uploads/2020/10/Palmiotto-Revisione-Finale.pdf>.

Parise V, 'Privacy protection: the complaint to the Garante, what it is and how to do it' (Cybersecurity360, 4 June 2019) <http://www.cybersecurity360.it/legal/privacy-dati-personali/tutela-privacy-il-reclamo-al-garante-che-cose-e-come-farlo/>.

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) <https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf>.

Security Without Borders, 'Exodus: New Spyware for Android Made in Italy' (29 March 2019) <https://securitywithoutborders.org/blog/2019/03/29/exodus-ita.html>.

Senate of the Republic, Legislature XVII, Draft Law no. 1722, presented on 19 December 2014, available online at <http://www.senato.it/service/PDF/PDFServer/BGT/00902175.pdf>.

Severio Puddu, 'Data Protection - Italy' (Linklaters, February 2020) <https://www.linklaters.com/en/insights/data-protected/data-protected---italy>.

Spedicato A, 'Decree n.101 / 2018: complaints and reports before the Garante, eliminated the appeal as a form of protection for violations of the rights of the data subjects' (Directio, 18 September 2018) <www.directio.it/multimedia/news/2018/09/18-decreto-101_reclami-segnalazioni-garante-eliminato-ricorso-violazioni-diritti-interessati.aspx>.

Stevens Y, 'The Promises and Perils of Artificial Intelligence: Why Human Rights and the Rule of Law Matter' (September 2017) <https://medium.com/@ystvns/the-promises-and-perils-of-artificial-intelligence-why-human-rights-norms-and-the-rule-of-law-40c57338e806>.

Ulenaers J, 'The Impact of Artificial Intelligence on the Right to a Fair Trial: Towards a Robot Judge?' Asian J Law Econ (21 July 2020) <https://doi.org/10.1515/ajle-2020-0008>.

Valli R, 'The Cyber Search and the Remote Search' (Il Penalista, 2017) <https://ilpenalista.it/articoli/focus/la-perquisizione-informatica-e-la-perquisizione-da-remoto>.

Watcher S, Mittelstadt B and Russel C, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' (3 March 2020) <https://ssrn.com/abstract=3547922>.

Case-law

Court of Appeal of Rome, Cesare Previti v. Wikimedia Foundation Inc, no. 4312, Rome Court of Appeal, 19 February 2018.

European Court of Justice, Eva Glawischnig Piesczek v. Facebook, Case C-18/18 [2019] ECLI:EU:C:2019:821.

European Court of Justice, joined cases: Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C236-08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08).

Italian Constitutional Court, 24 October 2017, judgment no. 348.

Italian Constitutional Court, 24 October 2017, judgment no. 349.

Italian Constitutional Court, 5 April 1973, judgement no. 38.

Italian Court of Cassation, 27 May 1975, judgment no. 2129.

Italian Court of Cassation, 20 April 1963, judgement no. 990.

Italian Supreme Court, Yahoo! v. RTI, no. 7708-9, sect. I, 19 March 2019.

Italian Supreme Court, Sez. un., 28 april 2016, no. 26889.

Milan Tribunal, Google v. Vivi Down case law saga: no. 1972, 24 february 2010; no. 8611, Court of Appeals of Milan, 21 december 2012; no. 5107, Supreme Court, sect. III, 17 December 2013.

Rome Tribunal, F.A. v. Google LLC, no. 81824, 1 February 2019.

Rome Tribunal, E. Caruso v. Associate Production Tirrena Asso Film S.p.A, judgement 14 September 1953.

Italian titles

Legislation

Carta dei Diritti Fondamentali dell'Unione Europea, OJ 2009 C 83/389.

Codice di Procedura Civile Italiano.

Codice di Procedura Penale Italiano.

Consiglio d'Europa, Convenzione sulla Criminalità Informatica (2001).

Consiglio d'Europa, Convenzione per la Protezione delle Persone con riguardo al Trattamento Automatico dei Dati Personali (1981).

Consiglio d'Europa, Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (1950).

Convenzione Europea dei diritti dell'uomo, 1950.

Convenzione Internazionale sui Diritti Civili e Politici, 16 dicembre 1966, entrata in vigore dal 23 Marzo 1976.

Costituzione della Repubblica Italiana 1947 (IT).

Decreto-Legge 17 Marzo 2020, n. 18 (Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19).

Decreto Legislativo 29 Dicembre 2017, n. 216, Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 Giugno 2017, n. 103.

Decreto Legislativo 1 Settembre 2011, n. 150, Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione, ai sensi dell'articolo 54 della legge 18 Giugno 2009.

Decreto Legislativo n. 5 del 25 Gennaio 2010, Attuazione della direttiva 2006/54/CE relativa al principio delle pari opportunità e della parità di trattamento fra uomini e donne in materia di occupazione e impiego (rifusione).

Decreto Legislativo n. 104 del 2 Luglio 2010, Attuazione dell'articolo 44 della legge 18 Giugno 2009, n. 69, recante delega al governo per il riordino del processo amministrativo.

Decreto Legislativo 11 Aprile 2006, n. 198, Codice delle pari opportunità tra uomo e donna, a norma dell'articolo 6 della legge 28 Novembre 2005, n. 246, art. 38.

Decreto Legislativo 9 Aprile 2003, n. 70, Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico.

Decreto Legislativo n. 196 del 30 Giugno 2003, Codice in materia di protezione dei dati personali, integrato dal Decreto Legislativo n. 101 del 4 Settembre 2018 recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 (IT).

Decreto Legislativo 9 Luglio 2003, n. 215, Attuazione della direttiva 2000/43/CE per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica.

Decreto Legislativo 9 Luglio 2003, n. 216, Attuazione della direttiva 2000/78/CE per la parità di trattamento in materia di occupazione e di condizioni di lavoro.

Decreto Legislativo 25 Luglio 1998, n. 286, Testo Unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero.

Dichiarazione dei Diritti in Internet, approvata dalla Commissione per i Diritti e i Doveri in Internet istituita presso la Camera dei Deputati nella seduta del 28 Luglio 2015.

Dichiarazione Universale dei Diritti Umani (adottata il 10 Dicembre 1948 UNGA Res 217 A(III)).

Direttiva 2006/54/CE del Parlamento Europeo e del Consiglio, del 5 Luglio 2006, riguardante l'attuazione del principio delle pari opportunità e della parità di trattamento fra uomini e donne in materia di occupazione e impiego (rifusione).

Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 Giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (Direttiva sul commercio elettronico).

Direttiva 2000/43/CE del Consiglio, del 29 Giugno 2000, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica.

Direttiva 2000/78/CE del Consiglio, del 27 Novembre 2000, che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro.

Legge n.7 del 28 Febbraio 2020, Conversione in legge, con modificazioni, del decreto-legge 30 Dicembre 2019, n. 161, recante modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni.

Legge n. 103 del 23 Giugno 2017, recante Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario.

Legge n. 675 del 31 Dicembre 1996, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

Legge n. 903 del 9 Dicembre 1977, Parità di trattamento tra uomini e donne in materia di lavoro.

Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a taluni aspetti giuridici del commercio elettronico nel mercato interno, COM (1998).

Proposta di Regolamento del Parlamento Europeo e del Consiglio, relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE.

Regolamento europeo 2016/679 del Parlamento europeo e del Consiglio del 27 Aprile 2016 sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali e sulla libertà di circolazione dei dati, e che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati).

Reports

Commissione Europea, Indice di digitalizzazione dell'economia e della società (DESI) 2020 Italia, pubblicato in data 11 Giugno 2020, disponibile online al sito <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66946>.

Commissione Europea, Libro bianco sull'intelligenza artificiale: un approccio europeo all'eccellenza e alla fiducia, Bruxelles, 19 Febbraio 2020.

Istituto Nazionale di Statistica (ISTAT), Rapporto Annuale 2020. La situazione del Paese, presentato in data 31 marzo 2020, disponibile *online* al sito: <https://www.istat.it/storage/rapporto-annuale/2020/Rapportoannuale2020.pdf?fbclid=IwAR1sVYU-tvYfwJhvNn0zrKEdlPwDfx_955b8mVf_uwfAfFIek3-tOaB7J_k>.

Parlamento europeo, Relazione con raccomandazioni alla Commissione su un quadro di aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, <https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_IT.html>.

Parlamento europeo, Relazione con raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, <https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_IT.html>.

Sellier E., Weyembergh A., Leggi di procedura penale nell'Unione Europea– Analisi comparata delle principali differenze selezionate e dell'impatto che queste hanno sullo sviluppo della legislazione europea', Studio richiesto dal comitato LIBE, agosto 2018.

Servizio Studi della Camera dei Deputati, L'adeguamento della disciplina sulla protezione dei dati personali al Regolamento (UE) 2016/679, A.G. 22 (2018).

Unità di Protezione dei Dati Personali del Consiglio d'Europa, Giurisprudenza della Corte Europea dei Diritti Umani riguardante la protezione dei dati personali (2018).

Books

Apa E. e Pollicino O., Disegnare la responsabilità dei Service Providers: Google vs. Vivi Down: una prospettiva Costituzionale (EGEA 2013).

Bistolfi C., Bolognini L., Pelino E., Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali (Giuffrè 2016).

Bolognini L., Pelino E., Il codice della disciplina privacy (Giuffrè 2019 Milano).

Codiglione G. e Bassini M., Dalla regolazione privata a quella pubblica. Protezione del Copyright nell'era digitale: una prospettiva comparatistica, (Copyright e Diritti Fondamentali nell'era digitale 2020).

Comandé G., Responsabilità ed accountability nell'era dell'Intelligenza Artificiale, in Giurisprudenza e Autorità indipendenti nell'epoca del diritto liquido (studi in onore di Roberto Pardolesi, Di Ciommo F., Troiano O., a cura di, Piacenza La Tribuna 2018).

D'Acquisto G., Naldi M., Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza (Giappichelli Editore Torino 2017).

Delmastro M., Nicita A., Big Data: come stanno cambiando il nostro mondo (Bologna Il Mulino 2019).

Faini F., Data Society. Governo dei dati e tutela dei diritti nell'era digitale (Milano Giuffrè 2019);

Finocchiaro G., Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati (Zanichelli Torino 2017).

Floridi L., Filosofia e Informatica: un'introduzione (Routledge 1999).

ID., Informazione: Una Breve Introduzione (Oxford University Press 2010).

ID., La Quarta Rivoluzione: come l'infosfera sta rimodellando la realtà umana (Oxford University Press 2014).

Gruppo di lavoro articolo 29, 'Linea guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del Regolamento UE 2016/679' <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237> consultato 2 Marzo 2021.

Harari Y. H., Homo Deus. Breve storia del futuro, (Bompiani Milano 2018).

Iaselli M., Internet of Things, droni e robotica: problemi giuridici e possibili soluzioni (Wolters Kluwer Italia Milano 2016).

Letsas G., La CEDU come strumento vivente: il suo significato e legittimità in Andreas Føllesdal, Birgit Peters and Geir Ulfstein (ed.) Constituire L'Europa: La Corte Europea dei

Diritti Umani in un contesto Nazionale, Europeo e Globale (Cambridge University Press 2013).

Menchini S., L'ultima "idea" del legislatore per accelerare i tempi della tutela dichiarativa dei diritti: il processo sommario di cognizione (Corr. Giur. 2009).

Orefice M., I Big Data e gli effetti su privacy, trasparenza e iniziativa economica (Aracne Editrice Roma 2018).

Panetta R. (a cura di), Circolazione e protezione dei dati personali, tra libertà e regole del mercato (Milano Giuffrè 2019).

Pasquale F., The Black Box Society, (Harvard University Press 2015).

Pizzetti F., Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo (Giappichelli Editore Torino 2016).

Pizzetti F., Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679, Turin, 2016.

Pizzetti F., Intelligenza artificiale, protezione dei dati personali e regolazione, Turin, 2018.

ID. Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679 (Giappichelli Editore Torino 2016).

ID., Intelligenza artificiale, protezione dei dati personali e regolazione (Giappichelli Editore Torino 2018).

ID., Protezione dei dati personali in Italia tra GDPR e codice novellato (Giappichelli Editore Torino 2021).

Rodotà S., Elaboratori elettronici e controllo sociale, (Società editrice il Mulino Bologna 1973).

ID., Tecnologie e diritti (Il Mulino 1995).

ID., Il mondo nella rete. Quali diritti, quali vincoli, (Laterza Roma-Bari 2014).

Rodotà S. e Paolo Conti, Intervista su Privacy e Libertà, (GLF Editori Laterza 2005).

Sarzana Di S. Ippolito F., Nicotra M., Diritto della blockchain, intelligenza artificiale e IoT (Wolters Kluwer Italia Milano 2018).

Sartor G., Intelligenza artificiale e diritto. Una introduzione (Giuffrè Editore Milano 1996).

Spinello R., Il diritto alla privacy nell'era della tecnologia digitale, nella privacy in un mondo digitale e in rete - Tecnologie, implicazioni e soluzioni (Zeadally Sherali e Badra Mohamad Springer International Publishing Switzerland 2015).

Troisi B., Atti di discriminazione e mediazione, in Quaderni di conciliazione, (Carlo Pilia Cagliari 2011).

Periodicals

Balkin J., Libertà di espressione e ambienti ostili (Columbia Law Review, 1999), consultato 10 Febbraio 2021 <https://digitalcommons.law.yale.edu/fss_papers/253>.

Bassini M., Diritti fondamentali e applicazione privata nell'era digitale (European Law Journal 25, no. 2 2019): 182–97, consultato 10 Febbraio 2021 <<https://doi.org/10.1111/eulj.12310>>.

ID., Mambo Italiano: la rischiosa via italiana sulla responsabilità dei service providers, (Fundamental Rights Protection Online, 2020), consultato 10 Febbraio 2021, <<https://www.elgaronline.com/view/edcoll/9781788976671/9797817889766.00014.xml>>

Bellezza M. e Frigerio F., 'Una nuova alba per la responsabilità dei service providers in Italia?' (MediaLaws, 2018), consultato 20 Febbraio 2021, <<http://www.medialaws.eu/a-new-dawn-for-the-isps-liability-in-italy/>>.

Borrillo B., La tutela della "privacy" e le nuove tecnologie: il principio di "accountability" e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR, in *dirittifondamentali.it*, 2020, 2.

Capponi M., Diritto antidiscriminatorio, fattore di rischio "nazionalità" e bandi di concorso nella pubblica amministrazione: l'ultimo approdo del giudice di merito, in *Lavoro, Diritti, Europa. Rivista nuova di Diritto del Lavoro*, 2018.

Caprioli F., Il "captatore informatico" come strumento di ricerca della prova in Italia (2017) 3(2) *Rev. brasileira dir. proc. pen.*

Coccoli, J. Le Sfide delle Nuove Tecnologie nell'Attuazione dei Diritti Umani: un'Analisi di alcuni Problemi Critici nell'Era Digitale (2017) 1(2) *Peace Human Rights Governance*.

De Gregorio G., La nascita del Costituzionalismo digitale nell'Unione Europea (SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 2019), consultato 15 Febbraio 2021, <<https://papers.ssrn.com/abstract=3506692>>.

De Pamphilis M., Il risarcimento del danno per illegittimo trattamento dei dati personali dopo il Reg. UE 2016/679, (2019) GC.com consultato 11 Febbraio 2021 <<http://giustiziacivile.com/danno-e-responsabilita/approfondimenti/il-risarcimento-del-danno-illegittimo-trattamento-dei-dati>>.

Faini F., Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione, in *federalismi.it*, 2020, 16.

Finocchiaro G., Italia: La Procedura Legislativa per un'armonizzazione nazionale al RGPD (2018), 4 *Eur Data Prot L Rev* 496.

Germani E., Ferola L., Il wearable computing e gli orizzonti futuri della privacy, in *Diritto dell'informazione e dell'informatica*, 2014.

Minardi M., Il processo sommario di cognizione, in *Procedura Civile*, *Altalex*, 2010. Available at: <<https://www.altalex.com/documents/news/2010/03/25/il-processo-sommario-di-cognizione>>.

Nuccio M. e Guerzoni M., Big Data: Inferno o Paradiso? Piattaforme digitali e potere di mercato nell'economia data-driven, (*Competition and change*, vol.23(3) 2019).

Naddeo F., Il consenso al trattamento dei dati personali del minore (*Diritto dell'Informazione e dell'Informatica*, II, fasc. 1, 1° Febbraio 2018).

Orofino M., Ne bis in idem e sistema sanzionatorio nella disciplina della protezione dei dati personali dopo l'adozione del GDPR, (2019) 4 *Diritto pubblico comparato ed europeo* 1139;

Pallone E.C., "Internet of Things" e l'importanza del diritto alla privacy tra opportunità e rischi, in *Cyberspazio e diritto*, n. 1, 2016.

Petkova B., La Privacy è il Primo Emendamento Europeo, (*European Law Journal* 25, no. 2, 2019).

Santaniello G., Il Codice della Privacy italiano in una prospettiva europea (*InterLex, Diritto Tecnologia Informazione*, 19 Gennaio 2004).

Simonato M., Diritti di difesa e uso della tecnologia nel procedimento penale (2014) 85 (1) *Revue internationale de droit penal*.

Stazi A., Big Data e diritto comparato, in *Comparazione e diritto civile*, 2019.

Valerini F., Le novità processuali in materia di privacy dopo il Reg. 679/2016 (GDPR) e il D. lgs. 101/2018 (Judicium, Pacini Giuridica, 23 Ottobre 2018).

Warren S. D. - Brandeis L. D., The right to privacy (Harvard Law Review, IV, no. 5, 1890).

Ziccardi G., Sorveglianza elettronica, data mining e trattamento indiscriminato delle informazioni dei cittadini tra esigenze di sicurezza e diritti di libertà, in *Ragion Pratica*, vol. 2018.

Zuddas P., Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria, pubblicato su Osservatorio Costituzionale dell'Associazione Italiana Costituzionalisti (AIC), n. 3/2020, in data 26 maggio 2020, disponibile *online* al sito <https://www.osservatorioaic.it/images/rivista/pdf/2020_3_17_Zuddas.pdf> ultimo accesso in data 20 Febbraio 2021.

Digital resources

Alù A., Longo A., Cos'è il digital divide: nuova discriminazione sociale (e culturale), pubblicato su AgendaDigitale.eu in data 13 Marzo 2020, disponibile online al sito: <<https://www.agendadigitale.eu/infrastrutture/il-digital-divide-culturale-e-una-nuova-discriminazione-sociale/>>.

Bove M., Il procedimento sommario di cognizione di cui agli articoli 702-bis ss. c.p.c., in *Judicium. Il processo civile in Italia e in Europa*. Available at: <<https://www.judicium.it/wp-content/uploads/saggi/36/bove%20%20procedimento%20sommario%20cognizione.pdf>>.

Carbone M.R., Se l'algoritmo è razzista: quali misure e norme a tutela dei soggetti deboli, 2019, available at: <<https://www.agendadigitale.eu/cultura-digitale/se-lalgoritmo-e-razzista-quali-misure-e-norme-a-tutela-dei-soggetti-deboli/>>.

Cavallari G., Il "medioevo digitale": il DESI 2020 e la posizione dell'Italia nella classifica sulla digitalizzazione, pubblicato su Ius in Itinere in data 13 Giugno 2020, disponibile online al sito <<https://www.iusinitinere.it/il-medioevo-digitale-il-desi-2020-e-la-posizione-dellitalia-nella-classifica-sulla-digitalizzazione-28850>>.

Cerquozzi F., “Diritto di accesso ad Internet e Costituzione”, pubblicato su Ius in Itinere in data 24 ottobre 2020, disponibile online al sito <<https://www.iusinitinere.it/diritto-di-accesso-ad-internet-e-costituzione-31496>>.

Chamberlain J., Reichel J., Il rapporto tra i danni e le sanzioni amministrative nel Regolamento generale sulla protezione dei dati dell'UE (SSRN, 7 Settembre 2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3447854>.

Comitato dei Ministri del Consiglio d'Europa, Dichiarazione sulle Capacità Manipolative dei Processi Algoritmici (2019), <https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b>.

Comitato dei Ministri del Consiglio d'Europa, Raccomandazione agli Stati Membri per la protezione della privacy su Internet contenente Linee Guida per la protezione delle persone rispetto alla raccolta e al trattamento di dati personali sulle autostrade dell'informazione, <www.garanteprivacy.it>.

Comitato dei Ministri del Consiglio d'Europa, Raccomandazioni del Comitato dei Ministri agli Stati membri sulla Guida ai diritti umani per gli utenti di Internet, CM/Rec(2014)6.

Comitato dei Ministri del Consiglio d'Europa, Raccomandazioni e Dichiarazioni del Comitato dei Ministri del Consiglio d'Europa nel campo dei media e della società dell'informazione (2015), <<https://rm.coe.int/1680645b44>>.

Comitato di Esperti sugli Intermediari Internet, Studio sulle Dimensioni dei Diritti Umani delle Tecniche di Elaborazione Automatizzata dei Dati (in particolare algoritmi) e Possibili Implicazioni Normative (2018) <<https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a>>.

Commissario per i Diritti Umani de Consiglio d'Europa, Disimballare l'Intelligenza Artificiale: 10 Passi per Proteggere i Diritti Umani (2019) <<https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64>>.

Commissione Europea, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni: una Strategia per il Mercato Digitale Unico in Europa (2015) <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192>>.

Commissione Europea, Libro Bianco sull'Intelligenza Artificiale: un Approccio Europeo all'Eccellenza e alla Fiducia (2020) <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf>.

Commissione Europea per l'Efficienza della Giustizia, Carta Etica Europea sull'Uso dell'Intelligenza Artificiale nei Sistemi Giudiziari e nel loro Ambiente (2018) <www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment> ultimo accesso 28 Febbraio 2021;

Commissione Europea, Piano di Sicurezza Informativa dell'UE per proteggere l'open Internet e la libertà e opportunità online (2013) <<https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>>.

De Marco L., Origine e caratteri del processo del lavoro (Diritto.it, 1° Maggio 2004) <<https://www.diritto.it/origine-e-caratteri-del-processo-del-lavoro/>>.

Di Stefano S., I Trojan horse nel processo penale, (Giustizia insieme, 2020) <<https://www.giustiziainsieme.it/it/diritto-processo-penale/1364-il-trojan-horse-nel-processo-penale?hitcount=>>.

Direzione Esterna per le Politiche Esterne, Sorveglianza e Censura: l'Impatto delle Tecnologie sui Diritti Umani (2015), <[www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU\(2015\)549034_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf)>.

Direzione Generale dei Diritti Umani e dello Stato di Diritto, Linee guida sull'Intelligenza Artificiale e la Protezione dei Dati (2019) <<https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>>.

Evgeni M., Diritti in materia di reclami e rimedi giudiziari (*Future Learn*) <<https://www.futurelearn.com/info/courses/general-data-protection-regulation/0/steps/32422>>.

Forastiere A., Principio di effettività della tutela giurisdizionale ed assorbimento dei motivi (Justowin, 4 Dicembre 2017) <<https://www.justowin.it/new/2017/12/04/principio-di-effettivita-della-tutela-giurisdizionale-ed-assorbimento-dei-motivi/#:~:text=Nel%20sistema%20processuale%20amministrativo%2C%20il,Costituzione%20e%20del%20diritto%20europeo>>.

Gabel D., Hickman T., Capitolo 16: Rimedi e sanzioni - Sbloccare il Regolamento generale sulla protezione dei dati dell'UE (*White&Case*, 5 Aprile 2019) <<https://www.whitecase.com/publications/article/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection>>.

Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Cavauto s.r.l. 26 Marzo 2020 n. 9446730 <<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9446730>>.

Garante per la Protezione dei Dati Personali, TikTok si adeguerà alle richieste del Garante privacy. Ma l'autorità vigilerà sull'effettiva efficacia delle misure che saranno adottate (2021) <www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9533424>.

Goretta R., GDPR, la guida per reclami, ricorsi e segnalazioni all'Autorità (Agendadigitale.eu, 2 Luglio 2019) <www.agendadigitale.eu/sicurezza/privacy/gdpr-la-guida-per-reclami-ricorsi-e-segnalazioni-allautorita/>.

JPMorgan Chase & Co, Tecnologia, globalizzazione e future del lavoro in Europa: Saggi sull'Occupazione in un'Economia Digitalizzata (2015) <www.ippr.org/files/publications/pdf/technology-globalisation-future-of-work_Mar2015.pdf?noredirect=1>.

Lasagni G., L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti" (Diritto Penale contemporaneo, 2016) <https://www.penalecontemporaneo.it/upload/LASAGNI_2016b.pdf>.

Minadeo M., Rito del lavoro: disciplina e peculiarità di tale processo speciale (*Ius in itinere*, 11 Luglio 2017) <<https://www.iusinitinere.it/rito-del-lavoro-disciplina-di-tale-processo-3987>>.

Meta F., Recovery Plan, per l'Italia digitale quasi 50 miliardi sul piatto, pubblicato su CorriereComunicazioni.it in data 7 Dicembre 2020, disponibile online al sito <<https://www.corrierecomunicazioni.it/digital-economy/recovery-plan-per-litalia-digitale-quasi-50-miliardi-sul-piatto/>>.

Ministero dell'Economia e delle Finanze, Piano Nazionale di Ripresa e Resilienza, ultima bozza presentata in data 12 Gennaio 2021, disponibile online al sito <https://www.ansa.it/documents/1610403841219_Bozza_Recovery_01_Cover.pdf>.

Ministero per l'innovazione tecnologica e la digitalizzazione, Italia 2025. Strategia per l'innovazione tecnologica e la digitalizzazione del Paese, disponibile online al sito: <<https://assets.innovazione.gov.it/1610546390-midbook2025.pdf>>.

Ministero per l'innovazione tecnologica e la digitalizzazione, Strategia Nazionale per le Competenze Digitali, approvata in data 21 Luglio 2020, disponibile online al sito <<https://assets.innovazione.gov.it/1610029655-dtd-1277-a-all1.pdf>>.

Ministero dello Sviluppo Economico, Strategia Nazionale Italiana per l'intelligenza artificiale (2020) <www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf>.

Nicotra G., Due sfide per l'Italia: digital divide e rete unica, pubblicato su Awarepec.com in data 3 Novembre 2020, disponibile online al sito: <<https://awarepec.com/europa/due-sfide-per-litalia-digital-divide-e-rete-unica/>>.

Nocera A., 'L'acquisizione delle chat whatsapp e messenger: intercettazione, perquisizione o sequestro?' (Il Penalista, 2018), <<https://ilpenalista.it/articoli/focus/lacquisizione-delle-chat-whatsapp-e-messenger-intercettazione-perquisizione-o>>.

Nucera S., Intelligenza artificiale ed intervento umano: tra lacune giuridiche ed opportunità per il XXI secolo, in Ratio Iuris, disponibile online al sito: <<https://www.ratioiuris.it/intelligenza-artificiale-ed-intervento-umano-tra-lacune-giuridiche-ed-opportunita-per-il-xxi-secolo/>>.

OHCHR, Principi Guida sul Business e i Diritti Umani (2011) <https://www.ohchr.org/documents/publications/guidingprinciplesbusinessshr_en.pdf>.

Palmiotto F., Captatori informatici e diritto alla difesa. Il caso Exodus (Giustizia Penale e Nuove tecnologie, 2020) <<http://www.la legislazione penale.eu/wp-content/uploads/2020/10/Palmiotto-Revisione-Finale.pdf>>.

Parise P., Tutela privacy: il reclamo al Garante, che cos'è e come farlo (Cybersecurity360, 4 Giugno 2019) <www.cybersecurity360.it/legal/privacy-dati-personali/tutela-privacy-il-reclamo-al-garante-che-cose-e-come-farlo/>.

Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla protezione dei dati personali nelle comunicazioni elettroniche e che

abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche),

<<https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/it/pdf>>.

Puddu S., Protezione dei dati – Italia (*Linklaters*, Febbraio 2020)
<<https://www.linklaters.com/en/insights/data-protected/data-protected---italy>>.

Riunione del Consiglio Affari Esteri, Linee guida dell'UE sui Diritti Umani sulla libertà di espressione online e offline (2014)
<www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142549.pdf>.

Security Without Borders, Exodus: Nuovo Spyware per Android Made in Italy (29.3.2019) <<https://securitywithoutborders.org/blog/2019/03/29/exodus-ita.html>>.

Senato della Repubblica, XVII Legislatura, Disegno di Legge n. 1722, presentato in data 19 Dicembre 2014, disponibile online al sito:
<<http://www.senato.it/service/PDF/PDFServer/BGT/00902175.pdf>>.

Simoncini A., L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà, in *BioLaw Journal*, no. 1/2019.

Spedicato A., Decreto n.101/2018: reclami e segnalazioni davanti al Garante, eliminato il ricorso come forma di tutela per le violazioni sui diritti degli interessati (*Directio*, 18 Settembre 2018)
<www.directio.it/multimedia/news/2018/09/18-decreto-101_reclami-segnalazioni-garante-eliminato-ricorso-violazioni-diritti-interessati.aspx>.

Valli R., La perquisizione informatica e la perquisizione da remoto (*Il Penalista*, 2017)
<<https://ilpenalista.it/articoli/focus/la-perquisizione-informatica-e-la-perquisizione-da-remoto>>.

Case-law

Corte Costituzionale Italiana, 24 Ottobre 2017, n. 348.

Corte Costituzionale Italiana, 24 Ottobre 2017, n. 349.

Corte Costituzionale Italiana, 5 Aprile 1973, n. 38.

Corte d'Appello di Roma, Cesare Previti v. Wikimedia Foundation Inc, n. 4312, 19 Febbraio 2018.

Corte di Cassazione, Sez. I civ., Yahoo! v. RTI , n. 7708-9, 19 Marzo 2019.

Corte di Cassazione, Sez. un., 28 Aprile 2016, n. 26889.

Corte di Cassazione Italiana, 27 Maggio 1975, n. 2129.

Corte di Cassazione Italiana, 20 Aprile 1963, n. 990.

Corte di Giustizia dell'Unione Europea, Eva Glawischnig Piesczek v. Facebook, C-18/18 [2019] ECLI:EU:C:2019:821.

Corte di Giustizia dell'Unione Europea, Cause riunite, Google France SARL e Google Inc. v Louis Vuitton Malletier SA (C236-08), Google France SARL v Viaticum SA e Luteciel SARL (C-237/08) e Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL e altri (C-238/08).

Tribunale di Milano, Google v. Vivi Down, n. 1972, 24 Febbraio 2010; n. 8611, Corte d'Appello di Milano, 21 Dicembre 2012; n. 5107, Corte di Cassazione, Sez. III pen., 17 Dicembre 2013.

Tribunale di Roma, F.A. v. Google LLC, n. 81824, 1 Febbraio 2019.

Tribunale di Roma, E. Caruso c/ Produzione associata Tirrena Asso Film S.p.A., 14 Settembre 1953.

ELSA LITHUANIA

Contributors

National Coordinator

Aušra Abraitytė

National Researchers

Danielė Giedraitytė

Algirdas Gedminas

Vytautas Pasvenskas

Kotryna Seliutaitė

Raminta Matulytė

Skaidrė Dudėnaitė

National Linguistic Editor

Raminta Matulytė

Skaidrė Dudėnaitė

National Technical Editor

Martynas Matusevičius

National Academic Supervisor

Miglė Petkevičienė

Dr. Ažuolas Čekanavičius

Introduction

Nowadays human rights and digital technologies are in coexistence, and this type of relationship creates many difficulties. It is known that AI may cause threats to human rights, for example, it tends to discriminate against humans (e.g. by race). But the biggest issues which Advanced Digital Technologies (ADT) pose are related to personal data protection. Lithuania is no exception to other Western countries and is making great progress in ADT development. As a result, legislations of these technologies are in lawmakers' and legal scholars' scope of debate.

Lithuania is a member state of the European Union (EU), therefore, the majority of legal regulation related to ADT is transferred from the EU legal system to the Lithuanian national legal system. The following report addresses aspects of Human Rights in the age of ADT in Lithuania, as well as other related issues and national specifics of regulation in our country's legal system.

1. Which human rights issues do Advanced Digital Technologies pose in your country?

The age of the fourth industrial revolution and the rapid development of digital technologies not only provides certain advantages in our everyday lives but poses risks to the rights of individuals on both - national and international levels. ADT do not have one precise definition under the national legal framework in Lithuania. According to common understanding, ADT are those technologies that are able to process more data and provide more complex results than regular digital technologies. Examples of such ADT are including but not limited to artificial intelligence (AI), Internet of Things (IoT), data pooling, biometrical data recognition (such as speech or face), virtual reality. Lithuania has made great progress in ADT development in recent years, especially in the context of the growing number of technological start-ups, therefore, the legal framework for ADT improvement gathers more and more attention.

As data is the necessary factor for ADT development, there is no doubt that ADT poses significant issues for the right to privacy and data protection. Even though there is a possibility for using anonymized data, the importance of personal information protection is growing. Standards for such protection at the national level in Lithuania resemble the ones at the international level. According to Article 22 of the national Constitution⁵⁶⁴ (the Constitution) 'The private life of a human being shall be inviolable.' Standards of the European Convention on Human Rights (ECHR) (Article 8) and Charter of Fundamental Rights of the European Union⁵⁶⁵ (Charter) (Article 7) are important not only as regulatory

⁵⁶⁴ Constitution of the Republic of Lithuania, approved on 25 October 1992.

⁵⁶⁵ Charter of Fundamental Rights of the European Union [2012] OJ C326/02.

guidelines for the legislative but for courts' doctrine as well as they cite these international human rights law instruments and the case-law of European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). However, the most important specific legal act - data protection instrument - applicable in Lithuania is the General Data Protection Regulation⁵⁶⁶ (GDPR), implementing the same requirements for processed personal data across the EU. Law of the Republic of Lithuania on the Legal Protection of Personal Data (Personal Data Protection Law)⁵⁶⁷ acknowledges the direct application of the GDPR. Another important legal standard is the Law of Electronic Communications⁵⁶⁸ which regulates some of the important issues related to direct marketing which is performed by Lithuanian companies by using some of the ADT tools.

In addition to threats to the right to privacy, some other issues may be mentioned as well. In the context of freedom of expression (Article 26 of the Constitution; Article 10 of ECHR) social media giants operating in Lithuania such as Facebook, Twitter, Youtube have implemented ADT based tools that mark and block automatically user-generated content that may interfere with other human rights. There could be some arguing that ADT operating in Lithuania may pose issues in relation to discrimination as well.

There is no doubt that it is of core importance to perform human rights impact assessments before the implementation of ADT. However, at the national level in Lithuania, there is no expressly regulated procedure for such assessments to be performed by national institutions. There could be some sectoral examples, such as investigations on data protection issues, executed by the State Data Protection Inspectorate (SDPI) but these assessments are performed more post-factum than prior to the implementation of a technological solution. It may be said that in Lithuania human rights impact assessments' performance is mostly left to businesses that create and implement ADT. There are no international human rights protection obligations posed on companies, however, according to Guiding Principles on Business and Human Rights,⁵⁶⁹ businesses are encouraged to perform due diligence which should include 'assessing actual and potential human rights impacts.' It may be said that the level of interference with human rights posed by ADT developed in Lithuania depends essentially on the social responsibility of the company owning such ADT.

⁵⁶⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

⁵⁶⁷ The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, approved on 11 June 1996.

⁵⁶⁸ The Law on Electronic Communications of the Republic of Lithuania, No. IX-2135, approved on 15 April 2004, art. 1.

⁵⁶⁹ United Nations. Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, endorsed on June 16 2011.

However, it could be said that an efficient way in Lithuania to measure ADT impact and ensure less intrusive interference with human rights is the legislative procedure. Under Article 7 of the Law on the Legislative Framework of the Republic of Lithuania⁵⁷⁰ during the process of proposal and approval of national legislation, non-governmental organisations as well as other stakeholders may share insights, concerns and suggestions on the human rights issues related to ADT policy legislation.

The above-mentioned risks raise numerous questions such as: to what extent national legislation in Lithuania is adapted to ADT posed risks for human rights; what are the legal possibilities to defend individual rights violated in relation to ADT development and operation; are national measures and proceedings sufficient to ensure the adequate level of protection of human rights? It is mandatory to have a clear and comprehensive view on ADT and provide possible solutions to prevent human rights violations in Lithuania. Therefore, a thorough analysis of these issues is displayed in our further report.

2. How is personal information protected in your national legislation?

In Lithuania, personal information is protected by various levels of legal acts: international, EU's legal framework and by national legal acts.

ECHR is a significant international legal act. Article 8(1) of the ECHR establishes the right to private life, under which everyone has the right to respect for private and family life. Lithuania ratified ECHR by law on 27 April 1995 and it entered into force on 20 June 1995, therefore, the ECHR has legislative force in Lithuania and is directly applicable.

As Lithuania has been a Member State of the EU since 1 May 2004, the Lithuanian legal system is highly influenced by EU legal acts. In the legal framework of the EU, the protection of personal information is guaranteed by the GDPR, directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime and directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Indeed, one of the main sources of personal data protection in Lithuania is the GDPR, which has been directly applicable since 25 May 2018.

⁵⁷⁰ The Law on Legislative Framework of the Republic of Lithuania, XI-2220, approved on 18 September 2012.

Considering national legislation, Article 22 of the Constitution establishes the inviolability of a person's private life. This Article obliges the State legislation to ensure effective protection and defence of the right to the inviolability of private life. Other national legal acts on protection of personal information mentioned below are required to be harmonised with EU law.

The Law on Legal Protection of Personal Data of the Republic of Lithuania shall implement the GDPR. Article 1(3) of the law states that “This Law shall apply in conjunction with Regulation (EU) 2016/679 and its implementing legislation.” Article 7 indicates the supervision of Regulation (EU) 2016/679 and the application of this law. The application of the Regulation in Lithuania is foreseen to be monitored by the SDPI and the Office of Inspector of Journalist Ethics (OIJE).

The concept of personal data was regulated by this law in Lithuania prior to the entry into force of the GDPR. From 1 April 1998 in Article 2(1) the concept was defined as: ‘Personal data - data about a concrete or a natural person identifiable from the data, his business relations and findings of the person on the basis of the data.’ In order for Lithuania to join the EU in 2000, formal negotiations have been initiated, legal norms have also been harmonised, therefore a different concept of personal data has been introduced in the new version of the Law since 1 January 2001. The concept was defined as indicated in Directive 95/46/EB (1995) (Data Protection Directive) Article 2(1).⁵⁷¹ Data Protection Directive has expired since 24 May 2018. The concept of personal data was in the law until 16 July 2018. The old version then changed quite significantly as the GDPR entered into force across the EU on 25 May 2018. The concept of personal data has been removed from the Law on Legal Protection of Personal Data of the Republic of Lithuania and the GDPR definition of personal data has been introduced. Whereas regulations apply directly to all EU countries (Treaty on the Functioning of the EU 288(2)),⁵⁷² Article 2(3) of the law states that ‘Other terms used in this law shall be interpreted as defined in Regulation (EU) 2016/679’.

Following national legal act is the Law on the Legal Protection of Personal Data of the Republic of Lithuania processed for the Prevention, Investigation, Disclosure or Prosecution of Criminal Offences, Penalty Enforcement or National Security or Defence Purposes. The Law implements Council directive 2016/680 (2016) also reveals the application of GDPR in Lithuania and refers to this Regulation.

⁵⁷¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281.

⁵⁷² The Treaty on the Functioning of the European Union [2012] OJ C326.

Article 9 of the Law on Cybersecurity of the Republic of Lithuania (Law on Cyber Security) establishes the powers of the SDPI in the field of cybersecurity: SDPI shall implement cybersecurity policy in the field of personal data protection and perform the tasks of the supervisory authority established by the GDPR.

Article 3 of the Resolution of the Government of the Republic of Lithuania ‘Regarding the Approval of the Regulations of the SDPI’⁵⁷³ states that the SDPI shall act in compliance with the Constitution, international treaties and agreements of the Republic of Lithuania and the GDPR. Article 16 of the aforementioned resolution states that ‘Inspectorate has the supervisory authority powers laid down in Regulation (EU) 2016/679’.

On the basis of all the aforementioned legal acts, protection of personal data in Lithuania becomes the totality of legal, technical and organisational measures intended to protect personal data from illegal management. This brief analysis of the protection of private information in the Lithuanian legal system shows that the regulation is heavily influenced by international legal acts and the EU legal system legislation, while the GDPR is one of the main acts of protection of private information, which is widely implemented in Lithuanian laws and other acts.

3. To which extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?

Personal data usage and data protection are highly controlled by the Lithuanian government and judicial bodies concerning human rights protection. The core principles stated in the GDPR impose the importance of data protection in the public sector and forewarn judicial and governmental bodies of the possible outcomes if such regulations are not complied with. However, revising the GDPR it becomes feasible that the private sector is not an exception to the regulation. The pure fact of the regulation concerning the private sector is quite surprising as, traditionally human rights, including right to privacy, put emphasis on the relationship between the citizens and the State. As the GDPR itself recognises that human rights can be violated by various private enterprises. The GDPR Recital 97 embodies the concept of a Data protection officer (DPO). The sole purpose of DPOs is to monitor the internal compliance with the GDPR. Nevertheless, in private sector companies and organizations DPOs are mandatory:⁵⁷⁴ (i) whereas the core activities of the company or the processor of general data require regular and systematic monitoring of data subjects on a large scale; or (ii) whereas the core activities of the company or the

⁵⁷³ The Resolution of the Government of the Republic of Lithuania “Regarding the Approval of the Regulations of the State Data Protection Inspectorate”, No. 1156, approved on 2001 September 25.

⁵⁷⁴ European Commission, Guidelines on Data Protection Officers (‘DPOs’) (wp243rev.01), adopted on 13 December 2016.

processor of the general data consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences. Other bodies of the Lithuanian private sector are not required to have a DPO but are advised by the SDPI to instate such a role in their company.

The self-regulation of data protection in the private sector is objectively reflected throughout the cooperation between DPOs and the supervisory authorities of Lithuania and also the accountability of the data controller. The cooperation between the DPO and the supervisory authorities is based on the Guidelines on DPO.⁵⁷⁵ The DPO acts as a contact point to facilitate the access by the supervisory authority to the documents and information for the performance of the tasks mentioned in Article 57 of the GDPR, as well as for the exercise of its investigative, corrective, authorisation, and advisory powers mentioned in Article 58 of the GDPR.⁵⁷⁶ The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, however, this does not prohibit the DPO from contacting and seeking advice from the supervisory authority on any other matter, where appropriate.⁵⁷⁷ The critical standpoint in self-regulation is that the responsibility for violations of the GDPR does not fall on the DPO itself. The responsibility falls on the company itself. GDPR clearly states that the data controller or processor shall be obligated to ensure compatible data processing regarding the requirements of the GDPR. The DPO itself acts in the private sector as an autonomous party, who is an intermediate between the interested stakeholders (for example – supervisory authority, data controllers and processors, or other business units of the organization). Regarding accountability – Article 24 of the GDPR allocates the liability of data protection to the data controllers. Importantly, the Article continues to implement functions of the data controllers as to a body which shall (if proportionate) be in charge of implementation of appropriate data protection policies. In the private sector, the accountability goes concretely with the expectations that companies shall implement certain appropriate technical and/or organisational measures to ensure they meet the GDPR requirements. Thus, individual implementation of various instruments is the standardized action leading to the self-regulation of the private sector through the GDPR. For explanatory purposes, the SDPI released recommendations and numerous guidelines to assist the private sector with the interpretation and application of the GDPR. In particular – (i) Recommendation on the Protection of Personal Data in the Context of Distance Healthcare; (ii) Recommendation on Processing of Personal Data of Employees by Organizing Work remotely; (iii) Recommendation to Small and Medium-sized Enterprises on the Application of the GDPR and etc. The most notable are the Recommendations for the Records of

⁵⁷⁵ *ibid.*

⁵⁷⁶ *ibid.*

⁵⁷⁷ Guidelines on Data Protection Officers (n 574).

Processing Activities.⁵⁷⁸ The recommendations included additional explanations and guidelines concerning Article 30 of the GDPR. Most importantly, the recommendation dispelled the widespread myth that companies with less than 250 employees are exempt from the obligation to maintain the records of processing and also, provide examples of which private bodies must regulate data protection and processing. In addition, SDPI frequently releases various guidelines, explanations and conducts conferences - all with the purpose of successful public education on self-regulation regarding data protection. By adaptation and issuance of such recommendations, guidelines, explanations and by organising conferences - the Lithuanian supervisory authorities promote self-regulation in the private sector and set the extent to which companies must regulate the personal data flow by themselves. To name a few examples - conduction of GDPR training for companies' employees internally; pseudonymisation of personal data which is processed internally at the company; the addition of annexes to contracts with contractors describing additional data protection conditions. Generalizing the information provided, the self-regulation of the Lithuanian private sector is automatized, and the supervisory authorities are allowed to act upon the regulations of the GDPR regarding general data protection to the extent, in which, the protected personal data is processed and protected correctly. Regarding the cooperation between the private and the public sectors of Lithuania – it is mostly apparent concerning cybersecurity. The Law on Cyber Security introduces inter-institutional cooperation regarding cybersecurity.⁵⁷⁹ The Law on Cyber Security institutes the Council of Cyber Security to monitor and analyse the current level of cybersecurity in Lithuania.⁵⁸⁰ One of the tasks of the Council of Cyber Security is to make proposals to cyber security for the public sector, businesses to cooperate in the field of cyber security.⁵⁸¹ The Law on Cyber Security itself promotes and provides the opportunity for the cooperation between the public and the private sector to maximize the security proportions of personal information.

4. What is the process of judicial review of cases of data protection breaches?

4.1. Is the right to data privacy defined in your legal system? If not, is it a part of another right protected by national law?

The Lithuanian legal system does not define the right to data privacy *expressis verbis*. However, such a right falls within the scope of protection of separately established - the

⁵⁷⁸ State Data Protection Inspectorate, Recommendation on records of data processing activities <<https://www.ada.lt/go.php/lit/Rekomendacija-del-duomenu-tvarkymo-veiklos-irau-2018-m>> accessed 16 February 2021.

⁵⁷⁹ The Law on Cyber Security of the Republic of Lithuania, No. XII-1428, approved on 11 December 2014, Article 1(1).

⁵⁸⁰ *ibid*, art. 4(2).

⁵⁸¹ *ibid*.

right to privacy and the right to data protection. In the Lithuanian legal system, such rights are protected by national-level laws, directly applicable EU (supranational) laws and ratified international laws.

Regarding the right to privacy, Lithuania is one of the 175 countries worldwide⁵⁸² that have recognised the right to privacy in the Constitution.⁵⁸³ On the level of basic national laws, the right is protected *inter alia* by Civil Code,⁵⁸⁴ Law on the Provision of Information to the Public⁵⁸⁵ and Criminal Code.⁵⁸⁶ Considering the international laws, the protection of a fundamental human right to privacy derives to the national legal system from various international laws such as the Universal Declaration of Human Rights,⁵⁸⁷ the International Covenant on Civil and Political Rights⁵⁸⁸, the Convention on the Rights of the Child,⁵⁸⁹ the Convention on the Rights of Persons with Disabilities⁵⁹⁰ and regional level acts such as the ECHR⁵⁹¹ and the Charter.

With regards to the definition of the right to privacy, the Constitutional Court of the Republic of Lithuania takes a similar approach to the ECtHR⁵⁹² and avoids giving a precise definition of the right to privacy. That results in the construction of a widely interpreted concept of private life⁵⁹³ in the national legal system.

The right to data protection, on the one hand, derives from and overlaps at certain aspects with the right to privacy, in the Lithuanian legal system primarily is protected by the GDPR. The main legal instrument regulating and stipulating general rules for protecting the right to data protection introduced by EU legislation, on the national level is supplemented by the Personal Data Protection Law⁵⁹⁴ and other laws such as Law on Legal Protection of Personal Data processed for the Prevention, Investigation, Disclosure or

⁵⁸² Comparative Constitutions Project

<https://www.constituteproject.org/search?lang=en&key=privacy&status=in_force>, accessed on 16 February 2021.

⁵⁸³ The Constitution of the Republic of Lithuania, art. 22.

⁵⁸⁴ Civil Code of the Republic of Lithuania, No. VIII-1864, approved on 18 July 2000, art. 2.23.

⁵⁸⁵ The Law on the Provision of Information to the Public of the Republic of Lithuania, No. I-1418, approved on 2 July 1996.

⁵⁸⁶ Criminal Code of the Republic of Lithuania, No. VIII-1968, approved on 26 September 2000.

⁵⁸⁷ Universal Declaration of Human Rights, adopted 10 December 1948 (UDHR), art. 12.

⁵⁸⁸ International Covenant on Civil and Political Rights, adopted 16 December 1966 (ICCPR), art. 17.

⁵⁸⁹ Convention on the Rights of the Child, adopted 20 November 1989, Article 16.

⁵⁹⁰ European Parliament resolution on the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities and the Optional Protocol [2010], OJ C184 E/111, art. 22.

⁵⁹¹ Convention for the Protection of Human Rights and Fundamental Freedoms [1953].

⁵⁹² Ehlers D., Becker U. *European Fundamental Rights and Freedoms*. (Berlin, 2007, 68–69).

⁵⁹³ Resolution of the Constitutional Court of the Republic of Lithuania on the compliance of Article 41(2) of the Code of Correctional Works of the Republic of Lithuania (wording of 2 July 1997) with the Constitution of the Republic of Lithuania, court ruling No. 3/01, 24 March 2003.

⁵⁹⁴ The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, adopted on 30 July 2018.

Prosecution of Criminal Offences, the Enforcement of Penalties or for National Security or Defence Purposes (transposing the Directive 2016/680)⁵⁹⁵ (Law No. 52-2511), Law on Electronic Communications (transposing the Directive 2002/58/EC),⁵⁹⁶ the Code of Administrative Offences⁵⁹⁷ and others. In contrast to the broad protection of the right to privacy on the international level, the right to data protection is only protected by the Charter and the Council of Europe (CoE) Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data.⁵⁹⁸

4.2. Can the data subject restrict or object the data processing? What are the circumstances and exceptions to this option?

Restriction and objection to the data processing are the data subject rights provided by the GDPR and the Law No. 52-2511 implementing Directive 2016/680.

The subject's right to restrict data processing is established by Article 18 of the GDPR and Article 14 of Law No. 52-2511 (implementing Article 16 of Directive 2016/680).

According to Article 18 of the GDPR, data subjects have the right to request the restriction of the processing of personal data about them in the following circumstances: (i) when the individual contested the accuracy of their personal data until that request is resolved; (ii) the data was unlawfully processed; (iii) the controller no longer needs the data, but the individual needs the controller to keep it to establish, exercise or defend a legal claim; or (iv) the data subject objected to the controller's processing under GDPR Article 21(1), and the controller is considering whether its legitimate grounds override those of the individual.⁵⁹⁹ If personal data is 'restricted', then the controller may only store the data.

Considering the exceptions to the restriction of the respective processing - the data controller may not further process the required data unless: (i) the individual consents; or (ii) the processing is necessary for the establishment of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important (EU or Member State) public interest.⁶⁰⁰

⁵⁹⁵ The Law on the Legal Protection of Personal Data processed for the Prevention, Investigation, Disclosure and Prosecution of Criminal Offences, Execution of Sentences and National Security or Defence of the Republic of Lithuania, No. XI-1336, adopted on 21 April 2011.

⁵⁹⁶ The Law on Electronic Communications of the Republic of Lithuania, No. IX-2135, adopted on 15 April 2004.

⁵⁹⁷ Code of Administrative Offences of the Republic of Lithuania, No. XII-1968, adopted on 25 July 2015.

⁵⁹⁸ European Commission Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] (CETS 108), art. 1.

⁵⁹⁹ Lydia F de la Torre, *The right to restrict processing under EU data protection law*

<<https://medium.com/golden-data/what-is-the-right-to-restrict-processing-under-eu-data-b6627db1319f>> accessed on 31 February 2021.

⁶⁰⁰ Right to erasure and right to restriction of processing

<<https://www.twobirds.com/~media/pdfs/gdpr-pdfs/34--guide-to-the-gdpr--right-to-erasure-and-right-to-restriction-of-processing.pdf?la=en>> accessed on 31 February 2021.

Article 14 of Law No. 52-2511 under its scope of applicability as well in a certain way provides the data subject with a right to restrict data processing. The mentioned article establishes that the data subject has a right to request the data controller to erase his personal data. However, where (i) the data subject contests the accuracy of personal data and their accuracy or inaccuracy cannot be confirmed or (ii) personal data must be retained for the purposes of evidence - the controller under such request for erasure, may only restrict the processing of personal data without erasing them. In such a way, this Article indirectly provides when the data subject is provided with a right to restrict data processing rather than erasure. Notably, the data controller (as it is understood by respective law) in this respect is provided with the quite broad and uncertain scope of possibilities not to accept such requests of the data subject and even not to provide with specified argumentation.

Concerning the right to objection, this data subject's right in the Lithuanian legal system is established and protected only by the GDPR. According to Article 21, the data subject has a right to object and ask to stop processing its personal data if it is being processed for the purpose of: direct marketing; scientific or historical research and statistics; own legitimate interest or in carrying out a task in the public interest/for an official authority. If the data subject objects to direct marketing, the data controller must stop using personal data and comply with such a request without asking for a fee.

With regards to the exceptions related to the right to object data processing, a data controller can continue to process one's personal data despite the objections, if: (i) in case of processing for scientific/historical research and statistics purposes, the processing is necessary for the performance of a task carried out for public interest reasons; (ii) in case of processing based on legitimate interests or on the performance of a task in the public interest/exercise of official authority, one can prove to have compelling legitimate grounds that override data subject's interests, rights and freedoms. Therefore, a balancing exercise is required.⁶⁰¹

4.3. In case of data protection breaches, what is the process to notify the data subject? Are there any exceptional grounds not to notify the data subject? If such grounds exist, what would be the ideal or optimal balance for necessity and proportionality?

4.3.1. Process to notify the data subject in case of data protection breaches

Lithuanian national legislation does not provide a separate *sui generis* regulation of the process to notify the data subject in case of data protection breaches other than directly

⁶⁰¹ Can I ask companies or organisations to stop processing my personal data? <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-organisation-stop-processing-my-personal-data_lt> accessed on 30 February 2021.

applicable or transposed EU legislation. Depending on the scope of applicability, notifications on personal data breaches shall be submitted to data subjects following Article 34 of the GDPR and Article 30 of the national Law No. 52-2511. Additionally, in accordance with the aforementioned laws, the SDPI has adopted a recommendation on the procedure for detecting, investigating, reporting and documenting breaches of personal data security (Recommendation).⁶⁰² The Recommendation provides the following summary guidance to the notification process of the data subject.

Where it is established that the breach has occurred and that there is a serious risk to the rights and freedoms of natural persons, the person responsible should immediately (recommended within 72 hours) inform the data subject whose rights and freedoms may be seriously compromised by the breach. The Recommendation precisely specifies the content and a way of the notification to the data subject. Data subjects should be directly informed of the breach and the message should be separated from other information sent. Where the provision of direct notification to a data subject would be disproportionately demanding, a breach may instead be made public or subject to a similar measure informing data subjects equally effectively. The controller should choose the means of notification to the data subject that maximise the possibility of adequately communicating information to all affected persons. The Recommendation suggests that the controller may choose several methods of reporting a breach to the data subject.⁶⁰³

4.3.2. Exceptional grounds not to notify the data subject

Article 32 of the Recommendation provides that in the event of a breach, notification to the data subject shall not be required if (i) the controller has implemented appropriate technical and organisational safeguards and those measures have been applied to personal data affected by the breach; (ii) immediately after the breach, the controller has taken measures to ensure that the rights and freedoms of individuals can no longer be seriously compromised; (iii) this would require disproportionate efforts to contact individuals (e.g. where their contact details have been lost as a result of the injury or first unknown). In such a case, the injury shall instead be made public or a similar measure shall be taken to inform data subjects equally effectively.

In addition to the afore-provided summarised exceptions, Article 30(5) of Law No. 52-2511 lays down further specified cases not to notify the data subject in cases falling under the scope of applicability of respective law. Notification to a data subject may be delayed, restricted or withheld in the cases provided for by national laws as long as it is

⁶⁰² Recommendation on the procedure for detecting, investigating, reporting and documenting breaches of personal data protection

<https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_ADSP_2018.pdf?fbclid=IwAR3Rh6u9E8zMPd0reheUB3C3zs8UI1ifdkEF4SchkjZBPoj2gI4mlJptbfc> accessed on 31 February 2021.

⁶⁰³ *ibid*, art. 25-31.

necessary and proportionate in a democratic society, taking into account the fundamental rights and legitimate interests of this natural person, in order to: (i) not interfere with official or legal investigations, investigations or procedures; (ii) not to prejudice the prevention, investigation, detection or prosecution of criminal acts or the execution of sentences; (iii) ensure public safety; (iv) ensure national security, and (v) protect the rights and freedoms of others.

4.3.3. Ideal or optimal balance for necessity and proportionality

The process of notifying the data subject of data protection breaches in the Lithuanian legal system is based on directly applicable and transposed EU legal acts described above. In this way, the balancing of proportionality and necessity in the laid down procedures is directly dependable on the EU legislative process. Therefore, whereas no national rulings or other kinds of official interpretations or commentaries to the laws are directly relevant to this matter, this section regarding balancing the principles of necessity and proportionality in formulating obligations and their exceptions to inform the data subject of data protection breaches shall only contain general considerations of the author.

Considering necessity and proportionality balance, there is an inherent issue of materially different threats to a person arising from different infringements and, accordingly, of the existence of actual damage (material or intangible). In other words, regardless of the generality of an established notification procedure, in practice, different breaches of personal data can lead to substantially different levels of potential harm to a particular data subject. Therefore, the optimal balance for necessity and proportionality in practice is directly dependable on individual data protection breach. A data controller who accidentally sends an e-mail message to a broad group of persons without hiding each of unrelated data subjects' personal data (such as the name and email address, as well as their relationship with the personal data controller) is liable for a breach practically resulting e-mail addresses being used for direct marketing without the prior consent of individuals. In another case, the data processor is liable for the extensive leakage of the database, resulting in the theft of individuals' identities leading to significant material and intangible harm. Regardless of liability matters, in such different situations, there is a risk of consequences of an absolutely different magnitude. Yet, in case any data protection breach (as it is defined) occurs, the notification procedure for an infringement is generally the same. Such material differences of potential risks lead to the broad scope of possible proportionality and necessity standards relatively optimal for each separate case. The obligation to notify the data subject of ideal necessity and proportionality balance should address the situations where the influence on the personal rights and the potential harm caused by the breach of personal data would be relatively material to the data subject concerned.

5. Does the review constitute effective protection of data privacy?

In Lithuania surveillance of protection of data privacy is constituted mainly by SDPI. As mentioned before, the SDPI field of actions consists of preventive inspections, audits, research and analysis and monitoring of legal regulation.⁶⁰⁴ In Article 11 of the Personal Data Protection Law is defined tasks and functions of SDPI: provide advice on the protection of personal data and privacy, as well as methodological recommendations on the protection of personal data; cooperate with other supervisory authorities and organizations for the protection of personal data; participate in and implement public policy in the field of personal data protection; implement the provisions of the Convention on the Protection of Persons in connection with the Automated Processing of Personal Data (ETS No 108) and its Protocols concluded in Strasbourg on 28 January 1981.⁶⁰⁵ Since GDPR came into force in 2018, SDPI carried out inspections of processing of personal data for direct marketing and loyalty program purposes, legality of the processing of biometric data in gyms, hotel inspections on the implementation of the principle of reduction of personal data in the processing of guests' personal data, summary of inspections of rental companies on the implementation of the principle of data minimisation in the processing of personal data to conclude and enforce a rental agreement.⁶⁰⁶

Personal data protection supervision activities are executed by OIJE, when personal data are processed for journalistic or academic, artistic or literary purposes (e.g., personal data is published on a website or local newspaper, Google displays insignificant personal data or a photo is posted on Facebook without a person's consent). OIJE's activity involves the following: (i) examination of complaints (applications) from individuals and violation of regulatory laws governing provision of information to the public; (ii) monitoring and analysis of public information; (iii) public information expertise; (iv) cooperation with other institutions, public education and consulting; (v) Drafting and provision of proposals for laws and other legal acts.⁶⁰⁷ Right now there might be a problem with the current system of punishing which is implemented by this body. When OIJE detects an infringement, it gives a warning according to Article 50(3)(1) of the Law on the Provision of Information to the Public. But OIJE also imposes a penalty in accordance with GDPR. This presupposes the situation of *non bis in idem*. The question of possible double punishment right now is in the Supreme Administrative Court of Lithuania.

⁶⁰⁴ The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, adopted on 30 July 2018, art. 7(1).

⁶⁰⁵ *ibid*, art. 11.

⁶⁰⁶ Summaries of inspection results of SDPI

<<https://vdai.lrv.lt/lt/patikrinimu-rezultatu-apibendrinimai/vdai-patikrinimu-rezultatu-apibendrinimai>> accessed on 30 February 2021.

⁶⁰⁷ The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. XIII-1426, adopted on 30 July 2018, art. 7(2).

To summarise Lithuania has two bodies that conduct protection of data privacy SDPI and OIJE. The competence of these bodies is divided into fields of interests.

In Lithuania, the process of judicial review for cases of data protection breaches starts when SDPI receives a persons' notice of infringement. Upon receiving information about a data protection breach, the SDPI evaluates the submitted information and decides whether an investigation is necessary. Infringements of the GDPR may lead to administrative penalties, which must be effective, proportionate and dissuasive in each case. Article 31(5) of the Personal Data Protection Law constitutes that SDPI's decisions can be appealed to a court under the procedure established by the Law on Administrative Proceedings.⁶⁰⁸

To conclude, in Lithuania the process of judicial review for cases of data protection breaches is implemented by administrative proceedings.

It is hard to evaluate the effectiveness of remedies to data protection breaches. This is because currently in Lithuania there is no systemic analysis of data about data protection status and effectiveness. However, based on publicly available information it can be declared that bodies that are responsible for data protection are doing their duties since fines are being imposed and data protection breaches are being moderate. On the other hand, recently, Lithuania had one of the biggest data leaks in decades.⁶⁰⁹ During the hack, a backup copy of customers data was stolen and made public on the black market. The investigation has just begun so it is unclear what remedies SDPI will impose on the company.

All in all, remedies are effective in order to prevent companies from repeating mistakes, but it does not preclude an irresponsible mentality about data protection and cyber-security.

SDPI publishes annual reports about its activity. They show that no fines have been imposed in the first year of GDPR implementation in 2018 three fines were imposed in 2019 and more than twenty fines in 2020. It can be concluded that supervision of data protection becomes more and more active every year. A couple of more noticeable fines can be mentioned. The first fine of € 61,500 was imposed in 2019 on MisterTango, which operates internationally and provides payment services to Lithuanian and foreign residents and companies. The fine was 1.5% of company turnover. The company violated Articles 5, 32 and 33 of GDPR.⁶¹⁰ More specifically the company did not properly process personal

⁶⁰⁸ *ibid*, art. 31(5).

⁶⁰⁹ Hackers target CityBee, sensitive data of 110 000 users leaked
<<https://www.lrt.lt/en/news-in-english/19/1345986/hackers-target-citybee-sensitive-data-of-110-000-users-leaked>> accessed on 30 February 2021.

⁶¹⁰ The company's liability will not escape – a significant fine imposed in Lithuania for violations of the General Data Protection Regulation
<<https://vdai.lrv.lt/lt/naujienos/imonės-atsakomybės-neisvengs-lietuvoje-skirta-zenkli-bauda-uz-bendrojo-duomenų-apsaugos-reglamento-pažeidimus>> accessed on 30 February 2021.

data: it processed too much data, stored it for longer than it had established itself. Also, it has made personal data public. Furthermore, MisterTango did not provide a report of a breach of personal data security. The second fine of € 15,000 was imposed in 2020 on Vilnius City Municipality Administration because it improperly processed the personal data of the parents of the adopted child.⁶¹¹ Apart from fines, data protection authorities may issue warnings and orders to implement corrections of existing breaches in the system.

In conclusion, the main sanctions are warnings and orders to make corrections, but from time-to-time fines are being imposed. The review constitutes effective protection of data privacy. However, the system is not perfect and has to be improved especially by improving companies' moderation and encouraging Lithuania business to be more serious about data protection.

6. What is the process of judicial review of anti-discrimination cases?

Despite the fact that soft legislation related to technological development is limited, it could be clearly stated that Lithuanian authorities recognize the idea that advanced technologies (such as ADT) can lead to discrimination and bias in automatic decision-making and risk evaluation processes.⁶¹² Although, according to Country Reports on Non-Discrimination of the Republic of Lithuania annually submitted to the European Commission,⁶¹³ the legal framework in the context of non-discrimination in relation to the increased use of technologies in everyday life has not changed over the last five years. Respectively, the legislation of the Republic of Lithuania does not provide any specific

⁶¹¹A fine has been imposed under the General Data Protection Regulation for improperly processing the personal data of the adopted child's parents <https://vdai.lrv.lt/lt/news/view_item/id.143> accessed on 30 February 2021.

⁶¹² Lithuanian Artificial Intelligence Strategy
<[https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT\(1\).pdf](https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf)> accessed on 30 February 2021.

⁶¹³ Country report Non-discrimination Transposition and implementation at national level of Council Directives 2000/43 and 2000/78 Lithuania 2020
<<https://www.equalitylaw.eu/downloads/5297-lithuania-country-report-non-discrimination-2020-2-81-mb>>; Country report Non-discrimination Transposition and implementation at national level of Council Directives 2000/43 and 2000/78 Lithuania 2019
<<https://www.equalitylaw.eu/downloads/5015-lithuania-country-report-non-discrimination-2019-pdf-1-77-mb>>; Country report Non-discrimination Transposition and implementation at national level of Council Directives 2000/43 and 2000/78 Lithuania 2018
<<https://www.equalitylaw.eu/downloads/4752-lithuania-country-report-non-discrimination-2018-pdf-2-50-mb>>; Country report Non-discrimination Transposition and implementation at national level of Council Directives 2000/43 and 2000/78 Lithuania 2017
<<https://www.equalitylaw.eu/downloads/4482-lithuania-country-report-non-discrimination-2017-pdf-1-84-mb>>; Country report Non-discrimination Transposition and implementation at national level of Council Directives 2000/43 and 2000/78 Lithuania 2016
<<https://www.equalitylaw.eu/downloads/3737-lithuania-country-report-non-discrimination-2016-pdf-1-35-mb>> accessed on 26 February 2021.

regulation on the judicial review of technology-driven anti-discrimination cases. This means that in the case of the infringement of the principle of non-discrimination as a result of faulty technologies and/or algorithms will be judicially reviewed in accordance with the general procedure.

Such a general procedure means that in the event of a case of discrimination related to technology, the entity that will examine the dispute in the pre-trial procedure will be determined precisely according to the area where such violation occurred. For instance, under Article 216 of the Labour Code⁶¹⁴ in case of discrimination cases related to employment relations a person may apply to the labour disputes commissions or courts directly. Meanwhile, in the area of public administration (i.e. in relation to social protection, social advantages, education and access to and the supply of goods and services available to the public) a person who believes that his/her rights have been infringed by individual administrative actions or by the actions (or omissions) of civil servants or municipal employees has the right to file a complaint with the Administrative Disputes Commission under the Law on Administrative Disputes Commissions of the Republic of Lithuania, or with the administrative courts under the Law on Administrative Procedure of the Republic of Lithuania.

However, given that the faster pace of technological development is most visible in the private sector, such technology-driven discrimination cases are likely to be brought before the Equal Opportunities Ombudsperson, a quasi-judicial body with the broadest powers in regard to the discrimination, under Article 24(1) of the Law on Equal Treatment of the Republic of Lithuania. In particular, the competence of this institution is limited to the grounds of discrimination as provisioned by laws and the forbidden discrimination domains such as activities related to the state and municipal institutions and agencies, educational establishments, research and education providers, employment of all types of ownership, sellers or producers of goods and providers of services, organisations of employers or employees, organisations. Moreover, since 2005, the Equal Opportunities Ombudsperson is considered to be the national equality body in terms of Article 13 of the Racial Equality Directive 2000/43/EC.

Besides the general decision to address an appropriate person and make a proposal to discontinue the actions (inactions) violating equal rights, in the course of the investigation the Equal Opportunities Ombudsperson may take a decision to initiate administrative proceedings resulting in appropriate fines. Decisions of the Equal Opportunities Ombudsperson to apply administrative sanctions are binding, although they can be overruled by a court.

⁶¹⁴ Labour Code of the Republic of Lithuania, No. XII-2603, adopted on 19 September 2016, art. 216.

Nonetheless, the Law on Equal Treatment of the Republic of Lithuania⁶¹⁵ and Law on Equal Opportunities for Women and Men of the Republic of Lithuania⁶¹⁶ additionally constitute that a person who has suffered discrimination shall have the right to claim compensation for the pecuniary and non-pecuniary damage from the persons guilty thereof in the manner prescribed by laws in the civil courts of the Republic of Lithuania. In addition to the compensation (civil liability) explicitly specified in the laws, other civil remedies provided for in the Civil Code may be also applied to protect violated rights by civil remedies (e.g. preventive action, a claim to put an end to the unlawful actions, etc.).

Despite such a wide range of options for defence against discrimination, the Lithuanian case-law does not include any cases related to the violation of the prohibition of discrimination based on technological developments, as well as any cases with some significance for the interpretation of the principle of equal treatment, the role of the technical aspects that result in discrimination, or discrimination related to the technologies *per se*. Respectively, at present, it is not possible to assess which aspects (technical or other) the Equal Opportunities Ombudsperson and/or court would consider more significant (if any) in technology-related cases and whether judicial review by the Ombudsperson and/or courts is effective in protection against discrimination in such cases, as Lithuanian society has so far not been inclined to defend its rights violated as a result of the use of technology to dispute resolution institutions.

7. Does your country have any specific regulations on Advanced Digital Technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?

The Lithuanian legislative system does not include any specific regulations on any ADT and does not provide any specific definitions of ADT in general, as well as its separate elements. Since Lithuania is a part of the EU, the recommendations, policies and general principles established on the state-of-the-art technologies at the EU level are considered as sufficient soft tools for the regulation of these trending technological solutions and to this date, no relevant changes in legislation in relation to technological development have been introduced. On the other hand, considering the indifference of the Lithuanian legislator to the development of new legal acts related to the ADT, it can be assumed that in Lithuania ADT themselves are not perceived as a completely new object for which it is necessary to create a fundamentally new regulation, i.e. it is considered that the existing national regulation covers the legal issues raised by the ADT.

⁶¹⁵ The Law on Equal Opportunities of the Republic of Lithuania, No. IX-1826, adopted on 18 November 2003, art. 13.

⁶¹⁶ The Law on Equal Opportunities for Women and Men of the Republic of Lithuania, No. VIII-947, adopted on 1 December 1998, art. 18.

A contrasting situation emerges regarding the soft national regulations. In the autumn of 2018, the Ministry of Economy and Innovation of the Republic of Lithuania and the expert group launched meetings and active discussions on the influence of AI technologies and the importance of AI in the country. The main goal of such public discussions was to set guidelines for the development of AI in Lithuania and to submit specific strategies and proposals. As a result, in 2019 ‘Lithuanian Artificial Intelligence Strategy: a vision for the future’ was shaped and an expert group is now still continuing the work by regulating the AI development and ensuring acting in accordance with recommendations provided in the strategy.⁶¹⁷ The core ethical and legal principles given to the state under the strategy are as follows: (i) to advise the public sector on ethical AI regulation and implementation; (ii) to increase public confidence in AI technologies and the rules, laws and regulations governing the development and use of responsible AI; (iii) to encourage transparency and fairness in AI applications; and (iv) to encourage conscious ethics. It is expected that the mentioned strategy and its tools will ensure the sustainable development of the field of AI in Lithuania and enable Lithuania to be competitive in the global market.

In addition to the mentioned above, in 2019 the AI Association was established which is a community of professionals and enthusiasts dedicated to promoting and encouraging AI integration and development in Lithuania. From the date of its establishment, this NGO dedicates its efforts to partnerships between the academic and private sectors, as well as government and public sectors. Moreover, this private initiative is representing the AI community in formulating and expressing guidelines for national AI strategy, including the ethics, legal questions of AI.

In addition to the above, the Lithuanian government bodies also have taken the first steps towards the regulation of ADT. In 2021, the Ministry of Economy and Innovation has announced the establishment of the Innovation Council, with the main goal to advise and adopt decisions on the development and implementation of new innovations and digital policies.

Generally, although Lithuania has not adopted any binding regulations regarding ADT, it seems that such changes in the regulation of ADT are planned to be implemented in the near future. In any case, it is evident that Lithuania will follow not only the recommendations of the above-mentioned public and private initiatives but also the established principles and general guidelines provided at the EU level, as from the publicly

⁶¹⁷ Alex Moltzau, *Lithuanian Artificial Intelligence Strategy 2019*
<<https://alexmoltzau.medium.com/lithuanian-artificial-intelligence-strategy-2019-919ded83cc86>> accessed on 30 February 2021.

available data⁶¹⁸ the Lithuanian institutions seek to improve Lithuania's position in the Digital Economy and Society Index measured in Europe.

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?

The case-law of the courts of the Republic of Lithuania explicitly states that 'control, recording and accumulation of information transmitted by electronic communication networks may be permitted only on the grounds and in accordance with the procedure laid down by law by a reasoned court ruling and in compliance with the requirements of proportionality'.⁶¹⁹

In regard of criminal investigations, the conditions for the lawful control, recording and accumulation of information transmitted by electronic communication networks is defined in Article 154 of the Code of Criminal Procedure of the Republic of Lithuania⁶²⁰ (Code of Criminal Procedure). This Article establishes that in order for pre-trial investigation officer to be able to lawfully listen to a person's private correspondence transmitted by electronic communication networks, make their records, control and record other information transmitted by electronic communication networks (including the encrypted/decrypted personal messages) it is necessary for the prosecutor in charge of the pre-trial investigation to approach the pre-trial judge with such a request and receive a positive ruling of the court. Such a positive ruling shall be taken when a pre-trial investigation judge assesses the circumstances presented in the prosecutor's request and establishes that there is a legitimate basis for an action of the extent requested. The judge's personal assessment is limited to a number of alternative conditions (the existence of at least one of which is necessary) provided for in the same Article of the CCP. Respectively, the judge may authorise the conduct referred to above actions only if (i) there is a legitimate basis for believing that data can be obtained on (a) a grave serious, serious or less serious crimes; or (b) specific minor offences listed in the Code of Criminal Procedure; or (ii) there is a risk of violence, rape or other illegal acts being conduct against the victim, witness or other participants in the proceedings or their relatives.

Different grounds for covert control of personal correspondence and other communications, as well as control and recording of the content of personal information transmitted via electronic communication networks during the criminal intelligence

⁶¹⁸ The Ministry of Economy and Innovation establishes the Innovation Council
<<https://eimin.lrv.lt/lt/naujienos/ekonomikos-ir-inovaciju-ministerija-steigia-inovaciju-taryba>> accessed on 30 February 2021.

⁶¹⁹ Judgment of the Court of Appeal of the Republic of Lithuania on 8 December 2020, civil case no. 2A-823-370.

⁶²⁰ Code of Criminal Procedure of the Republic of Lithuania, No. IX-785, adopted on 14 March 2002, art. 154.

investigations, are provided in the Law on Criminal Intelligence (Law on CI).⁶²¹ Under Article 8(1) of the Law on CI, such control is allowed only then: (i) there is already obtained information on (a) a grave serious, serious or less serious crimes listed in the Law on CI being prepared, being committed or committed or (b) on the persons involved in these crimes; or (ii) the suspect, accused or convicted person is in hiding; or (iii) the person disappears without knowledge; or (iv) the protection of persons against criminal effects is being conducted; or (v) the organised crime prevention measures are applied against a member of an organised crime group or a person associated with it. In the general procedure, the above-mentioned actions may be lawfully conducted only if there is a reasoned court ruling.⁶²² In urgent cases where human life, health, property, public or state security is endangered (the exact list of such cases is not regulated by law), the above-specified actions may be performed in accordance with the decision of the prosecutor which must be approved by a court ruling no later than 24 hours after the adoption of such a decision.⁶²³

The above regulation, unfortunately, does not provide for a requirement to decrypt the encrypted personal correspondence and make it accessible for criminal investigations/intelligence. The ruling which allows the pre-trial investigation officer to control, record and accumulate the information transmitted by electronic communication networks that may include encrypted/decrypted personal messages typically provides only the following information: (i) available data on the person against whom the actions are to be taken; (ii) data justifying the need for the permitted actions; (iii) the specific actions that are permitted; and (iv) duration of the permitted actions. This means that access to the content of the encrypted information collected during the criminal investigations/intelligence no longer is considered as a matter of the court but of the pre-trial investigation or criminal intelligence officer himself/herself. And although there is little information in the public sphere about the decryption capabilities of the Lithuanian criminal investigation/intelligence institutions, in the context of cybercrime investigations it was publicly noted that in practice the encryption is a factor that complicates the fight against crime and its prevention in Lithuania.⁶²⁴ Notwithstanding the fact that the Lithuanian criminal investigation/intelligence officers are using Europol's decryption resources and services, the following difficulties influencing the success of criminal investigations, are identified: (i) a lack of special hardware and software for data and data

⁶²¹ The Law on Criminal Intelligence of the Republic of Lithuania, No. XI-2234, adopted on 20 October 2012.

⁶²² *ibid*, art. 10(1).

⁶²³ *ibid*, art. 10(2).

⁶²⁴ The seventh phase of the peer review 'European Cybercrime practical policies for preventing and combating such crimes implementation and operation'. Evaluation report - Report on Lithuania [2016] (6520/1/16 REV 1 DCL 1), 58.

carriers decryption in the criminal investigation institutions; and (ii) a lack of cooperation in the decryption processes with private companies and the private sector experts.⁶²⁵

When assessing the adequacy of Lithuanian regulation, it should be noted that in connection with Article 8 of the ECHR, Article 22 of the Constitution establishes that information about a person's private life (including the personal correspondence) may be collected only by a reasoned court ruling and only according to the law. On the basis of the regulation and practice, it can be concluded that despite the fact that the access to the private correspondence of a person is restricted by grounds and procedures laid down by law, the same law leaves considerable space for the self-action of Lithuanian criminal investigation/intelligence institutions because such processes as decryption which are particularly relevant are not defined anywhere. This thought can also be supported by the case-law of the ECtHR, repeated in the courts of the Republic of Lithuania⁶²⁶, which states that, in the light of technological progress, clear, detailed rules are essential for this type of legislation.⁶²⁷

In addition, although the CCP and the Law on CI provide for the obligation of entities providing electronic communication networks and/or services to create conditions for control, recording and accumulation of the information transmitted by electronic communication networks, the recent case-law of the CJEU examining the concept of electronic communication networks and services also raises a number of doubts.^{628,629} According to the mentioned case-law, web-based services which do not themselves provide internet access (e.g. Gmail service provided by Google LLC) should not be considered as electronic communication services. And in the context of the control and collection of personal correspondence, this explanation may lead to situations where specific service providers will refuse to provide the requested information to the criminal investigation/intelligence officers and/or will not contribute to the decryption of such information, and the Lithuanian legislation will not be sufficient for the legal enforcement of such actions or even general validity of conduction of the control and collection.

⁶²⁵ *ibid.*

⁶²⁶ Ruling of the Supreme Court of the Republic of Lithuania on 1 June 2015, criminal case No. 2K-P-94-895/2015

<<http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=002b0d9a-1b50-41e6-be0a-28654380063b>>

⁶²⁷ *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, (62540/00) [2007] (28 June 2007).

⁶²⁸ Judgment of the Court, requesting for a preliminary ruling under Article 267 TFEU from the Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Higher Administrative Court for the Land of North Rhine-Westphalia, Germany), made by decision of 26 February 2018, received at the Court on 19 March 2018, in the proceedings, case No. C-193/18, 13 June 2019.

⁶²⁹ Judgment of the Court, requesting for a preliminary ruling under Article 267 TFEU from the cour d'appel de Bruxelles (Court of Appeal, Brussels, Belgium), made by decision of 7 February 2018, received at the Court on 23 February 2018, in the proceedings, case No. C-142/18, 5 June 2019.

Besides the above, in order to protect the individuals in the circumstances which allow the control and collection of personal correspondence the Lithuanian legislation provides a few protection measures. For instance, the CCP and the Law in CI emphasise that the restrictions on human rights addressed in this section are temporary and provide the statutory limitation periods during which the control, recording and accumulation of information transmitted by electronic communication networks can be conducted.^{630,631,632} Also, considering the possible information sensitivity, it is regulated that the collected data not directly relevant to the criminal investigation⁶³³ and information collected during criminal intelligence, when information about a person's criminal acts has not been confirmed or when the purposes of the criminal intelligence cannot be achieved,⁶³⁴ should be destroyed. In case the above-mentioned measures exclusively based on the internal assessment of criminal investigation institutions do not fully protect the individual, the Lithuanian legislation allows the individual to defend the violated rights by civil remedies provided for in the Civil Code. Moreover, as an *ultima ratio* measurement,⁶³⁵ states that the unlawful collection of information about a person's private life (including the collection of private correspondence and its decryption) could entail criminal liability not only when it is conducted by persons not entitled to conduct such actions but also when it is conducted by the officers who breach their authority or violate a court-sanctioned data collection procedure.⁶³⁶

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?

The Lithuanian national authorities show reluctance to take steps towards more advanced human rights protection or towards more possibilities for technological developments.

Despite this lack of national regulation, Lithuania is developing a more advanced GDPR enforcement mechanism in order to protect data of individuals. As described above, SDPI is more active in recent years in performing investigations of the companies and imposing fines, even though warnings are a way more popular sanction for data protection standards violations. However, compared with activity of other data protection authorities across the EU, Lithuanian supervisory authority does not provide as significant judicial review as could be expected. On the other hand, it is more convenient for businesses to feel safer

⁶³⁰ Code of Criminal Procedure of the Republic of Lithuania (n 620) art. 154(4).

⁶³¹ The Law on Criminal Intelligence of the Republic of Lithuania (n 621) art. 10(5).

⁶³² *ibid*, art. 10(6).

⁶³³ Code of Criminal Procedure of the Republic of Lithuania (n 620) art. 154(8).

⁶³⁴ The Law on Criminal Intelligence of the Republic of Lithuania (n 621) art. 5(7).

⁶³⁵ Criminal Code of the Republic of Lithuania (n 586) art. 166(1).

⁶³⁶ Criminal liability for personal privacy Violations of the privacy of European Human rights court and Lithuanian courts In the context of case law
<https://teise.org/wp-content/uploads/2016/06/Meskauskaite-Lankauskas-2016_1.pdf>, 74.

while developing digital advanced technologies that need huge amounts of data. This way they may expect less possibilities for proceedings before the authorities.

As mentioned above, in Lithuania self-regulation of companies regarding balance between digital technologies and human rights protection is of core importance. With lack of stricter national regulation and enforcement of GDPR, the most effective measure for protection of human rights should be considered individual company's willingness to develop technologies in the least intrusive way for individual rights.

To conclude, it could be said that in Lithuania the balance between allowing digital advancements and protecting human rights online is largely left to private actors because despite growing importance of GDPR requirements national authorities still lack a willingness to limit developments of ADT.

10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the upcoming five years?

Regarding protection of human rights online, it must be said that perspectives of legislation may be analysed from national and international perspectives.

At EU level one of the most recent examples is the E-privacy directive.⁶³⁷ Only in February of 2021 the European Council agreed on the draft of the E-Privacy regulation which provides users with more transparency, legal certainty and inclusion of GDPR standards into this regulation compared with its predecessor E-Privacy directive. Having the legal obligation to apply EU regulations directly, Lithuania will be legally bound by such updates in the E-Privacy field as well.

Another important point at international level is soft-law sources. At EU level European Data Protection Board (EDPB) does the most important explanatory work which provides EU entities with clearer GDPR standards' interpretation. However, guidelines of the EDPB should move forward and reflect more ongoing challenges for privacy and data protection rights - for example, legal opinions on growing businesses of data scraping, etc. Another soft-law development source is the CoE initiatives. At the CoE there is Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data⁶³⁸ which, of course, does not provide as high standards for data protection as GDPR does. However, initiatives at the CoE level are of core importance as for many

⁶³⁷ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2021] (5008/21).

⁶³⁸ European Commission Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] (Series No. 108).

member states GDPR is not applicable, therefore, the need to harmonize protection of individuals is significant for better cooperation between the EU and non-EU states. CoE initiatives also include consultative guidelines, aggregated data protection reports and other important soft-law sources.

As for autonomous legislation in Lithuania, it must be said that not lack of legal framework is the major problem in human rights protection but lack of judicial enforcement. Therefore, first steps shall be made towards creating a more effective judicial enforcement mechanism, first of all, in terms of activity of the SDPI. Another important factor shall be the development of soft-law sources from the same national supervisory authority. With growing incidents of data breaches Lithuanian companies, especially the ones that do not have DPOs, face difficulties with interpreting requirements of GDPR and Personal Data Protection Law. More accessible sources with interpretative guidance would lead companies to more clearness and better possibilities to balance protection of human rights and business interests while developing solutions that include ADT.

Conclusion

The protection of private information in the Lithuanian legal system is ensured by the legislation based mainly on the international and EU legal acts. The EU GDPR, following its scope of application, with supplementary national legislation, plays an essential role in the protection of personal data in the age of ADT. Regardless of the lack of fines and other enforcement measures taken by the SDPI, the private sector continues to adapt to the current legislation by establishing various technical or managerial instruments to remain lawful in front of the supervisory authorities of the Republic of Lithuania. Self-regulation of the private sector is standardized throughout the adaptation of the GDPR accountability principle and the cooperation of DPO's and the supervisory authorities of the Republic of Lithuania. The right to data privacy in the Lithuanian legal system falls within the scope of protection of separately established - the right to privacy and the right to data protection. Such rights are protected by national laws, directly applicable EU (supranational) laws and ratified international laws. The circumstances and exceptions to the data subject rights to restrict and to object data processing, as well as notifications on personal data breaches, are in detail provided by the GDPR and the Law No. 52-2511 implementing Directive 2016/680 in respect of the scope of application of each. Regardless of the generality of an established data subject notification of data protection breaches procedure, in practice, material differences of potential risks lead to the broad scope of possible proportionality and necessity standards relatively optimal for each separate case. Considering the effective protection of data privacy, remedies are effective to prevent companies from repeating mistakes, yet it does not preclude an irresponsible mentality about data protection and cyber-security. Main sanctions are warnings and orders to make corrections, but from time

to time, fines are being imposed. This proves that the system is imperfect and has to be improved. However, the case-law related to the violation of the prohibition of discrimination based on technological developments is still absent. That leaves rather an uncertainty that will persist until any relevant cases arise. Moving forward, specific ADT regulations or relevant adoptions of the legislation in force might be adopted or rather derive from international/EU legislation. In the Lithuanian legal system, any regulation, unfortunately, does not provide for a requirement to decrypt the encrypted personal correspondence and make it accessible for criminal investigations. Despite the fact that the access to the private correspondence of a person is restricted by grounds and procedures laid down by law, the same law leaves considerable space for the self-action of Lithuanian criminal investigation institutions. To protect the individuals in the above-mentioned circumstances, the Lithuanian law provides a few protection measurements, e.g. (i) limits time for during which the control, recording and accumulation of information transmitted by electronic networks can be conducted; (ii) recorded/collected data which is not relevant to the criminal investigation should be destroyed immediately and not be included in the case; (iii) unlawful collection of information about a person's private life (including the collection of private correspondence and its decryption) entails criminal liability. The balance between allowing digital advancements and protecting human rights online is largely left to private actors. Despite the growing importance of GDPR requirements, national authorities still are in a way of a lack of willingness to limit unsecured and undefined developments of ADT. Fast-paced ADT market calls for clear guidelines to ensure compliance in serving society's needs and private interests. Detailed and up-to-date supporting soft law sources with interpretative guidance, effective judicial enforcement mechanisms and pro-active supervisory authority are essential to lead society and business to more clearness and better possibilities to balance the protection of human rights and business interests in the rapid development of ADT solutions.

Table of legislation

Provision in Lithuanian	Corresponding translation in English
Lietuvos Respublikos Konstitucija, 22 straipsnis: Žmogaus privatus gyvenimas neliečiamas. Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami. Informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą. Įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsینimosi į jo garbę ir orumą.	The Constitution of the Republic of Lithuania, Article 22: The private life of a human being shall be inviolable. Personal correspondence, telephone conversations, telegraph messages, and other communications shall be inviolable. Information concerning the private life of a person may be collected only upon a justified court decision and only according to the law. The law and the court shall protect everyone from arbitrary or unlawful interference in his private and family life, from encroachment upon his honour and dignity.
Lietuvos Respublikos Konstitucija, 26 straipsnis Minties, tikėjimo ir sąžinės laisvė yra nevaržoma. Kiekvienas žmogus turi teisę laisvai pasirinkti bet kurią religiją arba tikėjimą ir vienas ar su kitais, privačiai ar viešai ją išpažinti, atlikinėti religines apeigas, praktikuoti tikėjimą ir mokyti jo. Niekas negali kito asmens versti nei būti verčiamas pasirinkti ar išpažinti kurią nors religiją arba tikėjimą. Žmogaus laisvė išpažinti ir skleisti religiją arba tikėjimą negali būti apribota kitaip, kaip tik įstatymu ir tik tada, kai būtina garantuoti visuomenės saugumą, viešąją tvarką, žmonių	The Constitution of the Republic of Lithuania, Article 26: Freedom of thought, conscience and religion shall not be restricted. Each human being shall have the right to freely choose any religion or belief and, either alone or with others, in private or in public, to profess his religion, to perform religious practices, to practice and teach his belief. No one may compel another person or be compelled to choose or profess any religion or belief. Freedom of a human being to profess and spread his religion or belief may not be limited otherwise than by law and only when this is necessary to guarantee the security of

sveikata ir dorovę, taip pat kitas asmens pagrindines teises ir laisves. Tėvai ir globėjai nevaržomi rūpinasi vaikų ir globotinių religiniu ir doroviniu auklėjimu pagal savo įsitikinimus.	society, the public order, the health and morals of the people as well as other basic rights and freedoms of the person. Parents and guardians shall, without restrictions, take care of the religious and moral education of their children and wards according to their own convictions.
Lietuvos Respublikos teisėkūros pagrindų įstatymas, Nr. XI-2220, 7 straipsnis: 1. Konsultavimosi su visuomene tikslas – užtikrinti teisėkūros atvirumą, skaidrumą, sužinoti visuomenės nuomonę apie teisinio reguliavimo problemas ir jų sprendimo būdus, sudaryti visuomenei galimybę daryti įtaką teisės akto projekto turiniui, geriau įvertinti numatomo ir galiojančio teisinio reguliavimo teigiamas ir neigiamas pasekmes, jo įgyvendinimo sąnaudas, teikti pasiūlymus dėl Teisės aktų informacinėje sistemoje paskelbtų teisėkūros iniciatyvų ir teisės aktų projektų, taip pat dėl galiojančio teisinio reguliavimo, kurio poveikio ex post vertinimas atliekamas. 2. Su visuomene turi būti konsultuojamasi laiku ir dėl esminių klausimų (konsultavimosi efektyvumas), taip pat tiek, kiek yra būtina (konsultavimosi proporcingumas). 3. Konsultavimosi su visuomene būdus ir rezultatų informavimo būdus pasirenka konsultavimasi su visuomene inicijuojantys subjektai. Informacija apie konsultavimosi su visuomene rezultatus turi būti teikiama teisės aktą priimančiam subjektui ir skelbiama viešai Teisės aktų informacinėje sistemoje.	The Law on Legislative Framework of the Republic of Lithuania, XI-2220, Article 7: 1. The purpose of public consultation is to ensure openness and transparency of legislation, to find out public opinion on legal regulation problems and their solutions, to enable the public to influence the content of draft legislation, to better assess the positive and negative consequences of planned and existing legal regulation, its implementation costs, to provide proposals for legislative initiatives and draft legislation published in the Legislation Information System, as well as for existing legislation subject to ex post impact assessment. 2. The public must be consulted timely and on substantive issues (effectiveness of consultation), as well as to the extent necessary (proportionality of consultation). 3. The methods of public consultation and the presentation of the results shall be chosen by the entities initiating the public consultation. Information on the results of the public consultation must be provided to the legislator and made public in the Legislation Information System.

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Nr. I-1374, 1 straipsnio 3 dalis: Šis įstatymas taikomas kartu su Reglamentu (ES) 2016/679 ir jo įgyvendinamaisiais teisės aktais.	The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, Article 1(3): This Law shall apply in conjunction with Regulation (EU) 2016/679 and its implementing legislation.
Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Nr. I-1374, 2 straipsnio 3 dalis: Kitos šiame įstatyme vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679.	The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, Article 2(3): Other terms used in this Law shall be interpreted as defined in Regulation (EU) 2016/679.
Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Nr. I-1374, 7 straipsnio 1 dalis: Valstybinė duomenų apsaugos inspekcija stebi, kaip taikomas Reglamentas (ES) 2016/679 ir šis įstatymas, ir užtikrina, kad šie teisės aktai būtų taikomi, išskyrus šio įstatymo straipsnius, kurių taikymas pagal šio straipsnio 2 dalį yra žurnalistų etikos inspektoriaus kompetencija.	The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, Article 7(1): The State Data Protection Inspectorate monitors the application of Regulation (EU) 2016/679 and this Law and ensures that these laws are applied, except for the articles of this Law, the application of which is the competence of the Inspector of Journalistic Ethics under Paragraph 2 of this Article.
Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Nr. I-1374, 7 straipsnio 2 dalis: Žurnalistų etikos inspektorius stebi, kaip taikomas Reglamentas (ES) 2016/679 ir šis įstatymas, ir užtikrina, kad šie teisės aktai būtų taikomi, kai asmens duomenys tvarkomi žurnalistikos tikslais ir akademinės, meninės ar literatūrinės saviraiškos tikslais. Žurnalistų etikos inspektorius atlieka Reglamente (ES) 2016/679 nustatytas priežiūros institucijos užduotis ir turi Reglamente (ES) 2016/679	The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, Article 7(2): The Inspector of Journalistic Ethics monitors the application of Regulation (EU) 2016/679 and this law and ensures that this legislation applies when personal data are processed for journalistic purposes and for academic, artistic or literary expression. The Inspector of Journalistic Ethics performs the tasks of the supervisory authority set out in Regulation (EU) 2016/679 and has the powers of the

nustatytus priežiūros institucijos įgaliojimus. Žurnalistų etikos inspektoriui netaikomi Reglamento (ES) 2016/679 57 straipsnio 1 dalies j–l ir n–t punktai, 58 straipsnio 1 dalies b ir c punktai, 2 dalies e, g, h ir j punktai, 3 dalies a, c ir e–j punktai.	supervisory authority set out in Regulation (EU) 2016/679. Article 57(1) paragraphs (j)-(l) and (n)-(t), Article 58 (1) paragraphs (b) and (c), Article 57(1) paragraphs (e), (g), (h) and (j), Article 57(3) paragraphs (a), (c) and (e)-(j).
Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Nr. I-1374, 11 straipsnio 1 dalis: Valstybinė duomenų apsaugos inspekcija atlieka Reglamente (ES) 2016/679 nustatytas priežiūros institucijos užduotis.	The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, Article 11 Part 1: The State Data Protection Inspectorate performs the tasks of the supervisory authority set out in Regulation (EU) 2016/679.
Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Nr. I-1374, 11 straipsnio 2 dalis: Valstybinė duomenų apsaugos inspekcija taip pat atlieka šias funkcijas: 1) teikia duomenų subjektams, duomenų valdytojams ir duomenų tvarkytojams konsultacijas dėl asmens duomenų ir privatumo apsaugos, taip pat rengia metodines rekomendacijas dėl asmens duomenų apsaugos ir jas viešai skelbia savo interneto svetainėje; 2) vadovaudamasi Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108), teikia pagalbą užsienyje gyvenantiems duomenų subjektams; 3) bendradarbiauja su kitų valstybių asmens duomenų apsaugos priežiūros institucijomis, Europos Sąjungos	The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, Article 11 Part 2: The State Data Protection Inspectorate also performs the following functions: 1) provide consultations to data subjects, data controllers and data processor on the protection of personal data and privacy, also prepare methodological recommendations on the protection of personal data and make them publicly available on their website; 2) provide assistance to data subjects residing abroad in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108); 3) cooperate with the supervisory authorities of the protection of personal data of other states, institutions, agencies and

institucijomis, įstaigomis ir tarptautinėmis organizacijomis ir dalyvauja jų veikloje; 4) dalyvauja formuojant valstybės politiką asmens duomenų apsaugos srityje ir ją įgyvendina; 5) įgyvendina 1981 m. sausio 28 d. Strasbūre sudarytos Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) ir jos protokolų nuostatas; 6) kitas šiame įstatyme ir kituose teisės aktuose nustatytas funkcijas.	international organisations of the European Union and participate in their activities; 4) participate in shaping state policy in the field of personal data protection and implement it; 5) implement the provisions of the Convention on the Protection of Persons created in Strasbourg on 28 January 1981 in connection with the Automated Processing of Personal Data (ETS No 108) and its Protocols; 6) other functions specified in this Law and other legal acts.
Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Nr. I-1374, 31 straipsnio 5 dalis: Priežiūros institucijos sprendimas gali būti skundžiamas teismui Administracinių bylų teisenos įstatymo nustatyta tvarka.	The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, Article 31(5): The decision of the supervisory institution may be appealed to the court in accordance with the procedure laid down by the Law on Administrative Proceedings.
Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, Nr. I-1374 (1996 m. birželio 11 d. redakcija), 2 straipsnis 1 dalis: Asmens duomenys – duomenys apie konkretų arba iš duomenų nustatomą fizinį asmenį, jo dalykinius santykius ir išvados apie asmenį, padarytos remiantis šiais duomenimis.	The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374 (11 June 1996 wording), Article 2(1): Personal data - data about a concrete or a natural person identifiable from the data, his business relations and findings about the person on the basis of the data.
Lietuvos Respublikos visuomenės informavimo įstatymas, Nr. I-1418, 50 straipsnio 3 dalies 1 punktas:	The Law on the Provision of Information to the Public of the Republic of Lithuania, No. I-1418, Article 50(3)(1):

Atlikdamas šio straipsnio 1 dalyje nurodytas funkcijas, inspektorius gali priimti sprendimą: 3) įspėti viešosios informacijos rengėjus ir skleidėjus, už visuomenės informavimo priemonių turinį atsakingus (fizinius) asmenis apie pastebėtus šio Įstatymo ir kitų visuomenės informavimą reglamentuojančių teisės aktų pažeidimus ir reikalauti juos pašalinti.	In performing the functions referred to in paragraph 1 of this Article, the Inspector may take a decision: 3) to warn producers and disseminators of public information, persons responsible for the content of the mass media (natural) about the observed violations of this Law and other legal acts regulating public information and to demand their elimination.
Lietuvos Respublikos Vyriausybės nutarimas „Dėl Valstybinės duomenų apsaugos inspekcijos nuostatų patvirtinimo“, Nr. 1156, 3 straipsnis: Inspekcija savo veikloje vadovaujasi Lietuvos Respublikos Konstitucija, Lietuvos Respublikos tarptautinėmis sutartimis ir susitarimais, 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119 p. 1) (toliau – Reglamentas (ES) 2016/679), kitais Europos Sąjungos ir tarptautiniais teisės aktais, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, Lietuvos Respublikos asmens duomenų tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymu, Lietuvos Respublikos elektroninių ryšių įstatymu, Lietuvos Respublikos kibernetinio saugumo įstatymu, kitais įstatymais, Lietuvos Respublikos Seimo priimtais teisės aktais,	The Resolution of the Government of the Republic of Lithuania ‘Regarding the Approval of the Regulations of the State Data Protection Inspectorate’, No. 1156, Article 3: In its activities, the Inspectorate follows the Constitution of the Republic of Lithuania, international treaties and agreements of the Republic of Lithuania. April 27 Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) (hereinafter - Regulation (EU) 2016/679), other European Union and international legal acts, the Law on the Legal Protection of Personal Data of the Republic of Lithuania, the prevention, investigation, disclosure or prosecution of criminal data processed in the Republic of Lithuania, enforcement of penalties or national security or for defence purposes, the Law on Legal Protection, the Law on Electronic Communications of the Republic of Lithuania, the Law on Cyber Security of the Republic of Lithuania, other laws, legal acts adopted by the Seimas of the Republic of

Vyriausybės nutarimais, Valstybinės duomenų apsaugos inspekcijos nuostatais (toliau – Nuostatai), taip pat kitais teisės aktais.	Lithuania, Government resolutions, Regulations of the State Data Protection Inspectorate (hereinafter - Regulations).
Lietuvos Respublikos Vyriausybės nutarimas „Dėl Valstybinės duomenų apsaugos inspekcijos nuostatų patvirtinimo“, Nr. 1156, 16 straipsnis: Inspekcija turi Reglamente (ES) 2016/679 nustatytus priežiūros institucijos įgaliojimus.	The Resolution of the Government of the Republic of Lithuania ‘Regarding the Approval of the Regulations of the State Data Protection Inspectorate’, No. 1156, Article 16 Inspectorate has the supervisory authority powers laid down in Regulation (EU) 2016/679.
Lietuvos Respublikos Kibernetinio saugumo įstatymas, Nr. XII-1428, 1 straipsnio 1 dalis: Šis įstatymas nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, taip pat tarpinstitucinį bendradarbiavimą.	The Law on Cyber Security of the Republic of Lithuania, No. XII-1428, Article 1(1): This Law establishes cyber security principles, specifies institutions which develop and implement cyber security policy, defines powers of such authorities in the field of cyber securities, and determines duties of cyber security entities as well as inter-institutional cooperation.
Lietuvos Respublikos Kibernetinio saugumo įstatymas, Nr. XII-1428, 4 straipsnio 2 dalis: Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija. Nacionalinis kibernetinio saugumo centras formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame įstatyme nustatytoms funkcijoms atlikti reikia nustatyti kibernetinio saugumo subjektų veiklos teisinį reguliavimą.	The Law on Cyber Security of the Republic of Lithuania, No. XII-1428, Article 4(2): Cyber security policy is developed, its implementation is organised, controlled, and coordinated by the Ministry of National Defence of the Republic of Lithuania. The National Cyber Security Centre takes part in the development of the cyber security policy to the extent to which legal regulation of activities of cyber security entities has to be established for the performance of functions laid down in this law.

Lietuvos Respublikos Kibernetinio saugumo įstatymas, Nr. XII-1428, 9 straipsnis: Valstybinė duomenų apsaugos inspekcija įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje ir atlieka 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1) nustatytas priežiūros institucijos užduotis.	The Law on Cyber Security of the Republic of Lithuania, No. XII-1428, Article 9: The State Data Protection Inspectorate implements the cyber security policy in the field of personal data protection and carries out the 2016 April 27 Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) tasks of the supervisory authority.
Lietuvos Respublikos civilinis kodeksas, Nr. VIII-1864, 2.23 straipsnis: 1. Fizinio asmens privatus gyvenimas neliečiamas. Informacija apie asmens privatų gyvenimą gali būti skelbiama tik jo sutikimu. Po asmens mirties tokių sutikimą gali duoti jo sutuoktinis, tėvai ar vaikai. 2. Privataus gyvenimo pažeidimu laikomas neteisėtas įėjimas į asmens gyvenamąsias ir kitokias patalpas, aptvertą privačią teritoriją, neteisėtas asmens stebėjimas, neteisėtas asmens ar jo turto apieškojimas, asmens telefoninių pokalbių, susirašinėjimo ar kitokios korespondencijos bei asmeninių užrašų ir informacijos konfidencialumo pažeidimas, duomenų apie asmens sveikatos būklę paskelbimas pažeidžiant įstatymų nustatytą tvarką bei kitokie neteisėti veiksmai. 3. Draudžiama rinkti informaciją apie privatų asmens gyvenimą pažeidžiant įstatymus. Asmuo turi teisę susipažinti su apie jį surinkta informacija, išskyrus įstatymų nustatytas	The Civil Code of the Republic of Lithuania, No. VIII-1864, Article 2.23: 1. Privacy of natural person shall be inviolable. Information on person's private life may be made public only with his consent. After person's death the said consent may be given by the person's spouse, children and parents. 2. Unlawful invasion of person's dwelling or other private premises as well as fenced private territory, keeping his private life under observation, unlawful search of the person or his property, intentional interception of person's telephone, post or other private communications as well as violation of the confidentiality of his personal notes and information, publication of the data on the state of his health in violation of the procedure prescribed by laws and other unlawful acts shall be deemed to violate person's private life.

išimtis. Draudžiama skleisti surinktą informaciją apie asmens privatų gyvenimą, nebent, atsižvelgiant į asmens einamas pareigas ar padėtį visuomenėje, tokios informacijos skleidimas atitinka teisėtą ir pagrįstą visuomenės interesą tokią informaciją žinoti. 4. Privataus asmens gyvenimo duomenų, nors ir atitinkančių tikrovę, paskelbimas, taip pat asmeninio susirašinėjimo paskelbimas pažeidžiant šio straipsnio 1 ir 3 dalyse nustatytą tvarką, taip pat įėjimas į asmens gyvenamąjį būstą be jo sutikimo, išskyrus įstatymų numatytas išimtis, asmens privataus gyvenimo stebėjimas ar informacijos rinkimas apie jį pažeidžiant įstatymą bei kiti neteisėti veiksmai, kuriais pažeidžiama teisė į privatų gyvenimą, yra pagrindas pareikšti ieškinį dėl tokių veiksmų padarytos turtinės ir neturtinės žalos atlyginimo. 5. Šio straipsnio 1 ir 3 dalyse numatyti apribojimai, susiję su informacijos apie asmenį skelbimu ir rinkimu, netaikomi, kai tai daroma motyvuotu teismo sprendimu.	3. Establishment of a file on another person's private life in violation of law shall be prohibited. A person may not be denied access to the information contained in the file except as otherwise provided by the law. Dissemination of the collected information on the person's private life shall be prohibited unless, taking into consideration person's official post and his status in the society, dissemination of the said information is in line with the lawful and well-grounded public interest to be aware of the said information. 4. Public announcement of facts of private life, however truthful they may be, as well as making private correspondence public in violation of the procedure prescribed in paragraphs 1 and 3 of the given Article as well as invasion of person's dwelling without his consent except as otherwise provided by the law, keeping his private life under observation or gathering of information about him in violation of law as well as other unlawful acts, infringing the right to privacy shall form the basis for bringing an action for repairing the property and non-pecuniary damage incurred by the said acts. 5. Where the said acts are committed on the basis of reasoned judgement of the court, restrictions imposed on the publication and collecting of information about the person which are laid down in the provisions of paragraphs 1 and 3 of the given Article shall not be applied.
Lietuvos Respublikos darbo kodeksas, Nr. XII-2603, 216 straipsnis:	The Labour Code of the Republic of Lithuania, No. XII-2603, Article 216:

1. Darbo ginčus dėl teisės nagrinėja: 1) darbo ginčų komisija; 2) teismas. 2. Darbo ginčai dėl teisės gali būti nagrinėjami komerciniame arbitraže pagal Lietuvos Respublikos komercinio arbitražo įstatymą, jeigu dėl tokio nagrinėjimo sutaria darbo ginčo šalys vėliau, negu kilo ginčas.	1. Labour disputes concerning the law shall be examined by: 1) the Labour Disputes Commission; 2) the court. 2. Labour disputes regarding the right may be examined in commercial arbitration in accordance with the Law on Commercial Arbitration of the Republic of Lithuania, if the parties to the labour dispute agree on such examination later than the dispute arose.
Lietuvos Respublikos lygių galimybių įstatymas, Nr. IX-1826, 13 straipsnis: Asmuo, patyręs diskriminaciją lyties, rasės, tautybės, pilietybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų, amžiaus, lytinės orientacijos, negalios, etninės priklausomybės, religijos pagrindu, turi teisę reikalauti iš kaltų asmenų atlyginti turtinę ir neturtinę žalą įstatymų nustatyta tvarka.	The Law on Equal Treatment of the Republic of Lithuania, No. IX-1826, Article 13: A person who has suffered discrimination on the grounds of sex, race, nationality, citizenship, language, origin, social status, religion, belief or opinion, age, sexual orientation, disability, ethnicity, religion has the right to claim pecuniary and non-pecuniary damages from the guilty persons in accordance with the procedure laid down in the legislation.
Lietuvos Respublikos lygių galimybių įstatymas, Nr. IX-1826, 24 straipsnio 1 dalis: Kiekvienas fizinis, juridinis asmuo, kita organizacija ir jos padalinys turi teisę pateikti lygių galimybių kontrolieriui skundą dėl lygių galimybių pažeidimo.	The Law on Equal Treatment of the Republic of Lithuania, No. IX-1826, Article 24(1): Every natural or legal person, other organization and its division has the right to submit a complaint to the Equal Opportunities Ombudsman regarding a violation of equal opportunities.
Lietuvos Respublikos moterų ir vyrų lygių galimybių įstatymas, Nr. VIII-947, 18 straipsnis: Asmuo, patyręs diskriminaciją, seksualinį priekabiavimą ar priekabiavimą lyties	The Law on Equal opportunities for women and men of the Republic of Lithuania, No. VIII-947, Article 18: A person who has suffered discrimination, sexual harassment or harassment on the

pagrindu, turi teisę reikalauti iš kaltų asmenų atlyginti turtinę ir neturtinę žalą įstatymų nustatyta tvarka.	grounds of sex has the right to demand compensation for pecuniary and non-pecuniary damage from guilty persons in accordance with the procedure established by law.
Lietuvos Respublikos baudžiamojo proceso kodeksas, Nr. IX-785, 154 straipsnis: 1. Kai pagal prokuroro prašymą yra priimta ikiteisminio tyrimo teisėjo nutartis, ikiteisminio tyrimo pareigūnas gali klausytis asmenų pokalbių, perduodamų elektroninių ryšių tinklais, daryti jų įrašus, kontroliuoti kitą elektroninių ryšių tinklais perduodamą informaciją ir ją fiksuoti bei kaupti, jeigu yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie rengiamą, daromą ar padarytą labai sunkų, sunkų ar apysunkį nusikaltimą arba apie nesunkius nusikaltimus, numatytus Lietuvos Respublikos baudžiamojo kodekso 152¹ straipsnyje, 162 straipsnio 2 dalyje, 170 straipsnyje, 198² straipsnio 1 dalyje, 309 straipsnio 2 dalyje, arba jeigu yra pavojus, kad nukentėjusiajam, liudytojui ar kitiems proceso dalyviams arba jų artimiesiems bus panaudotas smurtas, prievartavimas ar kitokios neteisėtos veikos. 2. Ikiteisminio tyrimo teisėjo nutartyje ar prokuroro nutarime klausytis asmenų pokalbių, perduodamų elektroninių ryšių tinklais, daryti jų įrašus, kontroliuoti kitą elektroninių ryšių tinklais perduodamą informaciją ir ją fiksuoti bei kaupti turi būti nurodyta: 1) turimi duomenys apie asmenį, prieš kurį veiksmai turi būti atlikti;	The Code of Criminal Procedure of the Republic of Lithuania, No. IX-785, Article 154: 1. When a pre-trial investigation judge's ruling has been issued at the request of the prosecutor, the pre-trial investigation officer may listen to, record and store other information transmitted by electronic communications networks if there is reason to believe that it is possible to receive data on a grave serious, serious, less serious or minor offences being prepared, committed provided for in Article 152¹, Article 162 (2), Article 170, Article 198²(1), Article 309(2) of the Criminal Code of the Republic of Lithuania, or if there is a danger that the victim, witness or other participants in the proceedings or their relatives will be subjected to violence, coercion or other illegal acts. 2. The order of a pre-trial investigation judge or the decision of a prosecutor to listen to the conversations of persons transmitted via electronic communications networks, to make their recordings, to control other information transmitted via electronic communications networks and to record and store it shall specify: 1) available data on the person against whom the action is to be taken

2) duomenys, kuriais pagrindžiama būtinybė atlikti šio straipsnio 1 dalyje numatytus veiksmus; 3) konkretūs šio straipsnio 1 dalyje numatyti veiksmai, kuriuos leidžiama atlikti; 4) veiksmų trukmė. 3. Šio straipsnio 1 dalyje nustatyta tvarka gali būti kontroliuojama ir fiksuojama elektroninių ryšių tinklais perduodama informacija, išskyrus jos turinį, jeigu yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie nesunkius nusikaltimus, numatytus Lietuvos Respublikos baudžiamojo kodekso 166, 198¹ straipsniuose, 309 straipsnio 1 dalyje. 4. Asmenų pokalbių, perduodamų elektroninių ryšių tinklais, klausymas, įrašų darymas ar kitos elektroninių ryšių tinklais perduodamos informacijos kontrolė, jos fiksavimas ir kaupimas negali trukti ilgiau kaip šešis mėnesius. Tiriant sudėtingą ar didelio masto nusikalstamą veiką, šios priemonės taikymas gali būti vieną kartą pratęstas trimis mėnesiams. 5. Ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, privalo sudaryti sąlygas klausytis asmenų pokalbių, perduodamų elektroninių ryšių tinklais, daryti jų įrašus ar kontroliuoti kitą elektroninių ryšių tinklais perduodamą informaciją, ją fiksuoti ir kaupti. Ūkio subjekto, teikiančio elektroninių ryšių tinklus ir (ar) paslaugas, darbuotojai, nevykdantys šios pareigos ar trukdantys atlikti šiame straipsnyje nurodytus veiksmus, gali	2) data justifying the need to carry out the actions provided for in Paragraph 1 of this Article; 3) the specific actions provided for in paragraph 1 that are permitted; 4) duration of the actions. 3. In accordance with the procedure established in Paragraph 1 of this Article, information transmitted via electronic communications networks, except for its content, may be controlled and recorded if there is reason to believe that data on minor crimes provided for in Articles 166, 198¹, Article 309(1) of the Criminal Code can be gathered. 4. The interception, recording of conversations, or other information transmitted by persons over electronic communications networks shall not exceed six months. In the case of a complex or large-scale criminal offense, this measure may be extended once for a period of three months. 5. Undertakings providing electronic communications networks and/or services must create conditions for listening to conversations of persons transmitted via electronic communications networks, making their recordings, or controlling other information transmitted via electronic communications networks, and recording and storing it. Employees of an undertaking providing electronic communications networks and/or services who fail to perform this obligation or obstruct the performance of the acts referred to in this Article may be

būti remiantis šio Kodekso 163 straipsniu nubausti bauda. 6. Nukentėjusiųjų, liudytojų ar kitų proceso dalyvių pokalbių, perduodamų elektroninių ryšių tinklais, galima klausytis, daryti jų įrašus, kontroliuoti kitą šių asmenų elektroninių ryšių tinklais perduodamą informaciją, ją fiksuoti ir kaupti šių asmenų prašymu arba jų sutikimu, nors ir nėra tuo reikalu priimtos ikiteisminio tyrimo teisėjo nutarties, jei nesinaudojama ūkio subjektų, teikiančių elektroninių ryšių tinklus ir (ar) paslaugas, paslaugomis ir įrenginiais. 7. Draudžiama klausytis gynėjo pokalbių su įtariamuoju ar kaltinamuoju, perduodamų elektroninių ryšių tinklais, daryti jų įrašus, kontroliuoti kitą elektroninių ryšių tinklais tarp jų perduodamą informaciją, ją fiksuoti ir kaupti. 8. Dėl pokalbių, perduodamų elektroninių ryšių tinklais, ar kitos elektroninių ryšių tinklais perduodamos informacijos turinio kontrolės fakto ikiteisminio tyrimo pareigūno surašytame protokole išdėstomas tik tyrimui reikšmingas duomenų bei garso įrašo turinys. Tyrimui reikšmės neturintys duomenys ir garso įrašai, kurie nėra bendroje laikmenoje su reikšmingais bylai duomenimis ir įrašais, prie bylos nepridedami ir tuoj pat prokuroro nutarimu sunaikinami surašius atitinkamą aktą.	subject to a fine in accordance with Article 163 of this Code. 6. Conversations of victims, witnesses or other participants in electronic communications networks may be listened to, recorded, controlled, and stored at the request or with the consent of such persons, although no pre-trial investigation has been conducted a ruling of a judge if the services and equipment of undertakings providing electronic communications networks and/or services are not used. 7. It is prohibited to listen to the counsel's conversations with the suspect or accused transmitted via electronic communications networks, to make recordings thereof, to control other information transmitted between them via electronic communications networks, and to store it. 8. The protocol drawn up by the pre-trial investigation officer regarding the fact of the control of the content of conversations transmitted via electronic communications networks or other information transmitted via electronic communications networks shall set out only the content of data and audio recording relevant to the investigation. Data and audio recordings that are not relevant to the investigation, which are not in a common medium with data and recordings relevant to the case, shall not be attached to the case and shall be destroyed immediately by a decision of the prosecutor upon drawing up the relevant act.

Lietuvos Respublikos baudžiamasis kodeksas, Nr. VIII-1968, 166 straipsnio 1 dalis: Tas, kas neteisėtai perėmė paštą ar per pasiuntinių paslaugos teikėją siunčiamą siuntą ar siuntinį arba neteisėtai perėmė, fiksavo ar stebėjo asmens elektroninių ryšių tinklais siunčiamus pranešimus, arba neteisėtai fiksavo, klausėsi ar stebėjo asmens pokalbius elektroninių ryšių tinklais, arba kitaip pažeidė asmens susižinojimo neliečiamumą, baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų.	The Criminal Code of the Republic of Lithuania, No. VIII-1968, Article 166(1): A person who illegally intercepts a parcel or parcel sent by post or a courier service provider or illegally intercepts, records or monitors messages sent by a person via electronic communication networks, or illegally records, listens to or monitors a person's conversations via electronic communication networks, or otherwise violates a person's inviolability of personal communication is punished by public works or a fine, or restriction of liberty, or arrest, or imprisonment for up to two years.
Lietuvos Respublikos kriminalinės žvalgybos įstatymas, Nr. XI-2234, 5 straipsnio 7 dalis: Kriminalinės žvalgybos metu ar pabaigus kriminalinės žvalgybos tyrimą nustatius, kad gauta kriminalinės žvalgybos informacija apie kriminalinės žvalgybos objektą nepasitvirtino arba kad kriminalinės žvalgybos uždaviniai nebus įgyvendinti, informacijos apie kriminalinės žvalgybos objektą rinkimas turi būti nedelsiant sustabdomas, o surinkta informacija sunaikinama. Jeigu pabaigus kriminalinės žvalgybos tyrimą kriminalinės žvalgybos informacija apie kriminalinės žvalgybos objektą nebuvo panaudota šio įstatymo 19 straipsnyje nustatyta tvarka, kriminalinės žvalgybos tyrimo metu surinkta informacija apie privatų asmens gyvenimą per 3 mėnesius turi būti sunaikinama. Prieš 1 mėnesį iki minėtos sankcionuotais kriminalinės žvalgybos informacijos rinkimo būdais surinktos informacijos sunaikinimo apie tai pranešama kriminalinės žvalgybos informacijos rinkimo būdus sankcionavusiam	The Law on Criminal Intelligence of the Republic of Lithuania, No. XI-2234, Article 5(7): If, during or after the conclusion of a criminal intelligence investigation, it is established that the received criminal intelligence information about the criminal intelligence object has not been confirmed or that the criminal intelligence objectives will not be fulfilled, the collection of criminal intelligence information shall be suspended immediately. If after the completion of the criminal intelligence investigation the criminal intelligence information about the object of criminal intelligence has not been used in accordance with Article 19 of this Law, the information about the private life of the person collected during the criminal intelligence investigation shall be destroyed within 3 months. 1 month prior to the destruction of the said information collected by authorized criminal intelligence gathering methods, the official who authorized the criminal intelligence

pareigūnui ir prokurorui, rengusiam motyvuotą teikimą dėl kriminalinės žvalgybos informacijos rinkimo būdų sankcionavimo. Kita nepanaudota informacija, esanti nutrauktose kriminalinio tyrimo bylose ar (ir) informacinėse sistemose, saugoma teisės aktų, kurie reglamentuoja kriminalinės žvalgybos tyrimo bylų ir duomenų, esančių informacinėse sistemose, saugojimą, naudojimą ir naikinimą, nustatyta tvarka. Surinktos informacijos naikinimo tvarką nustato kriminalinės žvalgybos pagrindinė institucija.	information gathering methods and the prosecutor who prepared a reasoned submission regarding the authorization of criminal intelligence gathering methods shall be notified thereof. Other unused information contained in discontinued criminal investigation files and/or information systems shall be protected in accordance with the procedure established by legal acts regulating the storage, use and destruction of criminal intelligence files and data contained in information systems. The procedure for the destruction of the collected information shall be established by the Central Criminal Intelligence Authority.
Lietuvos Respublikos kriminalinės žvalgybos įstatymas, Nr. XI-2234, 8 straipsnio 1 dalis: Kriminalinės žvalgybos tyrimas atliekamas, kai: 1) turima informacijos apie rengiamą, daromą ar padarytą labai sunkų ar sunkų nusikaltimą arba apie apysunkius nusikaltimus, numatytus Lietuvos Respublikos baudžiamojo kodekso 131 straipsnyje, 145 straipsnio 2 dalyje, 146 straipsnio 2 ir 3 dalyse, 151¹, 153, 172, 173, 174, 175 ir 175¹ straipsniuose, 178 straipsnio 2 dalyje, 180 straipsnio 1 dalyje, 181 straipsnio 1 dalyje, 182¹ straipsnyje, 187 straipsnio 2 dalyje, 189 straipsnio 1 ir 2 dalyse, 189¹ straipsnyje, 198 straipsnio 2 dalyje, 199 straipsnio 1 dalyje, 199¹ straipsnio 1 dalyje, 199² straipsnio 1 dalyje, 200 straipsnio 1 dalyje, 213 straipsnio 1 dalyje, 214 ir 215 straipsniuose, 225 straipsnio 1 dalyje, 226 straipsnio 1 ir 2 dalyse, 227 straipsnio 1 ir 2 dalyse, 228 straipsnio 1 dalyje, 228¹, 240, 250¹, 250³ ir 250⁶ ir 250⁶	The Law on Criminal Intelligence of the Republic of Lithuania, No. XI-2234, Article 8(1): A criminal intelligence investigation shall be conducted when: 1) available information on a grave serious, serious or less serious crimes being prepared, committed provided for in Article 131, Article 145(2), Article 146(2)-(3), 151¹, 153, 172, 173, 174, 175 of the Criminal Code of the Republic of Lithuania and Articles 175¹, 178(2), 180(1), 181(1), 182¹, 187(2), 189(1)-(2), 189¹, 198(2), 199(1), 199¹(1) , Article 1(1), Article 200(1), Article 213(1), Articles 214 and 215, Article 225(1), Article 226(1)-(2), Article 227(1)-(2), Article 228(1), Article 228¹, 240, 250¹ Articles 250³ and 250⁶, Article 251(1), Article 253(1), Article 256(1), Article 266(2), Article 300(2) -(3), Article 301(2), Article 302(2), Article 307(1)-(2), Article 309(3), or of

straipsniuose, 251 straipsnio 1 dalyje, 253 straipsnio 1 dalyje, 256 straipsnio 1 dalyje, 266 straipsnio 2 dalyje, 300 straipsnio 2 ir 3 dalyse, 301 straipsnio 2 dalyje, 302 straipsnio 2 dalyje, 307 straipsnio 1 ir 2 dalyse, 309 straipsnio 3 dalyje, arba apie šias veikas rengiančius, darančius ar padariusius asmenis; 2) pasislepia įtariamasis, kaltinamasis arba nuteistasis; 3) dingsta be žinios asmuo; 4) vykdoma asmenų apsauga nuo nusikalstamo poveikio; 5) į organizuotų nusikalstamų grupių sąrašą įtrauktos organizuotos nusikalstamos grupės nariui ar su ja susijusiam asmeniui taikomos organizuoto nusikalstamumo prevencijos priemonės.	persons who prepare, commit or have committed such acts; 2) the suspect, accused or convicted person is in hiding; 3) the person disappears without knowledge 4) the protection of persons against criminal effects is being conducted; 5) the organised crime prevention measures are applied against a member of an organised crime group or a person associated with it.
Lietuvos Respublikos kriminalinės žvalgybos įstatymas, Nr. XI-2234, 10 straipsnio 1 dalis: Techninių priemonių panaudojimą specialia tvarka, slapta pašto siuntų ir jų dokumentų apžiūrą, pašto siuntų kontrolę ir paėmimą, susirašinėjimo ir kitokio susižinojimo slapta kontrolę motyvuota nutartimi sankcionuoja apygardų teismų pirmininkai ar jų įgalioti teisėjai pagal prokurorų motyvuotus teikimus, parengtus pagal kriminalinės žvalgybos subjektų vadovų ar jų įgaliotų vadovų pavaduotojų pateiktus duomenis, kuriais patvirtinamas tokių veiksmų atlikimo būtinumas ir faktinis pagrindas. Elektroninių ryšių tinklais perduodamos asmenų informacijos turinio kontrolė ir jos fiksavimas, net ir žinant apie tokią kontrolę vienam iš jų, reikalauja motyvuotos teismo	The Law on Criminal Intelligence of the Republic of Lithuania, No. XI-2234, Article 10(1): The use of technical means in a special manner, covert inspection of postal items and their documents, control and seizure of postal items, covert control of correspondence and other communications shall be authorized by a reasoned order of district court presidents or their authorized judges on motivated submissions data provided by the Heads of the criminal intelligence subjects confirming the necessity and factual basis for such actions. The control and recording of the content of personal information transmitted over electronic communications networks, even with the knowledge of such control by one of them, shall require a reasoned court

nutarties, išskyrus atvejus, kai asmuo paprašo arba sutinka su tokia kontrole ar fiksavimu nesinaudojant ūkio subjektų, teikiančių elektroninių ryšių tinklus ir (ar) paslaugas, paslaugomis ir įrenginiais.	order, unless the person requests or agrees to such control or recording without the use of electronic communications networks and/or services, services, and facilities.
Lietuvos Respublikos kriminalinės žvalgybos įstatymas, Nr. XI-2234, 10 straipsnio 2 dalis: Neatidėliotinais atvejais, kai iškyla pavojus žmogaus gyvybei, sveikatai, nuosavybei, visuomenės ar valstybės saugumui, leidžiama atlikti šio straipsnio 1 dalyje nurodytus veiksmus vadovaujantis prokuroro nutarimu. Tokiu atveju prokuroras, priėmęs šį nutarimą, per 24 valandas šio straipsnio 1 dalyje nurodytam teisėjui pateikia teikimą dėl veiksmų teisėtumo ar pagrįstumo patvirtinimo motyvuota nutartimi. Jeigu terminas baigiasi poilsio ar švenčių dieną, teikimas pateikiamas kitą darbo dieną po poilsio ar švenčių dienos. Jeigu teisėjas nepatvirtina minėtų veiksmų teisėtumo ar pagrįstumo motyvuota nutartimi, veiksmai nutraukiami, o jų metu gauta informacija nedelsiant sunaikinama.	The Law on Criminal Intelligence of the Republic of Lithuania, No. XI-2234, Article 10(2): In urgent cases where human life, health, property, public or state security is endangered, the actions referred to in Paragraph 1 of this Article shall be permitted in accordance with the decision of the prosecutor. In such a case, the prosecutor shall make a submission to the judge referred to in Paragraph 1 of this Article within 24 hours after the adoption of this ruling, confirming the legality or justification of the actions by a reasoned order. If the period expires on a non-working day, the submission shall be submitted on the next working day after the non-working day. If the judge does not confirm the legality or justification of the said actions by a reasoned order, the actions shall be terminated and the information obtained during them shall be immediately destroyed.
Lietuvos Respublikos kriminalinės žvalgybos įstatymas, Nr. XI-2234, 10 straipsnio 5 dalis: Techninių priemonių panaudojimas specialia tvarka, slapta pašto siuntų ir jų dokumentų apžiūra, pašto siuntų kontrolė ir paėmimas, susirašinėjimo ir kitokio susižinojimo slapta kontrolė sankcionuojami ne ilgesniam kaip 3 mėnesių laikotarpiui. Šis laikotarpis gali būti pratęstas. Bendras laikotarpis negali būti	The Law on Criminal Intelligence of the Republic of Lithuania, No. XI-2234, Article 10(5): The use of technical means in accordance with special procedures, covert inspection of postal items and their documents, control and seizure of postal items, covert control of correspondence and other communications shall be authorized for a period not exceeding

ilgesnis negu 12 mėnesių, išskyrus atvejus, kai kriminalinės žvalgybos tyrimas atliekamas dėl turimos informacijos apie rengiamą, daromą ar padarytą labai sunkų ar sunkų nusikaltimą arba kai yra kriminalinės žvalgybos tyrimo pagrindų, numatytų šio įstatymo 8 straipsnio 1 dalies 2, 3 ir 4 punktuose. Šiais atvejais techninių priemonių panaudojimą specialia tvarka, slapta pašto siuntų ir jų dokumentų apžiūrą, pašto siuntų kontrolę ir paėmimą, susirašinėjimo ir kitokio susižinojimo slapta kontrolę ilgesniam negu 12 mėnesių laikotarpiui generalinio prokuroro ar jo įgalioto Generalinės prokuratūros prokuroro teikimu sankcionuoja apygardos teismo pirmininkas.	3 months. This period may be extended. The total period may not exceed 12 months, except in cases where the criminal intelligence investigation is carried out on the basis of available information on a grave serious or serious crime being prepared, committed, or was committed or there are grounds for criminal investigation provided for in Article 8(1) (2), (3) (4) paragraphs. In these cases, the use of technical means by special procedure, covert inspection of postal items and their documents, control and seizure of postal items, covert control of correspondence and other communications for a period longer than 12 months shall be authorized by the Chief Prosecutor or the prosecutor authorized by him.
Lietuvos Respublikos kriminalinės žvalgybos įstatymas, Nr. XI-2234, 10 straipsnio 6 dalis: Šio straipsnio 5 dalyje numatytas veiksmų pratęsimas sankcionuojamas ta pačia tvarka kaip ir šių veiksmų skyrimas. Pratęsimų skaičius neribojamas, tačiau kiekvienu atveju pratęsti galima ne ilgesniam negu šio straipsnio 5 dalyje nustatytam laikotarpiui.	The Law on Criminal Intelligence of the Republic of Lithuania, No. XI-2234, Article 10(6): The extension of actions provided for in Paragraph 5 shall be authorized in accordance with the same procedure as for the appointment of those actions. The number of extensions shall not be limited but may in any case be extended for a period not exceeding that provided for in Paragraph 5.

Bibliography

English titles

Legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

European Commission Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Constitution of the Republic of Lithuania

The Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374

Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374 (11 June 1996 wording)

The Law on Electronic Communications of the Republic of Lithuania, IX-2135

The Law on Legislative Framework of the Republic of Lithuania, XI-2220

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

The Treaty on the Functioning of the European Union

The Law on Cyber Security of the Republic of Lithuania, XIII-1299

The Labour Code of the Republic of Lithuania, No. XII-2603

Civil Code of the Republic of Lithuania, No. VIII-1864

The Law on Public Information of the Republic of Lithuania, No. I-1418

Criminal Code of the Republic of Lithuania, VIII-1968

The Law on Criminal Intelligence of the Republic of Lithuania, No. XI-2234

Universal Declaration of Human Rights

International Covenant on Civil and Political Rights

Convention for the Protection of Human Rights and Fundamental Freedoms

Charter of Fundamental rights of the European Union

The Law on the Legal Protection of Personal Data Processed for the Prevention, Investigation, Disclosure and Prosecution of Criminal Offenses, Execution of Sentences and National Security or Defence

Code of Administrative Offenses of the Republic of Lithuania, No. VIII-1968

Convention for the Protection of Individuals regarding Automatic Processing of Personal Data

The Law on Equal Opportunities of the Republic of Lithuania, No. IX-1826

The Law on Equal Opportunities for Women and Men of the Republic of Lithuania, No. VIII-947

Code of Criminal Procedure of the Republic of Lithuania, No. IX-785

The Resolution of the Government of the Republic of Lithuania ‘Regarding the Approval of the Regulations of the State Data Protection Inspectorate’, No. 1156

Reports

Country report Non-discrimination ‘Transposition and implementation at national level of Council Directives 2000/43 and 2000/78 Lithuania 2020

Country report Non-discrimination ‘Transposition and implementation at national level of Council Directives 2000/43 and 2000/78 Lithuania 2019

Country report Non-discrimination ‘Transposition and implementation at national level of Council Directives 2000/43 and 2000/78 Lithuania 2018

Country report Non-discrimination Transposition and implementation at national level of Council Directives 2000/43 and 2000/78 Lithuania 2017

Country report Non-discrimination Transposition and implementation at national level of Council Directives 2000/43 and 2000/78 Lithuania 2016

Books

Ehlers D., Becker U. European Fundamental Rights and Freedoms. Berlin, 2007

Digital resources

State Data Protection Inspectorate, Recommendation on records of data processing activities

<<https://vdai.lrv.lt/lt/informacija-visuomenei/metodine-informacija/valstybines-duomen-u-apsaugos-inspekcijos-metodine-informacija>>

Recommendation on the procedure for detecting, investigating, reporting and documenting breaches of personal data protection

<https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_ADSP_2018.pdf?fbclid=IwAR3Rh6u9E8zMPd0reheUB3C3zs8UI1ifdkEF4SchkjZBPoj2gI4mlJptbfc>

Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework

<https://www.ohchr.org/documents/publications/guidingprinciplesbusinessshr_en.pdf>

The seventh phase of the peer review 'European Cybercrime practical policies for preventing and combating such crimes implementation and operation'. Evaluation report - Report on Lithuania

<<https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf>>

Comparative Constitutions Project

<https://www.constituteproject.org/search?lang=en&key=privacy&status=in_force>

Lydia F de la Torre, The right to restrict processing under EU data protection law

<<https://medium.com/golden-data/what-is-the-right-to-restrict-processing-under-eu-data-b6627db1319f>>

Right to erasure and right to restriction of processing

<<https://www.twobirds.com/~media/pdfs/gdpr-pdfs/34--guide-to-the-gdpr--right-to-erasure-and-right-to-restriction-of-processing.pdf?la=en>>

Can I ask companies or organisations to stop processing my personal data?

<https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-organisation-stop-processing-my-personal-data_lt>

Summaries of inspection results of SDPI

<<https://vdai.lrv.lt/lt/patikrinimu-rezultatu-apibendrinimai/vdai-patikrinimu-rezultatu-apibendrinimai>>

Hackers target CityBee, sensitive data of 110,000 users leaked

<<https://www.lrt.lt/en/news-in-english/19/1345986/hackers-target-citybee-sensitive-data-of-110-000-users-leaked>>

The company's liability will not escape – a significant fine imposed in Lithuania for violations of the General Data Protection Regulation

<<https://vdai.lrv.lt/lt/naujienos/imones-atsakomybes-neisvengs-lietuvoje-skirta-zenkli-bauda-uz-bendrojo-duomenu-apsaugos-reglamento-pazeidimus>>

A fine has been imposed under the General Data Protection Regulation for improperly processing the personal data of the adopted child's parents

<https://vdai.lrv.lt/lt/news/view_item/id.143>

Alex Moltzau 莫战 Lithuanian Artificial Intelligence Strategy 2019

<<https://alexmoltzau.medium.com/lithuanian-artificial-intelligence-strategy-2019-919ded83cc86>>

The Ministry of Economy and Innovation establishes the Innovation Council

<<https://eimin.lrv.lt/lt/naujienos/ekonomikos-ir-inovaciju-ministerija-steigia-inovaciju-taryba>>

Lithuanian Artificial Intelligence Strategy

<[https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT\(1\).pdf](https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf)>

Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)

<https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>

Case-law

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, (62540/00)

Judgment of the Court of Appeal of the Republic of Lithuania on 8 December 2020, civil case no. 2A-823-370

Ruling of the Supreme Court of the Republic of Lithuania on 1 June 2015, criminal case No. 2K-P-94-895/2015

Resolution of the Constitutional Court of the Republic of Lithuania on the compliance of Article 41(2) of the Code of Correctional Works of the Republic of Lithuania (wording of 2 July 1997) with the Constitution of the Republic of Lithuania, court ruling No. 3/01, 24 March 2003

Judgment of the Court, requesting for a preliminary ruling under Article 267 TFEU from the Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Higher Administrative Court for the Land of North Rhine-Westphalia, Germany), made by decision of 26 February 2018, received at the Court on 19 March 2018, in the proceedings, case No. C-193/18, 13 June 2019

Judgment of the Court, requesting for a preliminary ruling under Article 267 TFEU from the cour d'appel de Bruxelles (Court of Appeal, Brussels, Belgium), made by decision of 7 February 2018, received at the Court on 23 February 2018, in the proceedings, case No. C-142/18, 5 June 2019

Lithuanian titles

Legislation

Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 2016 m. balandžio 27 d. dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)

Europos Parlamento ir Tarybos direktyva (ES) 2016/680 2016 m. balandžio 27 d. dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR

Europos Parlamento ir Tarybos direktyva 2002/58/EB 2002 m. liepos 12 d. dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių)

Pasiūlymas Europos Parlamento ir Tarybos reglamentas dėl teisės į privatą gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių)

Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu

Lietuvos Respublikos Konstitucija

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Nr. I-1374

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Nr. I-1374 (1996 m. birželio 11 d. redakcija)

Lietuvos Respublikos elektroninių ryšių įstatymas, Nr. IX-2135

Lietuvos Respublikos kibernetinio saugumo įstatymas, Nr. XII-1299

Lietuvos Respublikos civilinis kodeksas, Nr. VIII-1864

Lietuvos Respublikos visuomenės informavimo įstatymas, Nr. I-1418

Lietuvos Respublikos baudžiamasis kodeksas, Nr. VIII-1968

Lietuvos Respublikos kriminalinės žvalgybos įstatymas, Nr. XI-2234

Lietuvos Respublikos darbo kodeksas, Nr. XII-2603

Visuotinė žmogaus teisių deklaracijos rezoliucija Nr. 217A

Europos Sąjungos Pagrindinių teisių chartija

Lietuvos Respublikos administracinių nusižengimų kodeksas, Nr. XII-1869

Lietuvos Respublikos lygių galimybių įstatymas, Nr. IX-1826

Lietuvos Respublikos moterų ir vyrų lygių galimybių įstatymas, Nr. VIII-947

Lietuvos Respublikos baudžiamojo proceso kodeksas, Nr. IX-785

Lietuvos Respublikos Vyriausybės nutarimas „Dėl Valstybinės duomenų apsaugos inspekcijos nuostatų patvirtinimo“, Nr. 1156

Lietuvos Respublikos asmens duomenų, tvarkomų vykdančios policijos ir teisminių bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas, Nr. XI-1336

Lietuvos Respublikos Vyriausybės nutarimas dėl valstybinės duomenų apsaugos inspekcijos nuostatų patvirtinimo, Nr. 1156

Reports

Šalies ataskaita Nediskriminavimas Tarybos direktyvų 2000/43 ir 2000/78 perkėlimas ir įgyvendinimas nacionaliniu lygiu Lietuva 2020

Šalies ataskaita Nediskriminavimas Tarybos direktyvų 2000/43 ir 2000/78 perkėlimas ir įgyvendinimas nacionaliniu lygiu Lietuva 2019

Šalies ataskaita Nediskriminavimas Tarybos direktyvų 2000/43 ir 2000/78 perkėlimas ir įgyvendinimas nacionaliniu lygiu Lietuva 2018

Šalies ataskaita Nediskriminavimas Tarybos direktyvų 2000/43 ir 2000/78 perkėlimas ir įgyvendinimas nacionaliniu lygiu Lietuva 2017

Šalies ataskaita Nediskriminavimas Tarybos direktyvų 2000/43 ir 2000/78 perkėlimas ir įgyvendinimas nacionaliniu lygiu Lietuva 2016

Digital resources

Valstybinė duomenų apsaugos inspekcija, Rekomendacija dėl duomenų tvarkymo veiklos įrašų

<<https://vdai.lrv.lt/lt/informacija-visuomenei/metodine-informacija/valstybines-duomen-u-apsaugos-inspekcijos-metodine-informacija>>

Rekomendacija dėl asmens duomenų apsaugos pažeidimų nustatymo, tyrimo, pranešimo apie juos ir jų dokumentavimo tvarkos

<https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_ADSP_2018.pdf?fbclid=IwAR3Rh6u9E8zMPd0reheUB3C3zs8UI1ifdkEF4SchkjZBPoj2gI4mlJptbfc>

Verslo ir žmogaus teisių pagrindiniai principai: įgyvendinti Jungtinių Tautų sistemą „Apsaugoti, gerbti ir ištaisyti“

<https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf>

Septintasis tarpusavio vertinimo etapas „Europos kibernetinių nusikaltimų praktinė politika siekiant užkirsti kelią tokiems nusikaltimams ir kovoti su jais“. Vertinimo ataskaita - ataskaita apie Lietuvą

<<https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf>>

Lyginamasis Konstitucijų projektas

<https://www.constituteproject.org/search?lang=en&key=privacy&status=in_force>

Lydia F de la Torre, Teisė apriboti duomenų tvarkymą pagal ES duomenų apsaugos teisės aktus

<<https://medium.com/golden-data/what-is-the-right-to-restrict-processing-under-eu-data-b6627db1319f>>

Teisė ištrinti duomenis ir teisė apriboti duomenų tvarkymą

<<https://www.twobirds.com/~media/pdfs/gdpr-pdfs/34--guide-to-the-gdpr--right-to-erasure-and-right-to-restriction-of-processing.pdf?la=en>>

Ar galiu paprašyti, kad įmonė ar organizacija nutrauktų mano asmens tvarkymą

<https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-organisation-stop-processing-my-personal-data_lt>

VDAI patikrinimų rezultatų apibendrinimai

<<https://vdai.lrv.lt/lt/patikrinimu-rezultatu-apibendrinimai/vdai-patikrinimu-rezultatu-apibendrinimai>>

Įsilaužėliai taiko „CityBee“, nutekėjo neskelbtini 110 000 vartotojų duomenys

<<https://www.lrt.lt/en/news-in-english/19/1345986/hackers-target-citybee-sensitive-data-of-110-000-naudotojai-nutekejo>>

Įmonės neišvengs atsakomybės – Lietuvoje paskirta reikšminga bauda už Bendrosios duomenų apsaugos pažeidimus

<<https://vdai.lrv.lt/lt/naujienos/imonės-atsakomybės-neišvengs-lietuvoje-skirta-zenkli-bauda-uz-bendrojo-duomenų-apsaugos-reglamento-pazeidimus>>

Pagal Bendrąjį duomenų apsaugos reglamentą bauda paskirta už netinkamai tvarkomus įvaikinto asmens duomenis, <https://vdai.lrv.lt/lt/news/view_item/id.143>

莫 战 Alexas Moltzau, Lietuvos dirbtinio intelekto strategija,

<<https://alexmoltzau.medium.com/lithuanian-artificial-intelligence-strategy-2019-919ded83cc86>>

Ūkio ir inovacijų ministerija steigia Inovacijų tarybą

<<https://eimin.lrv.lt/lt/naujienos/ekonomikos-ir-inovaciju-ministerija-steigia-inovaciju-taryba>>

Lietuvos dirbtinio Intelektto strategija

<[https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT\(1\).pdf](https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf)>

Duomenų apsaugos pareigūnų (DAP) gairės (wp243rev.01)

<https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>

Case-law

Europos žmogaus teisių teismo Europos integracijos ir žmogaus teisių asociacijos penktojo skyriaus byla ir sprendimas Ekimdzhiev prieš Bulgariją (paraiška Nr. 62540/00) 2007 m. Birželio 28 d.

Lietuvos apeliacinio teismo sprendimas Lietuvos Respublikos vardu 2020 m. Gruodžio 8 d., civilinė byla Nr. 2A-823-370 / 2020

Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų 2015 m. Birželio 1 d. Kasacinė nutartis baudžiamojoje byloje Nr. 2K-P-94-895/2015.

Lietuvos Respublikos Konstitucinio Teismo nutarimas dėl Lietuvos Respublikos pataisos darbų kodekso 41 straipsnio (1997 m. Liepos 2 d. Redakcija) 2 dalies atitikties Lietuvos Respublikos konstitucijai, 2003 m. kovo 24 d., byla Nr. 3/01.

Teisingumo teismo sprendimas dėl Prašymo priimti prejudicinį sprendimą – Elektroninių ryšių tinklai ir paslaugos – Direktyva 2002/21/EB – 2 straipsnio c punktas – „Elektroninių ryšių paslaugos“ sąvoka – Signalų perdavimas – Internetu teikiama elektroninio pašto paslauga – „Gmail“ paslauga, bylos Nr. C-193/18, 2019 birželio 13 d.

Teisingumo teismo sprendimas dėl Prašymo priimti prejudicinį sprendimą – Elektroninių ryšių tinklai ir paslaugos – Direktyva 2002/21/EB – 2 straipsnio c punktas – Sąvoka „elektroninių ryšių paslauga“ – Signalų perdavimas – Interneto telefonijos (IP telefonijos) ir fiksuotojo ar mobiliojo ryšio telefono numerius paslauga – Paslauga SkypeOut, bylos Nr. C-142/18, 2019 birželio 5 d.

ELSA MALTA

Contributors

National Coordinator

Matthew Camilleri

National Academic Coordinator

Emma de Gabriele

National Researchers

Matthew Mifsud

Rebekah Cilia

Michaela Pia Camilleri

Kirsty Ellul

Elisa Micallef Peplow

Gianluca Vella

National Linguistic Editors

Maila Cimino

Karen Scerri

National Technical Editor

Luke Bonanno

National Academic Supervisor

Dr Jackie Malli

Introduction

1. Which human rights issues does Advanced Digital Technologies (ADT) pose in your country?

The digital revolution is the greatest dynamic force in our ever-changing world. The right to privacy and data protection in the age of advanced digital technologies (ADT) is not merely a topic of academic interest but one which should interest all because its effects are wide-ranging – from one's personal life to governance, politics and wars. Human rights and ADT, particularly artificial intelligence, have become intrinsically linked. While developments in the field of Artificial intelligence (AI) have many positive uses, AI-driven technology has the capacity to entrench already existing structures of inequality and injustice. AI applications can be used to generate new formations of power and to create a new normal where we are subject to decision-making and actions based on machine automation and tools that aim to predict behaviour, propensity and emotional states.

Artificial intelligence could at face value appear as a neutral matter in respect of human rights matters, but that is not necessarily the case. Any form of ADT is an object which delivers decisions based on algorithms and calculations. Relying on these could lead to a situation where humans trust these technologies on matters far beyond what was envisaged as the purpose of the software. Therefore, it can become a danger to human rights or any legal domain, especially where the basis upon which decisions are taken lack sufficient transparency. Central to any AI legal challenge is the general public's limited understanding of how AI and other advanced technology actually operates.

1.1. Is there or what is a legal framework that provides for procedure on human rights impact assessments? What are other instruments used for identifying human rights issues posed by ADT?

A human rights impact assessment (HRIA) is a process of identifying, understanding, assessing and addressing the adverse effects of a business project or activities on the human rights enjoyment of impacted rights-holders such as workers and community members.⁶³⁹ The prominence of the human rights discourse globally and the proliferation of human rights organisations in the face of continued violation and abuse raises important questions about putting principles into practice.⁶⁴⁰ There have been various forms of 'algorithmic impact assessments' that are applied by those who wish to procure advanced digital technology to improve and resolve any concerns or threats posed to human rights

⁶³⁹ 'Human Rights Impact Assessments | National Action Plans On Business And Human Rights' (National Action Plans on Business and Human Rights, 2021)

<<https://globalnaps.org/issue/human-rights-impact-assessments/>> accessed 2 March 2021.

⁶⁴⁰ Y. Ergas, Human Rights Impact: Developing An Agenda For Interdisciplinary, International Research (2009) 1 *Journal of Human Rights Practice*.

prior to application. Models such as the aforementioned ‘human rights impact assessment’ are concerned more with analysing the impact a system has on human rights rather than focusing on the system itself. With regards to human rights in Malta there is Chapter 4 of the Constitution which deals with laying down a list of fundamental human rights. This is accompanied by the European Convention on Human Rights which is incorporated in the local legal system by virtue of the European Convention Act (Chapter 319 of the Laws of Malta). This parallel protection of human rights is a fundamental aspect of human rights law in Malta, with complainants having the option of invoking the protection of both legal instruments in court proceedings.

1.2. AI and its concern with Human Rights

The ways in which AI is a human rights issue is a complex picture with risks involving various rights such as those of privacy, equality and non-discrimination, freedom of expression – as automatic filters could restrict legitimate speech and encroach on a person’s ability to express themselves – freedom of assembly and association as well as one of the most basic rights – the right to life. It also drastically affects the right to work as AI will lead to increasing automation of various industries and prevent certain people from accessing the labour market. Abroad there is an increased use of AI within the justice system, possibly hindering the right to liberty and fair trial. Particular AI programmes have also, on occasion, displayed gender and racial bias indicating low errors for determining the gender of light-skinned males but high errors in asserting the gender of darker-skinned women: ‘Many [ADT] systems utilise data driven profiling techniques to create digital profiles of individuals and groups across a wide range of contexts, sifting and sorting individuals into categories in order to assist decision-making. When used to automate and inform decision making that substantially affect the rights and significant interests of individuals, data-driven profiling may have serious consequences.’⁶⁴¹

This shows the importance of being vigilant of what we feed and input into these systems. The systems operate by being taught to analyse the data they are given and the more data that is given the more accurate they become. If one inputs data which is biased, it is inevitable that that bias will be ingrained within the system thus producing such unjust results. AI is invisible; it is a technology that weaves itself into the fabric of everyday life and it becomes hard to recognise.

Undoubtedly, the main legal issues posed by AI are threats to the right to privacy, data protection and bias. Privacy is a right to have a personal space free from interference by other people and organisations - it is a fundamental human right, but it is not absolute. AI machines are typically trained by being exposed to big data sets in order to create feedback

⁶⁴¹ *ibid.*

mechanisms. In Europe, the main law through which individuals' privacy is protected is the General Data Protection Regulation (hereinafter referred to as 'GDPR'), which is applicable to all EU member states. The Maltese Data Protection Act (Chapter 586 of the Laws of Malta) implements the GDPR and supplements it in certain situations. Being part of the European Union, Malta must conform to EU laws. Due to this, there are no specific human rights in Malta which are more susceptible to the risks posed by ADT and AI than in any other country and this is due to the enforcement of laws we have being members of the European Union. To reiterate, while the capabilities of AI can be advantageous, those very same capabilities can be used in ways that are fracturing, dividing and can dilute, undermine and threaten human rights.

1.3. The effects of ADT, locally

The same Charter of Human Rights applies across the EU. Malta is also faithful when it comes to implementing data protection laws and laws which safeguard the protection of the individual. However, there could be certain risks when it comes to personal data due to Malta being such a small country. Our population size could pose a risk in the sense that since, in general, Malta is a tight-knit community, any leakage of data could spread faster than it would in other countries. But all in all, Malta is not particularly at risk for a human rights violation than anywhere else. An additional risk in Malta could be the fact that the Maltese government is thoroughly involved in many sectors including education and healthcare. In fact, there are already plans to collate the healthcare data which, although not a harmful thing in itself, if any other information such as tax information and other private details are included, then that could result in a security and privacy risk. Therefore, if a government starts centralising all information about an individual and then, over and above that, adds an AI system, then it could be an issue. The merit of AI is in being able to analyse information at a faster and deeper level than a human being. So, if it recognises patterns and linkages faster than a human being, then data protection might be at risk. Therefore, if a government centralises all this data, it could pose a privacy issue.

Apart from this, the charges and fines posed by the Maltese government for breach of the GDPR are massive but the government itself is liable to smaller fines if found guilty of the same violation. Hence, the fact that a governmental breach of data protection is not treated in the same way as a breach by a private individual or corporation is a risk as it could lead to a misuse of power while endangering confidential information of an individual and going against established international laws entrenched in our own laws.

1.4. How will AI be governed in Malta?

In November 2018, the Maltese government appointed the Malta.AI Task Force to develop a national strategy on Artificial Intelligence. This laid out a plan in order to

integrate AI into society. In addition to this, a framework was compiled to curb risks posed by AI. An ethical framework is absolutely necessary when designing and implementing artificial intelligence solutions for legal professionals. A cornerstone of the Malta Ethical AI Framework is to define the ‘ethical code’ by which AI will be governed. This is because one must focus not solely on AI as technology but also on the effect it has on certain fundamental human rights and be able to intervene where certain applications are considered as high risk, even though the criteria for what is considered to be high risk is contentious. The framework establishes four ethical principles for reliable yet trustworthy AI, namely:

1. human autonomy – humans interacting with AI systems must be able to keep full and effective self-determination over themselves;
2. harm prevention – AI systems should not cause harm at any stage of their lifecycle to humans, the natural environment or other living beings;
3. fairness – the development, deployment, use and operation of AI systems must be fair; and
4. explicability – end-users and other members of the public should be able to understand and challenge the operation of AI systems.⁶⁴²

These principles are formed from the European Commission’s AI HLEG Ethics Guidelines for Trustworthy AI.

2. How is personal information protected in your national legislation?

The progress of technology and information has undoubtedly facilitated our lives, however it has brought about unprecedented ramifications, predominantly the threat to personal privacy. As a result, States have had to react by implementing legislation aimed at the protection of data, dubbed as ‘data protection legislation’, which stipulates how individuals’ personal data should be treated in order that it is protected.

Within the Maltese legal order, the most prominent data protection legislation is the Regulation (EU) 2016/679, the ‘General Data Protection Regulation’, of the European Parliament and the Council of Europe of the 27th April 2016, which was harmonised into the Maltese legal regime as a member state of the European Union.

This regulation deals with the protection of natural persons with regard to the processing of their personal information, and the free movement of such data. This regulation is a

⁶⁴² ‘Understanding Malta’s Artificial Intelligence Framework’ (Times of Malta, 2021) <<https://timesofmalta.com/articles/view/understanding-maltas-artificial-intelligence-framework.747060>> accessed 26 February 2021.

reflection of EU ideology that everyone has the right to have their personal data protected.⁶⁴³

2.1 What is personal information?

The definition of personal data is extracted from the GDPR into the Maltese Data Protection Act (Chapter 586 of the Laws of Malta), which states that the definitions in Article 4 of the EU Regulation apply to it. Personal data is defined in the GDPR as the data relating to an identified or identifiable natural person, the data subject – a natural person to whom the personal data relates.⁶⁴⁴ This includes information such as a person's ID card number, passport number and credit card number. Special categories of sensitive personal data are also protected. This includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, genetic or biometric data which uniquely identifies a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation.

2.2 The Maltese Data Protection Act

The Maltese Data Protection Act, which transposed the GDPR into Maltese law, came into effect on the 28th of May 2018. Both pieces of legislation regulate the processing of personal data, held electronically or manually, to prevent the breach of individuals' personal data.⁶⁴⁵ They aim to prevent breaches of security leading to the accidental or unlawful loss, destruction, alteration, or unauthorised access to data. These laws also offer legal remedies if such breaches occur.

Chapter 586 not only transposed the EU Regulation into the Maltese legal system, but further specified the extent of the law.⁶⁴⁶ It also prevents abuse by the data controller who determines the purposes and means of processing of personal data. In conjunction, the data processor, who processes personal data on behalf of the controller, is equally liable. A data subject may institute an action against the controller and processor if they believe their rights were infringed as a result of the processing of their personal data.⁶⁴⁷

Both the GDPR and the Maltese Data Protection Act provide six key principles which a person who is processing personal data (the 'data controller') must adhere to.

The first principle requires that personal data be processed lawfully, fairly and in a transparent way.⁶⁴⁸ Data subjects must be informed before the data is collected and where

⁶⁴³ Treaty on the Functioning of the European Union, art.16(1).

⁶⁴⁴ GDPR, art. 4.

⁶⁴⁵ *ibid.*

⁶⁴⁶ Data Protection Act, art. 2 (DPA).

⁶⁴⁷ DPA, art. 30.

⁶⁴⁸ GDPR, art. 5(1)(a).

subsequent changes are made. There must be no unlawful use of data such as a breach of confidence, or the improper exercise of power by an authority over such data.

The second principle holds that personal data must be collected for specified, explicit and legitimate purposes in the present and future.⁶⁴⁹ Transparency is necessary in establishing the intention behind collecting such data, as well as fair processing requirements, such as privacy notices to individuals. Should there be a change in purpose, the data subject's consent is required once again. The personal data must be relevant to the purpose in relation to the processing which must be done in the public interest.

The third principle requires data minimisation, whereby personal data acquired is adequate, relevant and limited to what is necessary for the purpose for which they are being processed.⁶⁵⁰

The fourth principle stresses the importance of holding accurate and up to date data as much as reasonably possible, and that the source of the data is clear.⁶⁵¹

The fifth principle expects that personal data be retained no longer than necessary, for the purpose it was processed, as regulated by retention policies. Data that is no longer needed for the intended purpose must be securely deleted.⁶⁵²

The sixth principle is that of integrity and confidentiality whereby personal data shall be processed in a way that ensures its security against unauthorised access, loss, damage and destruction, using appropriate technical or organisational measures.⁶⁵³ A risk assessment must be done on the security of personal data, regarding the extent of access to the data, the number of staff, the presence of a Data protection officer within the premises concerned and more.

2.3 To whom does the Data Protection Act apply?

The Act applies to the processing of personal data with regards to activities of an establishment of a controller or processor in Malta, or in a Maltese Embassy or High Commission overseas and to the processing of personal data of data subjects in Malta by a controller or processor not established in the EU. It also applies to the processing of data collected relating to the offering of goods and services.⁶⁵⁴

2.4 To whom does the Data Protection Act not apply?

⁶⁴⁹ GDPR, art. 5 (1)(b).

⁶⁵⁰ GDPR, art. 5(1)(c).

⁶⁵¹ GDPR, art. 5(1)(d).

⁶⁵² GDPR, art. 5(1)(e).

⁶⁵³ GDPR, art. 5(1)(f).

⁶⁵⁴ DPA, art. 4(2).

The Act does not apply to the processing of personal data collected throughout activities which fall outside the scope of Union law, neither the processing of personal data by the Government of Malta in its activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union, nor the processing by a person in their personal activities, and neither the processing by the competent authorities to prevent, investigate, detect and prosecute criminal offences. It also does not apply in the processing operations concerning public security, defence, state security and activities of the state.⁶⁵⁵

2.5 Subsidiary Legislation

The Data Protection Act is accompanied by various pieces of subsidiary legislation, or 'regulations' in the implementation of the EU Regulation. These deal with matters such as the processing of health information for insurance purposes and the processing of personal data in relation to the General Election Act, and the Local Councils Act. These regulations are:

- Processing of Personal Data (Electronic Communications Sector) 2003 ('the Electronic Communications Regulations')
- Notification and Fees (Data Protection Act) 2003 ('the Notification and Fees Regulations')
- Third Country (Data Protection Act) 2003
- Processing of Personal Data (Protection of Minors) 2004 ('the Protection of Minors Regulations')
- Transfer of Personal Data to Third Countries Order 2012
- Processing of Personal Data for the purposes of the General Election Act and the Local Councils Act 2013
- Processing of Personal Data (Education Sector) 2015
- Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties 2018 ('the Criminal Data Processing Regulations')
- Restriction of the Data Protection (Obligations and Rights) 2018
- Processing of Data concerning Health for Insurance Purposes 2018 ('the Processing Health Data for Insurance Purposes Regulations')
- Processing of Child's Personal Data in relation to the Offer of Information Society Services 2018 ('the Processing of Child's Data Regulations')

2.6 Supervisory and Adjudicating Authorities

⁶⁵⁵ DPA art. 4(1).

The Information and Data Protection Commission (IDPC) was set up as a national supervisory authority on data protection, which publishes several guidelines on its website on the matter and states the rights of individuals and organisations in the matter. It monitors and enforces the provisions of the GDPR, the Data Protection Act and the Freedom of Information Act, ensuring that public authorities observe the requirements therein contained.

The IDPC's objectives are the entrenchment within society that the safeguarding of data protection is not a mere legal burden but a natural process within organisations' operations. It also takes action against controllers who infringe the GDPR and data protection law. Furthermore, it assists in the consistent application of the GDPR by cooperation with other European bodies of a similar role.

The decisions of the IDPC regarding data breaches can be appealed to the Information and Data Protection Appeals Tribunal, after which the parties may take the case to the Court of appeal.⁶⁵⁶⁶⁵⁷ Moreover, a data subject may also institute an action against the controller and processor by a sworn application to the First Hall of the Civil Court.⁶⁵⁸

Another supervisory official is the Data Protection Officer (DPO) appointed when processing is carried out by a public authority.⁶⁵⁹ The DPO is to inform the controller or processor of GDPR obligations, monitor compliance, provide advice regarding impact assessments, cooperate with the supervisory authority and assess risks associated with processing operations.

2.7 Data Protection Impact Assessment

As previously mentioned, a role of the DPO is to give advice on impact assessments. Data Protection Impact Assessments help public authorities identify and reduce the privacy risks of a new system dealing with the collection or processing of personal data.⁶⁶⁰ Public authorities must propose solutions to minimise possible risk factors, such as deciding not to collect or store particular types of information, devising retention periods and implementing security measures.

⁶⁵⁶ DPA, art. 26.

⁶⁵⁷ Code of Organisation and Civil Procedure, Article 41(6) (COCP).

⁶⁵⁸ DPA, art. 30.

⁶⁵⁹ DPA, art. 33.

⁶⁶⁰ GDPR, art. 35.

3. To what extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?

One cannot really speak of any additional regulation in this field of law over and above the two main pieces of legislation already amply discussed, namely the GDPR and the Data Protection Act. The fact that these laws are cross-sectoral - they apply in the same manner to all sectors, both public and private – is another reason why self-regulation by the private sector is not of particular importance or necessity.

However, the official IDPC website does make reference to a number of sector-specific ‘guidelines’ issued following a collaborative exercise between the relevant associations and authorities in the concerned sectors and the IDPC itself.⁶⁶¹

For instance, the Malta Bankers’ Association and the Malta Gaming Authority, following consultation with the IDPC, issued two documents titled ‘Data Protection Guidelines for Banks’ and ‘The General Data Protection Regulation Guidelines issued by the Malta Gaming Authority, in consultation with the Information and Data Protection Commissioner, for the Maltese Gaming Industry’ respectively.⁶⁶²⁶⁶³ These documents are intended to clarify those sections of the GDPR which may not be entirely clear, or which could lend themselves to differing interpretations, in order that a common understanding is arrived at and a consistent interpretation is applied across the banking and gaming sectors.

The IDPC has also, unilaterally, issued further documentation containing sector-specific guidelines on political campaigning and credit referencing.⁶⁶⁴⁶⁶⁵

4. What is the process of judicial review of cases data protection breaches?

4.1. Judicial Review in Data Protection Breaches

Maltese Administrative Law creates a system whereby Legislative Acts of Parliament establish administrative tribunals which are empowered to welcome appeals from aggrieved persons assessing the legality of administrative acts. As a result, such administrative tribunals are endowed with a judicial, or more accurately, a quasi-judicial function. Generally speaking, decisions from such administrative tribunals are subject to appeal to

⁶⁶¹ Information and Data Protection Commissioner, ‘Data Protection for Organisations: Guidelines’ (idpc.org.mt), < <https://idpc.org.mt/for-organisations/guidelines/> > accessed 25 May 2021.

⁶⁶² *ibid.*

⁶⁶³ *ibid.*

⁶⁶⁴ *ibid.*

⁶⁶⁵ *ibid.*

the Courts of Justice. The relevant tribunals in cases of data protection breaches are the Administrative Review Tribunal established by the Administrative Justice Act and the Information and Data Protection Appeals Tribunal established by the Data Protection Act 2018.

However, before going to an analysis of these tribunals, it is important to take a step back and analyse the other main players involved in data protection breaches which will help the reader understand the judicial process in this scenario more effectively.

The Data Protection Act is an important point of analysis. The Act was overhauled after the enactment of the General Data Protection Regulation of the European Union.⁶⁶⁶ The regulation of the European Union has direct effect on the Member State, in this case Malta, without the need for transposition of the law for it to be binding on the Member State. However, the Maltese legislator felt the need to ‘implement and further specif(y) the relevant provisions’ of the GDPR.⁶⁶⁷

4.2. The Information, Data Commissioner and Statutory Requirements for the Establishment of the Commissioner’s Office.

Amongst other things, the Data Protection Act establishes the office of ‘The Information and Data Protection Commissioner’.⁶⁶⁸ The office of the Commissioner was established before the enactment of the General Data Protection Regulation of the EU; indeed, it was established prior to Malta’s accession to the European Union. The original article establishing its office was Article 36 of Part VIII of Chapter 440 of the Laws of Malta enacted in 2002, which has since been repealed. The new Data Protection Act was amended and enacted as a new act in order to adhere to the requirements established by the GDPR. Indeed, Article 11 of the said act, provides that the Commissioner is to be the statutory supervisory authority required by Chapter VI of the GDPR.⁶⁶⁹

Under the current domestic law, the Commissioner is appointed by the Prime Minister, who in Malta, is the head of the executive organ of the state. In this case, as is the case in many similar appointments, the Prime Minister is bound to consult with the Leader of the Opposition when appointing the Commissioner. No requirement of agreement between the two is required. Under the current Executive portfolio, the Commissioner falls under the Ministry of Justice, Equality and Governance. At the time of writing the most recent

⁶⁶⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

⁶⁶⁷ DPA, art. 2.

⁶⁶⁸ DPA, art. 11.

⁶⁶⁹ GDPR, art. 51.

appointment was made by the Government of Malta after the publishing of a notice in the Government Gazette with effect from the 21st December 2020 of Mr. Ian Deguara.

The tenure of office is of a term of five years at the expiration of which the Commissioner can be reappointed.⁶⁷⁰ It is important to note that the Commissioner enjoys security of tenure. Indeed, his removal can only be made after a vote obtaining a qualified majority of all the members, not merely of those present & voting, of the House of Representatives on the grounds of 'proved inability to perform the duties of his office (whether arising from infirmity of body or mind or any other cause) or proved misbehaviour'.⁶⁷¹ This is particularly significant in the backdrop of Article 52 of the GDPR which provides that the supervisory authority of the Member State must be independent from external influence be it direct or indirect.⁶⁷²

4.3. Competence and Functions of the Commissioner

In order to better understand the remedies available to the individual in cases of data protection breaches, it is imperative to clarify the competence afforded to the Commissioner in its supervisory, regulatory and judicial functions.

The points of reference here are Articles 55 and 56 of the GDPR in comparison with ad hoc provisions found in the Data Protection Act. There exist significant overlaps between the two, with the latter providing for certain powers going beyond the Regulation which are helpful for the purposes of this domestic research.

Article 11(2) of the Data Protection Act states that the Commissioner is the legal person responsible 'to protect the fundamental rights and freedoms of natural persons in relation to processing of personal data and to facilitate the free flow of personal data'.⁶⁷³

Article 57 of the Regulation lays down the tasks with which the Commissioner is endowed. These include supervisory, enforcement, social, advisory, regulatory, investigatory functions inter alia. For the purposes of this journal, it is of imperative importance to note that the individual has the right of complaint to such authority whenever any one of his or her rights to data protection have been breached. In turn, the Commissioner is obliged to consider the complaint and investigate the merits of such a complaint.

The question arises as to how the Commissioner is expected to investigate. Indeed, both the GDPR and the Data Protection Act endow the Commissioner with investigative powers. These include the right of access to information to enable the Commissioner to

⁶⁷⁰ DPA, art. 14.

⁶⁷¹ DPA, art. 14 (3.)

⁶⁷² GDPR, art. 52.

⁶⁷³ GDPR, art. 51.

gather a complete picture of the situation. This includes physical access and powers to search premises. Such an operation can be carried out with the assistance of the Executive Police.

4.4. The Controller

Having established the competence and function of the Commissioner, one now needs to turn to the obligations of the controller and the role he plays in ensuring that the rights of the individual are not overlooked and indeed safeguarded.⁶⁷⁴

The controller is defined as a natural or legal person which plays a role in determining the purposes and means used in processing personal data.⁶⁷⁵

Thus, it is abundantly clear that the controller is the central figure in the collection and processing of data from the data subject. This in turn burdens him with obligations to ensure that the principles relating to processing of personal data are upheld. These include those principles relating to lawfulness, fairness, and transparency, purpose limitation, data minimisation, accuracy of data, storage limitation and integrity and confidentiality. The controller is accountable and responsible for any breaches of the abovementioned principles.⁶⁷⁶ Moreover, it is the controller who is attributed the legal burden of liability in cases of breaches.⁶⁷⁷

4.5. The Individual and The Data Subject

The different rights of the individual have already been commented upon at length. Here, the judicial process pursuant to a data protection breach is of particular relevance.

When any individual feels aggrieved that his rights and freedoms with regards to data protection have been breached, there are a number of avenues available to him. The point of departure is that the individual has a right to confirm whether or not his or her data is being collected or processed by the controller.⁶⁷⁸ This is referred to as the individuals' right of access. Thus, what the individual can do, and should do, in suspected breaches is to check whether in the first place his or her data has been or is being collected and / or processed. The controller in turn is under the legal obligation to provide a copy of any of the data being processed.

If at this juncture the individual feels that there has been a breach of his or her rights to data protection, there are a number of avenues which one can explore in order to enforce

⁶⁷⁴ GDPR, art. 24 – 43.

⁶⁷⁵ GDPR, art. 4.

⁶⁷⁶ GDPR, art. 5.

⁶⁷⁷ DPA, art. 20.

⁶⁷⁸ GDPR, art. 15.

his data protection rights. The first option is to contact the controller himself quoting the data protection breach in question; requesting rectification or erasure. Alternatively, the data subject has the right to lodge a complaint with the Commissioner who is then under the obligation to take it upon himself to investigate and determine the outcome of the complaint.

Moreover, the data subject has a right to an effective judicial remedy against the controller or processor.⁶⁷⁹ This includes the right to compensation and liability.⁶⁸⁰ The compensation is subject to damages caused which might be pecuniary and non-pecuniary which has arisen as a result of the infringement of the Regulation.

In essence, what this means is that the data subject, either following the Commissioner's investigation, or from his own esteem, may institute proceedings against the controller and/or processor for the damages which may have arisen from the infringement. The data subject thus has a normal right of access to a court whereby he would have to prove juridical interest as is the case in any other civil matter. In Malta, civil matters are heard by the First Hall of the Civil Court subject to an appeal to the Court of Appeal.⁶⁸¹ Thus, here it can be said that the judicial process relating to the parties which are the data subject and the controller and / or processor are undergone in front of the Courts of Justice of Malta in their Civil jurisdiction. Matters between private individuals, and data breaches between the said individuals, are not dealt with as such by statutory tribunals. The action of the aggrieved individual is time-barred by a period of twelve months from when the data subject became aware, or reasonably ought to have become aware. When there is a data protection breach undertaken by a public administration a different procedure and process is triggered which will be discussed further below.

4.6. Liability arising from Administrative Fines and Criminal Offences

It must be said that such liability from the controller regarding the data subject arises independently from any administrative fine which might be issued by the Commissioner. Indeed, Part VI of the Data Protection Act deals with Administrative Fines and Penalties. It is said that the Commissioner exercises both an investigative and judicial function, in that it is his office that investigates complaints and possible data protection breaches, and it is the same office of the Commissioner which dishes out the relevant administrative fine.

An example of the issuing of an administrative fine to a private legal person can be identified when the Commissioner imposed a €5000 fine to HSBC following a complaint lodged by an employee of the bank in 2019. The complaint was lodged on two grounds.

⁶⁷⁹ GDPR, art. 79.

⁶⁸⁰ GDPR, art. 82.

⁶⁸¹ COCP, art. 2.

The first related to the fact that the bank had carried out ‘a fact-finding mission’ which entailed the monitoring of the employee’s bank account. The Commissioner found that the bank had unlawfully processed the employee’s data and imposed the administrative fine.⁶⁸² The second ground which was not accepted by the Commissioner as a breach of data protection was based on the fact that the bank had knowingly taken and processed social media posts of the individual without his consent. The Commissioner found that there had been no breach of data protection here because the bank had a policy regarding social media use.

Article 22 of the Data Protection Act also creates a number of criminal offences related to data breaches. These include the purposeful provision of false information to the Commissioner while the latter is investigating, and the non-compliance with any of his lawful requests. In such cases, the sanctions are, of course, no longer administrative, but criminal in nature with fines up to €50,000 and / or imprisonment up to six months. The type of sanction here indicates that the offences outlined in this section can be classified as crimes rather than contraventions.⁶⁸³ The law clearly states that since this section involves a criminal sanction, the Commissioner is to involve and provide information to the Executive Police.

5. Does the review constitute effective protection of data privacy?

5.1 The Data and Information Protection Appeals Tribunal

The judicial function of the Commissioner in imposing administrative fines is no derogation to the rule of *nemo iudex in causa propria* since in the case of such administrative fines and offences the ‘accused’ has the right of appeal to an independent and impartial tribunal. In cases of data breaches, the relevant tribunal is established by Article 24 of the Data Protection Act named ‘The Information and Data Protection Appeals Tribunal’. The Tribunal is composed of a chairperson and two other members appointed by the Minister. The chairperson is to be a technical person with a minimum of twelve years’ experience as an advocate, together with the necessary qualifications, experience and skills in the protection of personal data. The members of the Tribunal cannot be removed unless it is proven that they are no longer able to perform their functions or in cases of proved misbehaviour.⁶⁸⁴

Any person who is subject to a decision from the Commissioner is legally bound by such decision. That person, however, has a right of appeal to the tribunal made within twenty

⁶⁸² Times of Malta, ‘HSBC Fined 5000 for monitoring employees bank account’ (Timesofmalta.com), <<https://timesofmalta.com/articles/view/hsbc-fined-5000-for-monitoring-employees-bank-account.728921>> accessed 25 May 2021.

⁶⁸³ Criminal code, art. 7 (1).

⁶⁸⁴ DPA, art. 24 (5).

days from the intimation of such decision. This appeal can be based on the grounds that there had been a material error as to the facts of the situation, that there had been a material procedural error or that the decision possesses some sort of illegality deriving from a lack of reasonableness or proportionality.⁶⁸⁵

The decision of the Tribunal is final and binding and has the same powers as is afforded to the First Hall, Civil Court according to law. Naturally, the Tribunal is empowered with the prerogative to summon persons to appear before it for reasons of evidence. It also has the power to appoint experts as it deems necessary to assist and advise it on matters of a technical nature. The procedure of the Tribunal is also regulated by itself. Upon deciding, the Tribunal has the discretion to dismiss the appeal and confirm the decision of the Commissioner in its entirety, to substitute, modify, vary, or annul the decision.⁶⁸⁶

Article 29 of the Data Protection Act also provides for the possibility of a further appeal to the Court of Appeal. This appeal may be made both by the Commissioner or by the initial plaintiff, should either party feel aggrieved by the decision of the Tribunal. Such application must be filed within twenty days from the date of the intimation of the decision of the Tribunal.⁶⁸⁷

This essentially means that while the Commissioner has a judicial function in carrying out its enforcement and regulatory competence, as is expected in a functioning system governed by the rule of law, there is a right of appeal in front of an impartial and independent statutory tribunal which acts as a court of first instance. As in other areas of the law, there is a further appeal to the Court of Appeal of the Courts of Justice.

In cases where an administrative fine is issued by the Commissioner such fine shall not be final (*res judicata*) until the person to whom the fine is issued has exhausted all the remedies available to him, or if that person has allowed the time-limits available to him to expire. In such a case, his liability would arise with effect, and with the possibility of the Commissioner using its capacity as a legal person to institute civil proceedings to claim such liability civilly in order to render effective the sanction.

A Freedom of Information Request to the Commissioner in 2020 revealed that the Commissioner has issued a total of 30 administrative fines from 2013 to 2020. Nineteen of these fines were imposed using the legal power granted to the Commissioner by the old Data Protection Act, whilst another nine were issued under the GDPR. After the direct

⁶⁸⁵ DPA, art. 26 (2).

⁶⁸⁶ DPA, art. 28.

⁶⁸⁷ DPA, art. 29.

effect of the GDPR came into force, the Maltese supervisory Authority, the Commissioner, has almost always resorted to the GDPR in imposing fines.⁶⁸⁸

5.2. The Right to an Effective Remedy against the Commissioner by the Data Subject

There are still a number of issues that must be dealt with in order to create a comprehensive picture that includes other possibilities between the players involved. The next point to be discussed is the right that the data subject has to an effective remedy against the Commissioner.

Indeed, as has been outlined previously, the data subject has the right to lodge a complaint with the Commissioner who in turn has the powers available to him to investigate and establish the facts of a given situation to determine whether or not there has been a breach of data protection. If the data subject feels that the Commissioner has not handled the complaint adequately, then the aggrieved data subject may bring the matter before the Tribunal.^{689 690} In turn, the Tribunal, if it feels that the data subject is justified in his appeal, then it may order the Commissioner to act in the adequate manner to remedy the situation.

These provisions ensure that the Commissioner does not abdicate from his supervisory function whilst ensuring that the data subject has his right of complaint upheld by the competent public administration.

5.3. Administrative Fines imposed on the Public Administration

Matters relating to administrative fines imposed upon the public administration itself merit a discussion of themselves. In this scenario, the Office of the Commissioner is in a peculiar position. The Commissioner is a civil servant and thus part of the public administration in general. Central to the role of the public administration in general, is the collection and processing of data for countless reasons, *inter alia*, public security, convenience, health & safety, accounting, employment, payroll, taxes, utility billing, planning, licenses. This is done through different databases by different public authorities endowed with separate legal personalities (which will be of relevance shortly).

Public authorities vested with special authority are still subject to the principles of lawfulness of processing. Indeed, their special position means that data processing is justified because it is in the public interest to have centralised databases of the State:

⁶⁸⁸ View Malta, 'Violations Of Data Protection Laws In Malta – 30 Fines Of Less Than €5,000 In 7 Years' (Transparency Malta, 2021) <<https://transparencymalta.wordpress.com/2020/04/03/violations-of-data-protection-laws-in-malta-30-fines-in-7-years-of-less-than-e5000/?fbclid=IwAR3SR6edsXUf-loVrPu1fbb1g-818NV09YNboqtQOBOnD29vA0tas1QJrg>> accessed 29 May 2021.

⁶⁸⁹ DPA, art. 31.

⁶⁹⁰ GDPR, art. 78 (2).

essential for any well-functioning society.⁶⁹¹ Having said that, public authorities are still subject to the same principles and breaches thereof would result in an administrative penalty that can amount to a maximum of up to €25,000, and €50 for each day the violation persists.⁶⁹²

The most notable case of such data breach was made by the Lands Authority, which had failed to ensure that security measures were up to standard to prevent access by unauthorised third-parties to data of private data subjects.⁶⁹³ As a result, over 10 gigabytes of such data were available to the general public which was accessible via a simple google search. After an investigation by the Commissioner, it was found that the leaked data had contained sensitive data which included correspondence between individuals and the Lands Authority.⁶⁹⁴ The Lands Authority was fined a total of €5,000, the biggest fine ever imposed by the Commissioner to date.

5.4. A General Overview of Judicial Review of Administrative Action in Malta

The next step is to analyse the effective remedy that the data subject has when the alleged breach has been committed by a public authority. As has been previously discussed, the individual data subject has the ordinary civil right to take action against the controller of the processor. What is being contemplated here is the very real possibility that the controller or processor is the public authority itself. This touches greatly upon administrative law.

In order to engage in a resourceful discussion as to the process of judicial review in cases of data protection breaches in Malta, one needs to qualify the process of judicial review more generally in the local context within the national legal system.

Judicial review is the assessment made by a competent authority, in the form of a court or tribunal, of a decision of the public administration.⁶⁹⁵ Thus, the author shall be dealing with judicial review of administrative action in Malta, first generally, then applying those facts to data protection breaches more specifically.

The point of departure is that judicial review in Malta has a rich history with the Maltese Courts of Justice long asserting their role as ‘reviewers’ of the administration.⁶⁹⁶ The doctrine of judicial review is derived and based on an Anglo-Saxon Model. Indeed, similar

⁶⁹¹ GDPR, art. 6 (1) (e).

⁶⁹² DPA, art. 21.

⁶⁹³ Land Authority Act.

⁶⁹⁴ IDPC, ‘Lands Authority Personal Data Breach’ (edpb, 2021)

<https://edpb.europa.eu/news/national-news/2019/idpc-lands-authority-personal-data-breach_en> accessed 29 May 2021.

⁶⁹⁵ Ivan Mifsud, *Judicial Review of Administrative Action in Malta*.

⁶⁹⁶ *ibid.*

to the UK, in the Maltese Legal System there exists no special administrative judicial organ such as the Conseil d'Etat in France.⁶⁹⁷ On the contrary, this function is taken upon by the Courts of Justice which assess and review acts of the administration. Having said that, it must be noted that such matters are often resolved at preliminary stages either through internal review carried out by the public administration itself or by statutory tribunals which are available to grant an adequate remedy without having to resort to the Courts of Justice.

These powers of scrutiny afforded to the Maltese Courts can be, and indeed have been, used to review actions of the public administration relating to its executive, judicial and legislative functions. The most important points of reference in this scenario are article 469A of the Code of Organisation and Civil Procedure, and article 116 of the Constitution of Malta.⁶⁹⁸⁶⁹⁹

Article 469A deals with the review of 'administrative acts' defined as follows: '*administrative act* includes the issuing by a public authority of any order, licence, permit, warrant, decision, or a refusal to any demand of a claimant, but does not include any measure intended for internal organization or administration within the said authority.'

From a *prima facie* analysis, one can extrapolate the fact that this definition is not exhaustive but indicative of what the words 'administrative act' include. The Court, in its undertakings during a judicial review action, establishes whether the act that it is being called upon to review, is indeed an administrative act as per this definition.

This is an area which lacks clarity and is subject to great debate. The situation is such that the review of acts of a legislative nature has to be requested through a constitutional action, though it is still as such a prerogative of the public administration. On the other hand, the review of other administrative acts, including those of an executive and judicial nature, has to be requested through article 469-A of the COCP. These are subject to different procedures, and a confusion of either at an early stage could result in one's case being thrown out on this technicality. This is done notwithstanding the fact that all the above-mentioned acts are essentially acts of the public administration which are, or should be reviewable, albeit on the basis of a separate article of law. Thus, this somewhat 'subjective' nature of the act: whether it is a judicial, legislative or executive act is a determining factor for the admissibility of the action brought forth.

The above analysis is a simplistic, and perhaps distorted, insight into the workings of judicial review actions in Malta. More relevant to the question at hand is the Administrative

⁶⁹⁷ [1972] John Lowell noe et v. Onor. Carmelo Caruana et (FH).

⁶⁹⁸ COCP, art. 469A.

⁶⁹⁹ Constitution of Malta, art. 116.

Justice Act.⁷⁰⁰ Article 5 sets up the Administrative Review Tribunal which is competent to review administrative acts of the public administration on points of law and points of fact.

Acts of the public administration undoubtedly include the processing of data of its subjects and otherwise. This fact opens up the possibility of breaches of data protection rules and principles. The data subject like in any other situation may lodge a complaint with the Information and Data Protection Commissioner. As discussed above, the Commissioner may issue an administrative fine to the public authority. But how may the data subject get an effective remedy from the public authority?

The point of departure is the unassailable rule that the data subject may not resort to the ordinary courts on a judicial review action if he has another mode of contestation available to him.⁷⁰¹ This means it is imperative to analyse whether or not there is another mode of contestation available to the data subject

The data subject has a right enshrined in legislation to request the data controller to rectify or erase his or her data as the case may be. The question arises as to whether the exercise of this right would be a mode of contestation. A recent account of Maltese jurisprudence shows that this would not be a mode of contestation because the strict interpretation has been that such contestation must be made available before a court or tribunal.⁷⁰²

This leads us to take a look at the tribunals available for remedy to the data subject. The Information and Data Protection Tribunal as analysed above, is largely limited to appeals lodged by a ‘defendant’ or else by a data subject who feels that his complaint lodged to the Commissioner has not been given due attention.

This leaves us with the Administrative Review Tribunal which is the relevant tribunal for matters of review of administrative actions. The data subject can thus bring his case before the Administrative Review Tribunal which will determine whether or not the public authority has followed good administrative practice in particular with regard to the data protection principles. It will also see to the question whether the data protection breach alleged is a justified derogation to the rule or not subject to the principles of proportionality and reasonableness. There is an appeal from the Administrative Review Tribunal to the Court of Appeal which may uphold, substitute, alter, or revoke the tribunal’s decision.

⁷⁰⁰Administrative Justice Act, art. 5.

⁷⁰¹ [2020] John Cutajar v. Alfred Sant Manduca.

⁷⁰² [2018] Lt. Colonel Andrew Mallia v. Commander Armed Forces of Malta.

6. What is the process of judicial review of anti-discrimination cases?

Similar to any other situation of data protection breach which may arise, the competent authority dealing with cases of anti-discrimination is the Information Data Protection Commissioner (IDPC).

As analysed above, individuals have an individual right of complaint to the IDPC in cases of discrimination whereby the IDPC and his office is empowered by law to investigate and establish facts of such alleged discrimination.

Discrimination is prohibited expressly by law both statutorily and also constitutionally. The law lays down that profiling which results in the discrimination against natural persons on the basis of their particular categorisation is prohibited.⁷⁰³ This categorisation includes the processing of data which reveals racial, ethnic origin, political opinions, religious and philosophical beliefs *inter alia*. These are the principles which govern the subsidiary legislation abovementioned.

The IDPC, in the exercise of its functions, also issues sectorial advice to ensure compliance with such anti-discrimination principles.⁷⁰⁴ For instance, if, in the banking sector, there is a personal data breach of the bank's clients, then the bank shall notify the IDPC if the data breach includes data profiling or processing which could potentially lead to discrimination against that particular individual.

Moreover, an aggrieved individual also has the right to lodge a complaint with the Parliamentary Ombudsman's office if the alleged discrimination was carried out by the Public Administration.⁷⁰⁵ The Ombudsman is empowered to scrutinise administrative acts, both on his own initiative but also upon receipt of a complaint from the general public.⁷⁰⁶ It is felt that the Ombudsman has more resources than the IDPC given that it is a Parliamentary office. However, depending on how technical the issue at hand is, and whether it at all deals with the public administration, the individual is at liberty to lodge a complaint at either of the two statutory bodies.

If it is found that as a result of the data processing or data breach there has been discrimination or there is the possibility of discrimination, the private individual has the right to lodge a constitutional action or a civil action.⁷⁰⁷ The individual may claim material

⁷⁰³ Legal Notice 168 of 2018, art. 10-11.

⁷⁰⁴ IDPC, 'Data Protection Guidelines for Banking' (Idpc.org.mt, 2021). <<https://idpc.org.mt/wp-content/uploads/2020/07/Data-Protection-guidelines-for-banking.pdf>> accessed 29 May 2021.

⁷⁰⁵ Ivan Mifsud, *The Ombudsman Remedy In Malta* (1st edn, Book Distributors Ltd 2020).

⁷⁰⁶ *ibid.*

⁷⁰⁷ Constitution of Malta, art. 45.

and moral damages. Though it is unlikely that non-pecuniary damages be granted to the plaintiff due to the rigid interpretation of the Latin principle *restitutio in integrum*.

7. Does your country have any specific regulations on advanced digital technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?

Advanced digital technologies include a wide variety of technologies that within their very nature bring about societal change. This impact is dependent on their use and this necessitates that such technologies are legislated.⁷⁰⁸ In 2018, Malta became one of the first countries to enact a regulatory framework for blockchain technologies and cryptocurrency, which falls within the general term of advanced digital technologies. Blockchain, while still synonymous with financial applications, has the power to go beyond this sector. One example is the AID:Tech project which tracks the flow of refugees through conflict zones.⁷⁰⁹

Three bills were enacted into law, focusing on blocking and the concept of distributed ledger technology (DLT). One of the laws created the Malta Digital Innovation Authority (MDIA) which serves as the local regulator for blockchain technology.⁷¹⁰ Malta is one of the first countries whereby such an authority will solely focus on cryptocurrencies, avoiding conflict with the stock market.

Malta also enacted the Innovative Technology Arrangements and Services Act (ITAS) to govern the registration of technology service providers and the certification of software and IT architectures used in designing and delivery DLT contracts. This Act provides strict rules in order for such entities to be certified, as well as giving legal status to smart contracts, in the same way as traditional contracts.⁷¹¹

Smart contracts, as defined in the MDIA Act, Article 2, must be contrasted with traditional contract law as stipulated in the Maltese Civil Code, although it can be deemed that the ITAS Act does not consider the essential requisites of a smart contract in the same way as the Civil Code. It has been concluded that the ITAS act did not seek to tackle or expressly take a position as to whether smart contracts are considered legally valid contracts at law.⁷¹²

⁷⁰⁸ Karen Yeung, 'A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework', (2019) DGI 05.

⁷⁰⁹ Andrej Witter, Mathilde Boisee-Despiaux, 'Blockchain for humanitarian action and development aid' (2018) 3 Journal of International Humanitarian Action <<https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-018-0044-5>> accessed 1 March 2021.

⁷¹⁰ The Malta Digital Authority Act 2018, s. 2.

⁷¹¹ Innovative Technology Arrangements and Services Act.

⁷¹² Emma Blake, 'Smart Contracts: Legal Regulation in a Decentralized Environment', LL.B. thesis, University of Malta (2019).

Another legislation was enacted named the Virtual Financial Assets Bill which set up a framework for cryptocurrency-related services.⁷¹³ A government agency, called Tech.mt, was also created to provide for better communication between the government and future foreign investors.⁷¹⁴ Locally, the idea was also floated that blockchain could be used in the healthcare industry for the handling of an individual's medical data.⁷¹⁵ A number of guidelines have also been issued on the subject by the MDIA.⁷¹⁶

The MDIA is the Authority that deals with all matters related to advanced digital technologies. One of its aims is to ensure that Malta, in dealing with advanced digital technologies, is in line with internal norms, particularly those of the EU. It is also this Authority that provides initiatives for legislation on the subject. It also works with Data Protection Authorities to protect personal data.⁷¹⁷ It has been argued that the European Data Protection Regulation and the ancillary framework (GDPR) have come into conflict with blockchain technology. The GDPR came about before blockchain was legislated and failed to take into account many of the principles of blockchain technology.⁷¹⁸

The GDPR, for example, requires the need of one data controller, however, this goes against the concept of blockchain, which decentralizes responsibility. The GDPR also ensures that personal data can only be modified or erased, following a request from the data controller. However, with blockchain, this cannot be done and is probably the keystone of the technology. DLT's require replication of data while the GDPR calls for data minimization. Having said this, blockchain is also instrumental to data transparency, provides increased control on who accesses the data, which is the basis of Article 15 of the GDPR, as well as the better management of personal data, covered by Article 20 of the GDPR.⁷¹⁹

On artificial intelligence, in October 2019, Malta launched a strategy with the aim being for Malta to gain a strategic competitive advantage in the global economy as a leader in the field of AI. As with blockchain, and other such technologies, AI could affect and impinge on human rights and the strategy took this into consideration by aiming to set up a

⁷¹³ Virtual Financial Assets Act.

⁷¹⁴ Supporting the Technology Industry in Malta' (tech.mt) < <https://tech.mt/technology-industry-malta/> > accessed 01 March 2021.

⁷¹⁵ Emeka Chukwu and Lalit Garg, 'A systematic review of blockchain in healthcare: frameworks, prototypes and implementations' (2020) IEEE Access 21196; Priscilla Mifsud Parker, 'A blockchain for the provision of healthcare' (Chetcuti Cauchi Advocates, 1 October 2019) <<https://www.ccmlta.com/publications/a-blockchain-for-the-provision-of-healthcare>> accessed 1 March 2021.

⁷¹⁶ Malta Digital Innovative Authority, <<https://mdia.gov.mt/sa-guidelines/>> accessed 2 March 2021.

⁷¹⁷ *ibid.*

⁷¹⁸ Michele Finck, 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?' Scientific Foresight Unit (July 2019) accessed 2 March 2021.

⁷¹⁹ *ibid.*

Technology Regulation Advisory Committee.⁷²⁰ AI, along with other such advanced digital technologies challenge our existing legal, moral and social conceptions of responsibility. Task automation and machine autonomy, just to name two attributes, are likely to affect others.⁷²¹

This Committee would be formed to advise on laws and regulation with respect to AI matters and the creation of regulatory and data sandboxes. It shall have the specific aim of assessing and determining the extent to which existing laws and regulations will apply to AI technologies (matters relating to IP and liability-related issues will be a priority). The Committee shall also analyse local laws and regulations that may need to change to keep pace with technology, monitor and consider developments at a European level, and advise on the setting up of a Regulatory Sandbox for AI.⁷²²

Malta is also currently working on a Private Law Bill that aims to provide clarity on specific provisions related to IP and liability issues in the context of DLT. Malta also aims to analyse if further regulation is necessary to deal with IP rights in AI-generated outputs. Issues such as liability-related issues, open-source development and automated decision making will also be looked into from a legal perspective to make sure the AI systems can flourish but also to ensure the technologies are clearly legislated. Furthermore, Malta will look into competition law and the antitrust aspects of AI with respect to the control of data.

It is thought that there might be certain regulations which restrict new AI applications and for this reason, Malta is to set up a Regulatory Sandbox for AI. Such a sandbox will allow exemptions from legislation to explore these new technologies with proportionate safeguards, in a contained environment for a well-defined duration. Sandbox tests are expected to be modelled on particular use cases. The Technology Regulation Advisory Committee will work with the MDIA as to the best way this sandbox can function.⁷²³

Having said that, Malta is committed to ensuring that personal data is protected (through the GDPR) and therefore, the Office of the Information and Data Protection Commissioner (IDPC), as national data protection authority, should eventually set up a Data Sandbox to support organizations that need to use personal data in the process of developing or testing innovative products and services in the specific area of AI. Such an organization must keep in line with the GDPR, and it is this the IDPC that will assist in such matters.⁷²⁴

⁷²⁰ 'A strategy and vision for artificial intelligence in Malta 2030' (*malta.ai*, October 2019) < <https://malta.ai> > accessed 2 March 2021.

⁷²¹ *ibid* (n 644).

⁷²² *ibid* (n 648).

⁷²³ *ibid*.

⁷²⁴ *ibid*.

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?

Encryption remains a controversial topic around the globe, with different countries providing different solutions, none of which are straightforward.⁷²⁵ As technology also advances, especially at the rapid rate it has currently set, challenges also arise within the legal world.

Within the context of criminal investigations, encryption is a major obstacle across the different fields of criminal law.⁷²⁶ Devices, like mobile phones which are encrypted, provide criminals with a path for communication, which goes beyond the means of interception of the police. This is further compounded by the use of encryption by social media companies, which also add to the challenges faced during criminal investigations. This is especially perturbed when end-to-end encryption is used by these companies, meaning that they are unable to provide assistance to the police (or other law enforcement).⁷²⁷

While law enforcement's intervention is a subject which is highly controversial due to privacy and secrecy of communications, which are widely recognised as reasonable expectations of citizens, it is commonly acknowledged that law enforcement does need to intervene. This would need to be done with a legitimate reason for intervention, keeping in mind the public trust and privacy, but how it is done remains the question to be answered.⁷²⁸

One of the solutions proposed by Levy and Robinson in a paper they wrote was to include a 'ghost' participant in the call or chat, but this has not been widely received by all, especially when considered that this would defeat the purpose of end-to-end encryption, apart from a whole host of technical challenges.^{729 730}

Encryption can be dealt with in two ways: either by brute force which would result in lawful intercept or by asking the owner of the device to hand over the encryption key or access code. The former method is an arduous task and could result in data being lost. While laptops can be intercepted using brute force, mobile phones usually employ a facility to wipe out the data when interception by brute force is applied.⁷³¹

⁷²⁵ Europol and Eurojust, 'Second report of the observatory function on encryption' (2020).

⁷²⁶ Maria Koomen, 'The Encryption Debate in the European Union' (2019) <https://carnegieendowment.org/files/WP_The_Encryption_Debate_in_the_EU.pdf> accessed 2 March 2021.

⁷²⁷ Dorothy E Denning, William E Baugh, 'Encryption and evolving technologies: Tools of organized crime and terrorism' (1997).

⁷²⁸ Ed Hagen, 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations' Computer Crime and Intellectual Property Section Criminal Division.

⁷²⁹ I. Levy; C. Robinson, 'Principles for a More Informed Exceptional Access Debate' (2019).

⁷³⁰ N. Cardozo, 'Give Up the Ghost: A Backdoor by Another Name, Just Security', (2019).

⁷³¹ *ibid* (n 657).

With regards to the latter method, most countries rely on general legal provisions, although some countries do have specific provisions on the matter. In the United Kingdom, for example, if the device is taken during a search warrant, the police have the legal right to examine the device, even if it means the device may be damaged or destroyed.⁷³² This is akin to the situation in Malta.

Under Section 397 of the Maltese Criminal Code, the court may ‘...order an inquest, search, experiment, the taking of any sample and any other measure or thing necessary for the fullest investigation of the case.’ Prima facie this would mean that the suspect, third party or even service provider may be requested to produce the encrypted data or access code. Should this take place voluntarily, under Maltese law, however, this request is not possible, despite the fact that there is no legislation regulating the manner. The principle of *nemo tenetur*, however, is applied in such cases and the suspect cannot be requested to hand over such information if it would incriminate him.

This seems to be generally the situation in many countries around Europe, with only four EU Member States and the United Kingdom having specific legal provisions requiring the suspect to hand over such information.

In Malta, it is common practice to take fingerprints, under Section 397 of the Maltese Criminal Code, although the law is silent on them being used for opening devices. As far as this author is aware, there is no local case law on the subject if a suspect’s fingerprints were used to open a device. The law, however, does provide that should the accused person be convicted, unless he was previously convicted of a crime, then the fingerprint impressions must be destroyed or handed over to the person acquitted.⁷³³

Furthermore, on the subject, one can refer to the European Court of Human Rights case of *Saunders vs UK* (2000)⁷³⁴ In this case, the ECtHR stated that ‘[the right to not self-incriminate] does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing’.⁷³⁵

After the murder of journalist Daphne Caruana Galizia in Malta, who was assassinated in a car bomb in October of 2017, the police went on to clone her mobile sim card, following the recovery of her mobile phone which was found destroyed at the scene of the crime.

⁷³² Criminal Code, Article 337G.

⁷³³ Criminal code, Article 397 (3).

⁷³⁴ [1996] *Saunders v. the United Kingdom*.

⁷³⁵ *ibid*, para 69.

Unfortunately, the case has not yet been concluded but details have emerged from the investigations. The details, however, are only from sources and cannot qualify as legal findings. Journalists have reported that her sim card was cloned with the help of mobile service providers, which provided assistance on the case. It was reported that while her messages, especially those on the WhatsApp platform were retrieved, since the messaging application is encrypted, the messages could not be seen.⁷³⁶

On 6 November 2020, the Council of the European Union put forward a Draft Resolution on Encryption which called for the Member States to provide access to encrypted messages as part of a criminal investigation into terrorism and organized crime. It also dealt with the issue of the non-consistent regulatory framework across the EU's Member States. This Draft Resolution also mentioned that a better balance is necessary to protect the fundamental rights which arise from encryption but also providing competent authorities with access to relevant data.⁷³⁷ This was not well received by certain NGOs like the Committee to Protect Journalists as it is also well known that journalists rely on encryption to protect their sources.⁷³⁸ Daphne Caruana Galizia herself used WhatsApp to communicate with her sources, making it very clear that such messages were encrypted and so it was safe to contact her in that manner.⁷³⁹

In contrast, in the same case of the murder of Daphne Caruana Galizia, the alleged criminals were instructed to use encrypted services like WhatsApp and Signal to communicate. It is not clear how Europol obtained this data, but an expert testified, according to reports, that data on the phone was extracted.⁷⁴⁰

It would appear then that while Malta has no specific legislation concerning encrypted personal messages to be decrypted and accessible, it seems standard practice to allow for the method of attacking such encryption through brute force. This has emerged from the ongoing case of the murder of Daphne Caruana Galizia. In this same tone, would it be possible to apply the same technique to get into the journalist's phone thus reducing the safety net of many journalists around the globe? As to the other method of compelling the

⁷³⁶ Rachel Attard, 'Daphne's Murder: Laptop was not found at the Crime Scene – Source' (2017).

⁷³⁷ Council of Europe, 'Draft Resolution on Encryption', (2020) 12143/1/20 Rev 1.

⁷³⁸ Committee to Protect Journalists, 'EU should withdraw draft resolution that threatens encryption', 10 November 2020, <
<https://cpj.org/2020/11/eu-should-withdraw-draft-resolution-that-threatens-encryption/>> accessed 2 March 2021.

⁷³⁹ Daphne Caruana Galizia, 'Former and current employees of the Malta Financial Services Authority, the Financial Intelligence Analysis Unit, the police and other state authorities, and Pilatus Bank can contact me in full confidence on WhatsApp' <
<https://daphnecaruanagalizia.com/2017/04/former-current-employees-malta-financial-services-authority-financial-intelligence-analysis-unit-police-state-authorities-pilatus-bank-can-contact-full-confid/>> accessed 02 March 2021.

⁷⁴⁰ Edwina Brincat and Bertrand Borg, 'As it happened: Europol experts testify in Daphne murder case' (2020).

suspect to provide the decryption key, so far, in Malta, the *nemo tenetur* principle seems to be applied, although there is no case law on the matter.

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?

When determining whether or not a balance has been achieved in any area of law, it is always subject to interpretation depending on which party is being questioned. Throughout this chapter, focus will be placed on outlining the Human Rights which clash with the current AI framework. This focus will aid to determine whether or not Maltese law has reached an adequate balance between allowing digital advancements and protecting human rights online.

Malta's vision is to become the Ultimate AI launchpad.⁷⁴¹ For this to materialise and for developers to develop AI technology, the consumer needs to feel safe and protected using such technologies. Many AI applications process personal data and while this collection of data may lead to better governance and social knowledge, there is also the risk that without proper balance and security, countries can transform into 'surveillance states', falling prey to the extremes of 'surveillance capitalism'. Without a trustworthy framework, the work of developers can be hindered, even though laws should not, on the other hand, be too stringent as to inhibit AI developers from further progressing.⁷⁴²

One of the pillars for creating a trustworthy framework is the 'respect for all applicable laws and regulations, human rights and democratic values'.⁷⁴³ Even though ethical norms obviously vary from one Member State to another, Maltese law will base these ethical norms on the fundamental rights enshrined in the EU treaties and the EU Charter.⁷⁴⁴ The main Human Rights which need to be taken into consideration when dealing with AI are the respect for human dignity, right of privacy, freedom of the individual and equality and non-discrimination.

Through the latest amendments driven by Regulation 2016/679/EU, both data controllers and data processors are now under the obligation to keep a record of all processing activities performed on behalf of the controller, implement appropriate security measures to protect personal data, send notification to controller of data breaches in a timely manner and also adhere to a number of obligations to be included in data processing agreements. In the case of failure to comply with these obligations, the data controllers and data processors themselves shall be held liable, as stated in Article 30 of Chapter 586 of the

⁷⁴¹ 'Malta the Ultimate AI Launchpad; A Strategy and Vision for Artificial Intelligence in Malta 2030' (2019).

⁷⁴² 'Malta: Towards Trustworthy AI' Malta's Ethical AI Framework, (2019), 7.

⁷⁴³ *ibid.*

⁷⁴⁴ *ibid.*

Laws of Malta. The data subject has the right under Maltese Law to institute proceedings against the data processors or data controllers and if the latter are found liable of breaching data protection rules, they are personally responsible for damages, including moral damages.⁷⁴⁵

As previously mentioned, data processors, under the aforementioned Act have the duty to send notification to data controllers and subsequently, data controllers must report a data breach, no matter how small, to the Data Protection Commissioner within 72 hours of becoming aware of the breach. Data subjects affected must in turn be notified of this breach, however, this act of notifying is only compulsory when the data breach imposes a high risk to the rights and freedoms of the data subjects.

Through the amended requirements of the GDPR, there has also been a steep increase of stricter consent requirements. Consent now has to be given by a clear affirmative action, and inactivity will not result in tacit consent, rather, it would amount to invalid consent. Also, the data subject may at any point withdraw their consent and this process of withdrawal should be ‘as easy as to give consent’. Just like in all contracts, in order for an individual to give consent, they must know what they are consenting to and because of this, the GDPR has enhanced focus on transparency of the data collected. Controllers are obliged to process personal data legally, transparently, and fairly and also in a minimalistic manner, meaning that data controllers should only process data where necessary. Whether they have done so will be assessed through the imposition of the legal obligation to carry out a data protection impact assessment.

The GDPR also provided the data subject with stronger rights than ever before, such as the ‘right to be forgotten’ when data is no longer necessary, the right to ‘data portability’ where the data subject has the right to receive a copy of his personal data, the ‘right of access’, data restriction as well as objection to processing.⁷⁴⁶

Through this brief analysis of the EU GDPR, which being an EU regulation, is directly applicable into Maltese law, and the Maltese Data Protection Act as well as subsidiary legislation, it is clear that there is a great number of safeguards of human rights protection awarded to the data subjects. Regarding the issue of whether Maltese law has achieved an adequate balance between allowing digital advancements and protecting human rights online, this still remains to a certain extent subjective. For instance, if one were to ask a data subject whether he feels properly safeguarded by the provisions in place, one might opine that even though protection is awarded, additional safeguards should be in place.

⁷⁴⁵ *ibid* (30).

⁷⁴⁶ *ibid*.

By way of example, as previously outlined, the GDPR requires that the data subject should be informed only when a data protection breach imposes a high risk to the rights and freedoms of the data subjects. The data subject may complain that they should always be notified, even when the breach is low risk. Also, when reflecting on whether the GDPR and Maltese law hinder innovation in this sphere, it does not appear to do so, as developers can still continue to do so as long as they do so according to the provisions listed above.

However, even though this issue of balance is of a subjective nature, it is evident that the EU, and in turn EU Member States, such as Malta, have come a long way in ensuring human rights protection in the online sphere.

10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the coming 5 years? Incorporate the answers, you have given to the previous questions, and the main results of your research.

In the majority of AI sectors, such as automated cars, the law tends to adopt a responsive approach whereby legislation is drafted to address an issue which already exists, rather than a potential issue. Because of this ‘response mechanism’, the law is amended to address gaps in legislation, and not to anticipate potential problems.

As previously mentioned, Malta aims to become the ‘Ultimate AI Launchpad’⁷⁴⁷. The Malta AI strategy team has dedicated its energy to developing a national strategy founded on three distinct and important notions: investment, innovation and adoption of AI, as well as various enablers that provide a support system that would protect this industry and those individuals impacted by its operation as well as providing the means to allow it to thrive. The three aforementioned pillars showcase Malta’s desire to present itself as a hub for the AI sector indicating its progressive disposition. The enablers, on the other hand, identify Malta’s understanding that progress within this sector is a balancing act and that the data fed to AI technology to improve its operating system must be done in such a way that it protects individuals. These enablers constitute an integral part of the strategy’s focus and refer to legal means through which the AI industry is regulated, ensuring that this activity remains ethical and rigorously monitored, as well as providing the infrastructure and education necessary to support its development. These provisions are a vital element as, together with EU directives, they provide a structure that emphasises and ensures the protection of fundamental human rights in the areas AI technology functions.

Through the Maltese ethical framework, ‘Malta: Towards Trustworthy AI’, provisions have been outlined that dictate that AI as a presence ought not to cause harm to human beings

⁷⁴⁷ *ibid.*

at any stage of their lifecycle and are able to develop and operate only if the systems are fair and understandable. This strategy is built on a human-centric approach and is thus regulated to ensure it operates for the good of society and doesn't become a destabilising force. This goal which is strived for by the Maltese government is supported and realised through four fundamental pillars: firstly, AI ought to function in such a way that it 'preserves the dignity, autonomy and self-determination of an impacted individual'. Secondly, the advancement of AI technology must occur with the mentality that 'man operates the machine'. This is firmly established as the notions of liability, responsibility and accountability are of immense interest and importance within this sector. Moreover, AI development ought to be inclusive to 'facilitate greater benefits for society' and ought to be 'designed and deployed in a manner that is equitable and prevents bias.' Therefore, with regards to Maltese legislation in the coming years, it is likely to be based on the abovementioned pillars.

However, as seen throughout this national report, the larger part of Maltese law related to this area of law has been transposed by EU instruments, and in the next five years, amendments in Maltese legislation are also most likely to be the result of amendments at EU level. In the recent study titled 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' conducted by the Panel for the Future of Science and Technology to the European Parliament, the relationship between the GDPR and AI is analysed and suggestions are put forward.⁷⁴⁸

The final considerations of the said report outline that the current GDPR does not appear to require major changes as it adequately protects data subject, and does not place EU companies at a disadvantage when compared to third-country competitors. That being said, some suggestions for minor changes mainly related to guidance are put forward. This includes adequate guidance on how AI may be applied consistently with GDPR, and on available technologies for doing so. The reason behind this need for guidance is to improve compliance and available technologies will lower costs for the EU companies.

This report also puts focus on the broader scheme relating to social impacts of mass processing rather than the individual data subject. The GDPR, as seen throughout, protects the individuals, however, it is suggested that a helpful exercise would be to examine which AI applications are socially acceptable, which will result in more security of fairness as well as protection of the fundamental right of equality and non-discrimination. Since Malta is currently working on becoming the 'Ultimate AI Launchpad', this exercise would be helpful.

⁷⁴⁸ 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' conducted by the Panel for the Future of Science and Technology to the European Parliament (2020).

The Report also makes reference to the autonomous nature of AI. Article 22 of the current GDPR presents derogations that allow fully automated decision making, however, as stated in the above mentioned report, there is the need for guidance relating to profiling and automated decision making to truly allow the full potential of AI technologies. The report states that: ‘an obligation of reasonableness – including normative and reliability aspects – should be imposed on controllers engaging in profiling, mostly, but not only when profiling is aimed at automated decision-making.’ It is also stated that with regards to the individual explanations required by the GDPR for automated decision making, this should only be required to the extent that this is possible according to the adopted AI technology and reasonable according to costs and benefits. The explanations may be high-level, but they should still enable users to contest detrimental outcomes.

As can be analysed through the suggestions put forward in the latter Report, what is expected in the coming years at Union Level in relation to the GDPR is a ‘gap filling’ of the current legislation. It appears that GDPR will not be subject to any drastic amendments, but rather, subject to additional guidelines on the ‘gaps’ that currently exist. If the suggestions discussed formerly are transposed into the GDPR, being an EU Regulation, it will be directly applicable to Maltese Law.

Conclusion

As can be regarded through the formation and continuous work of Malta’s recently launched AI strategy team, it is evident that our country is looking to the future, recognising the importance of AI while understanding that for it to be of the most benefit to citizens, it must be regulated in such a way that it respects the rights of those whom it affects. The steadily increasing widespread reach of AI can be noted in all sectors which is why it is important that protections must be complied to preserve and respect the rights and dignity of all individuals.

It is undeniable that the desire to develop and advance AI technology and the need to protect human rights, such as and most importantly privacy, are contradictory wants. They are limiting factors on one another and the relationship between the two often begs the question whether or not a mutually beneficial balance can be reached between them. This is a highly subjective notion resulting in there being no definitive answer as to whether or not a country has been able to attain this goal. As has been noted, in order for AI to function and perform as intended, it requires extensive amounts of data to process. This enables the machinery to be trained to analyse information and recognise trends and associations within given data in a much faster and more accurate manner than man is able to.

However, there exist multiple issues, such as that of bias as the results produced by this technology are only as thorough as the data it's being fed. Additionally, we are able to identify data protection as another major problem that arises, whereby AI's use of consumer data must be used in conjunction with literature prescribed by EU regulations. An example is the provision of the GDPR which lays down that the secondary use of data is prohibited, meaning data can only be used for a single declared purpose. This is a clear illustration of how, through regulation, the value of an AI system is limited.

While some may regard the various measures in place as being too restrictive, viewing them primarily as an instrument to curtail the improvement of AI, it is imperative that people are protected and feel secure with this technology that is steadily permeating more aspects of our daily lives. Human freedom is given primacy within the strategies outlined in the Maltese ethical framework 'Malta: Towards Trustworthy AI', indicating the country's commitment to attempting to find the balance between development that doesn't impinge on humankind but rather protects their rights and freedoms.

AI is the future. This is a fact that has become increasingly evident over the course of the last century through the incredible developments that have taken place, irrevocably changing the manner in which the world operates. Therefore, Malta's strategy regarding this technology and the means through which it ought to operate with regards to human rights concerns is fundamental and essential to the advancement of the country. As a framework, it falls in line with the thinking that sophistication of AI machinery is highly desirable, but as we are able to note from the measures outlined, this sophistication cannot come through the exploitation of the data of individuals, nor at the expense of their fundamental rights.

Table of Legislation

Title of the Legal Act	Provision text in English language
General Data Protection Regulation (GDPR) Article 4 (1)	1. ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Protection Act, Chapter 586 of The Laws of Malta - Article 2.	2. This Act implements and further specifies the relevant provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data’.
Data Protection Act, Chapter 586 of The Laws of Malta - Article 4.	4. The provisions of this Act shall apply to the processing of personal data, wholly or partly, by automated means and to such processing other than by automated means where such personal data forms part of a filing system or is

	intended to form part of a filing system.’
Data Protection Act, Chapter 586 of The Laws of Malta - Article 30 (1)	(1) Without prejudice to any other remedy available to him, including the right to lodge a complaint with the Commissioner, a data subject may, where he believes that his rights under the Regulation or this Act have been infringed as a result of the processing of his personal data in contravention of the provisions of the Regulation or this Act, by sworn application filed before the First Hall of the Civil Court, institute an action for an effective judicial remedy against the controller or processor concerned.
Data Protection Act, Chapter 586 of The Laws of Malta - Article 26 (2)	(2) An appeal to the Tribunal may be made on any of the following grounds:(a) that a material error as to the facts has been made;(b) that there was a material procedural error;(c) that an error of law has been made;(d) that there was some material illegality, including unreasonableness or lack of proportionality.

Bibliography

Legislation

European Charter on Human Rights

Constitution of Malta 1964

European Convention Act 1987

General Data Protection Regulation [2016] OJ 2 119/35

Consolidated version of the Treaty on the Functioning of the European Union 2012.

Administrative Justice Act

Data Protection Act 2018.

Criminal Code Chapter 9 of the Laws of Malta

Code of Organisation and Civil Procedure 1854

The Malta Digital Authority Act 2018, Act XXXI of 2018 of the Laws of Malta.

Innovative Technology Arrangements and Services Act, Chapter 592 of the Laws of Malta.

Regulation of Investigatory Powers Act 2000

Digital Resources

'A Brief Overview Of The EU General Data Protection Regulation (GDPR)' (Mamotcv.com, 2021) accessed 11 March 2021

'White Paper On Artificial Intelligence: A European Approach To Excellence And Trust' (European Commission - European Commission, 2021) 'A European Approach To AI 2020' (Medium, 2021) accessed 3 March 2021

'Understanding Malta's Artificial Intelligence Framework' (Times of Malta, 2019) 'The Toronto Declaration • Toronto Declaration' (Toronto Declaration, 2021) accessed 3 March 2021

Information and Data Protection Commissioner, 'Data Protection for Organisations: Guidelines' (idpc.org.mt), < <https://idpc.org.mt/for-organisations/guidelines/> > accessed 25 May 2021

'HSBC Fined €5,000 For Monitoring Employee'S Bank Account' (Times of Malta, 2021)
accessed 11 March 2021
https://edpb.europa.eu/news/national-news/2019/idpc-lands-authority-personal-data-breach_en

Mifsud I, Judicial Review Of Administrative Action In Malta

Yeung K, 'A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework', DGI (2019) 05

Zwitter A, and Boisse-Despiaux M, 'Blockchain For Humanitarian Action And Development Aid' (2018) 3 Journal of International Humanitarian Action

Blake E, 'Smart Contracts: Legal Regulation in a Decentralized Environment' (LL.B. thesis, University of Malta, 2019)

Tech.mt, < <https://tech.mt/technology-industry-malta/> > 01 March 2021

Emeka Chukwu and Lalit Garg, 'A systematic review of blockchain in healthcare: frameworks, prototypes and implementations' (2020 IEEE Access); Priscilla Mifsud Parker, 'A blockchain for the provision of healthcare' (Chetcuti Cauchi Advocates, 1 October 2019)
<<https://www.ccmalta.com/publications/ablockchain-for-the-provision-of-healthcare>> 1 March 2021

Malta Digital Innovative Authority, 2 March 2021

European Parliament, 'Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?' Scientific Foresight Unit (STOA) July 2019

Malta.AI, 'A strategy and vision for artificial intelligence in Malta 2030', October 2019

Europol and Eurojust, 'Second report of the observatory function on encryption' (18 February 2020)

Koomen M, 'The Encryption Debate in the European Union' (May 2019)
<https://carnegieendowment.org/files/WP_The_Encryption_Debate_in_the_EU.pdf> 2 March 2021

Dorothy E Denning, William E Baugh, 'Encryption and evolving technologies: Tools of organized crime and terrorism' (1997) 3 Trends Organ Crim 84

Hagen E, 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations' Computer Crime and Intellectual Property Section Criminal Division

Robinson L.C, Principles for a More Informed Exceptional Access Debate, Lawfare, 29/11/19, [online]
<https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate>

Parsons T, 'Is Schedule 7 of the Terrorism Act 2000 compatible with the European Convention on Human Rights' (Thesis for Law, Oxford Brooke University, 2016)

Attard R, 'Daphne's Murder: Laptop Was Not Found At The Crime Scene - Sources - The Malta Independent' (Independent.com.mt, 2021) accessed 11 March 2021

Committee to Protect Journalists, 'EU should withdraw draft resolution that threatens encryption', 10 November 2020, <
<https://cpj.org/2020/11/eu-should-withdraw-draft-resolution-that-threatensencryption/>>
2 March 2021

Caruana Galizia D, 'Former And Current Employees Of The Malta Financial Services Authority, The Financial Intelligence Analysis Unit, The Police And Other State Authorities, And Pilatus Bank Can Contact Me In Full Confidence On Whatsapp' accessed 11 March 2021

Brincat E, and Borg B, 'As It Happened: Europol Experts Testify In Daphne Murder Case' (Times of Malta, 2021) accessed 11 March 2021

Case Law

Sanders vs UK (European Court of Human Rights) (2000)

[1972] John Lowell noe et v. Onor. Carmelo Caruana et (FH)

ELSA PORTUGAL

Contributors

National Coordinator

Nina Blakeway

National Researchers

Maria Carolina Nicolini

Bárbara da Rosa Lazarotto

Marta Lages Almeida

Natacha Alves

Luisa Matos

Francisco Lima

Beatriz Assunção Ribeiro

National Linguistic Editor

Inês Alves

National Technical Editor

Inês Henriques Fraga da Costa

Diogo Gambini Neves

National Academic Supervisor

Professora Paula Ribeiro Alves

Introduction

This report focuses on one of the most important subjects of the modern world: the impact of Advanced Digital Technologies on human rights. Advanced digital technologies and services bring with them extraordinary promise, but the emergence of these technologies has also been accompanied by rising public anxiety concerning their potentially damaging effects on human rights.

Society is facing, for a few years already, an age of fierce developments in all fronts when we talk about Artificial Intelligence (AI), which has been changing and affecting our life in general – for both good and bad -, as well as our personal, and public relations. Globalisation, highly impulsed by the technologies and the utopia of a connected online world, has been extinguishing frontiers, namely geographic and legal ones, which can represent a huge advantage; but it also has a paradoxical effect, namely the dependency on the demanding of digital life. This – as Aldous Huxley would say – Brave New World is changing our ways of communication and interaction with others, being our time, more than ever, dependent on AI, as well as other technologies, constantly appearing and changing our perspectives. This demands a fundamental and necessary reflection on the achievement of legislation - an improvement of legislation.

If, as we know, law origins are the human relations and the human interaction, and if they are, as we said, more than ever, so dependent on technologies, the way of law acts is highly challenged by the disruptive nature of AI, which – we can say – has already some years in advance of legislation capability, that is highly misfit, having in consideration the technological evolution. The so known and promised 4th Industrial Revolution, that even challenges the own idea of what we establish as human beings, can't be defined through only one set of technologies that can be extinguished in themselves, nor even a hegemony of an exact type of technology, resulting instead in a constant interaction between physical, virtual, biologic and juridic realities.

The huge and fierce technological developments have started a cultural extraordinary change, in which penal and procedural law are not an exception, in their juridic, epistemological and ethical ways, as we have the growing use of AI on court; fostering a debate on the opposition between the crescent use of digital proof and the guarantee of private life, foresaw as a human right through article 12 of the Universal Declaration of Human Rights (UDHR), which foresees that no one shall be subjected to arbitrary interference with his/her privacy. We can assume that, in one hand, the resource to technological and AI devices brings, besides what we established before, undeniable advantages to procedural law, for example when we talk about saving time and charges; in

the other hand, it comes to show and polarize the differences between social classes, already economically separated, and challenging the procedure fundamental rights

The right to the protection of personal data has been enshrined in the Portuguese Constitution since 1976 in its article 35, framing it in the set of 'rights, freedoms and guarantees', being, in this sense, a matter of extreme importance.

Throughout this report, it is possible to understand how human rights associated with technologies are protected at national level through legislation and their framework at an international and European level.

It is presented to what extent the private sector has freedom in the application of these subjects and its cooperation with the public sector. A study of the process of guaranteeing these rights through judicial means and the judicial process of breaches of data protection and an analysis of how the dissemination of platforms and social networks spread discrimination is made, combining its treatment in Portugal and to which extent there are specific laws for these advanced digital technologies and the need for encrypted personal messages to be decrypted and accessible for criminal investigations.

There is also an analysis of the behaviour of Portugal, specifically whether or not a balance has already been reached between allowing digital advances and the conservation and protection of human rights, concluding this report with a view on the development of Portuguese legislation in the next half decade.

1. Which human rights issues do Advanced Digital Technologies pose in your country?

When the matter is human rights in the digital age and the challenges that this intersection presents, it can be noted that Portugal has been searching for ways to adapt to this new reality. Portugal already highlights the importance of having a regulation about the rights, freedoms, and guarantees that are threatened in the virtual scenario. It can be highlighted as the main points of concern, which has been prioritized by its regulation, issues such as data protection, the right and access to the digital environment and protection against misinformation, in order to protect society against natural or legal persons, who produce, reproduce or disseminate a narrative considered to be disinformation. The Portuguese State has been concerned with supporting the creation of fact-checking structures by duly registered media and encourages the attribution of quality seals by trustworthy entities endowed with the status of public utility.

The right to be forgotten, cybersecurity, the right to privacy in a digital environment and the regulation of the use of artificial intelligence, in which attention must be paid to non-discrimination and tolerance, are also gaining more and more notoriety in the Portuguese scenario. In addition, the Portuguese law does not overlook issues concerning

the right to protection from abusive geolocation, in the way that the use of the data of the geographical position of a user's equipment should only be done with the user's consent or legal authorization.

Seeking to anticipate future demands, the Portuguese State also wants to provide for the right to a digital will, in which all people would be able to express their will in advance with regard to the provision of their contents and personal data, namely those contained in their profiles and personal accounts on digital platforms, under the terms of the contractual conditions for the provision of the service and the applicable legislation, including the testamentary capacity.

In this way, Portugal has been showing concern in keeping the national and European agenda aligned in the joint commitment to the ethical dimension in the digital age. A concern for the contribution to a digital transition model that strengthens the human dimension in the digital ecosystem is perceived.

1.1. Is there or what is a legal framework that provides for procedures on human rights impact assessments?

By dealing with the legislation that protects human rights in the scope of technology, since they are rights that aim to protect the human being, it is necessary to focus the discussion on article 35 of the Constitution of the Portuguese Republic of 1976. This article enshrines the protection of citizens against the processing of computerised personal data, as well as highlights that the use of data processing is prohibited in some specific cases, where it could even be a threat to human rights. Besides this, it also guarantees minimum guidelines with which the data should be treated.

Indeed, the Portuguese legal regime for the protection of personal data is consecrated, in general terms, in Law no. 67/98, from the 26th of October, the Law on the Protection of Personal Data, which resulted from the transposition of Directive no. 95/46/EC and which was revoked due to the application of the GDPR. There is also the Law no. 58/2019, from the 8th of August, which ensures the implementation, in the national legal order, of Regulation (EU) 2016/679 of the Parliament and of the Council, from the 27th of April, on the protection of individuals with regard to the processing of personal data and the free movement of such data. However, it should be noted that given the Deliberation (2019/494) of the Portuguese National Data Commission on the poor transposition of some articles of the GDPR into the law, some articles should not be applied due to their poor transposition. In such cases, the use of the provisions of the GDPR is determined.

However, one cannot forget the existence of specific legislation for certain areas, such as the law that regulates the processing of personal data in the context of publicly available

electronic communications networks and services, Law no. 41/2004, from the 18 August, amended by Law no. 46/2012, from the 29 August.

In addition, the Portuguese Charter of Human Rights in the digital age should be highlighted⁷⁴⁹. It is referred to in its 21 articles issues such as the digital living will, the right to be forgotten, fake news, quality seals, artificial intelligence and social network tariffs. Such articles were presented in order to promote human rights and fundamental freedoms, the rule of law and democratic principles in the digital world, seeking to allow a fair, transparent, sustainable, innovative, and a safe and competitive environment. This law is also based on the communication 'Digital Compass 2030: the European Road to the Digital Decade', presented by the European Commission in March 2021, and on the 'Berlin Declaration on Digital Society and Value-Based Digital Governance', launched by the German presidency of the EU Council in December 2020.

1.2. What are other instruments used for identifying human rights issues posed by ADT?

In 2017, the Portuguese government proposed the 'e.2030 Digital Skills National Initiative, with the Portuguese acronym determined as Portugal INcoDe.2030'. This would be an integrated public policy program that focuses on promoting digital skills. This proposal also seeks to fulfill the human rights provided for by the International Convention on economic, social and cultural rights, which are listed as the right to work in fair and favorable conditions, the right to social protection, an adequate standard of living and the highest attainable standards of physical and mental well-being and the right to education and to enjoy the benefits of cultural freedom and scientific progress.

Thus, the programme presented by Portugal has a set of actions that is structured in five axes determined as inclusion, education, qualification, specialisation and research. Such actions then seek to meet three challenges that are set by the Portuguese government. The challenges are listed as how to guarantee digital literacy and inclusion for the full exercise of citizenship, stimulate specialisation in digital technologies and applications for job qualification, an economy with greater added value and produce new knowledge in international cooperation.

Such positioning points out that the issue of digital inclusion is a social issue. The aim is letting people who have never benefited from being able to have a mobile phone connected to the internet, use a social network, be able to see others at a distance and talk to them using a wifi network, probably even for free. These goals were also pointed out by the Minister for the Presidency and Administrative Modernisation of Portugal - Maria Manuel Leitão Marques.

⁷⁴⁹ ASSEMBLEIA DA REPÚBLICA PORTUGUESA. Lei n.º 27/2021. Diário da República n.º 95/2021, Série I de 2021-05-17. Access at <https://dre.pt/web/guest/home/-/dre/163442504/details/maximized>.

1.3. What national and international standards of human rights protection are at risk due to the ADT development and implementation?

The future is not foreseen, but predictions are never far from reality. One thing we take for granted is that the future will come, and its form and content will be less and less unknown. There is not necessarily the question of choosing between human rights and technology, as technology can be used in favor of human rights.

However, it can be seen from the European Parliament's report on human rights and technology that there has been concern about that relationship for some time.⁷⁵⁰ In the document, the protection that must exist before the right to privacy and freedom of expression is highlighted. The report also reaffirms that EU standards, namely the EU Charter of Fundamental Rights, must prevail in the assessment of incidents involving the use of dual-use technologies in a way that could limit human rights.⁷⁵¹

It should also be noted what was appointed by a group of experts determined by the European Commission, which presented documents containing ethical guidelines for reliable artificial intelligence.⁷⁵² When analysing the documents, we can see that the group focused on the areas they considered to be the most at risk from the use of artificial intelligence. This action is part of the AI strategy announced by the European Commission, with the aim of building trust in human-centric AI.

Based on fundamental rights and ethical principles, the guidelines list seven key requirements that AI systems should meet in order to be trustworthy. Such requirements are determined as: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being and accountability.

In addition, the rights to private life and associated freedoms are considered fundamental human rights. This concept is the basis of EU data protection laws. Functionally, international human rights law is based on agreements between countries to promote and protect human rights at international, regional and domestic levels, such as the Universal Declaration of Human Rights (UDHR).

⁷⁵⁰ M Schaake, 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries' (Report, 2014/2232(INI), 3 June 2015); adopted as the European Parliament Resolution of 8 September 201
<https://www.europarl.europa.eu/doceo/document/TA-8-2015-0288_PT.html> accessed on the 16th of February 2021.

⁷⁵¹ *ibid*, para 39.

⁷⁵² European Commission, High-Level Expert Group on Artificial Intelligence (AI HLEG), "The Ethics Guidelines for Trustworthy Artificial Intelligence (AI)" (2018)
<<https://ec.europa.eu/futurium/en/ai-alliance-consultation>> accessed on the 16 February 2021.

The UDHR contains specific provisions related to the right to private and family life and freedom of expression. The principles enshrined in the Declaration provided the basis for European data protection laws and standards. The right to private life and associated freedoms are contained in article 12 of the UDHR.

2. How is personal information protected in your national legislation?

2.1. How is personal information defined by your national legislation (or by a legal framework that affects your national legislation, e.g. GDPR)?

On the 25th of May 2018, the GDPR - Regulation (EU) 2016/679 - entered into force in the European Union, and consequently, in Portugal. The main objectives of the GDPR were to regulate the processing of personal data of natural persons, establish rules regarding the free movement of personal data and create fundamental rights and freedoms of natural persons relating to their data.

Portugal is a Member State of the European Union, therefore being subjected to binding legislative acts taken by the latter within its competencies, such as Regulations. This way, the legal framework in force is the GDPR.

Personal information is defined by the GDPR in article 4 which says that personal data is 'any information related to an identified or identifiable natural person'. It can be a name, an identification number, location data, or any genetic, physical, psychological, genetic, mental, economic, cultural, or social identity data related to a person.

The National Portuguese legislation, Law n.º 58/2019 does not provide us new definitions, instead just regulates the application of the Regulation (EU) 2016/679.

2.2. If your country is a Member State of the European Union, please provide a concise analysis of the extent to which your country's laws regarding protection of personal information are compatible with EU law, particularly the General Data Protection Regulation (GDPR).

The Portuguese Constitution dates from 1976 and protects personal data as one of the fundamental rights in article 35. This article protects the right to access personal data, correct it and update it, and also protects the consent of the owner of the data so it can be used in several situations such as political parties and religious affiliations.

Regarding incompatibilities, there are some yet to be addressed. When the GDPR was introduced, Portugal approved Law n.º 58/2019 which regulates the compatibility and the application of the GDPR within the Portuguese legislative system. This law repealed the current Data Protection Law and made a series of alterations to it, creating the National Data Protection Commission. In fact the Commission already existed since 1994, but it was not adapted to the GDPR. However, there were a few points that were not covered by

this law. At first glance, one may think that there is an incompatibility between the GDPR and the Portuguese Civil Code regarding minimum age. According to Article 130 of the Civil Code, a person is considered an adult and is able to give consent relating to its civil responsibilities at eighteen years old. On the other side, Article 8, n.º 1 of the GDPR provides that a child can give consent relating to personal data at sixteen years old, and gives Member States the possibility to decide by law a lower age, as long as this age is not under thirteen years old. However, in accordance with article 16, n.º 1 of Law n.º 58/2019, children can only give consent regarding their data when they reach thirteen years old. This way we can infer that the Civil Code is not applicable at this matter and therefore there is no incompatibility.

Another incompatibility is within articles 20 and 21 of the Portuguese Labour Code, which permits the use of video vigilance of workplaces, even though article 19, No 2, d) of Law n.º 58/2019 determines that video vigilance is prohibited in areas regarding workers, and demand the authorisation of the National Data Protection Commission, which was not granted.

The use of personal data by health insurance is also another point that must be analysed. According to article 9 of the GDPR, health insurance contracts are not enough for the processing of certain health data, where consent is needed. At the same time, Member States need to adapt the GDPR by qualifying the health insurance activity as public interest. The main point is that Portuguese Law No. 58/2019 which regulates the application of the GDPR in Portugal just established other conditions related to the activity of health insurance and failed to give the public interest status to them. This way, the current situation is that consent is needed to process certain health data, therefore the contracts which do not have this consent may be invalid.⁷⁵³

2.3. How do external instruments (such as the abovementioned GDPR) influence the data protection in your country?

The GDPR had a big influence on data protection in Portugal, since Law No. 58/2019 imposed a series of actions so internal legislation was adapted to the Regulation. One of the main influences was the changes on the National Data Protection Commission competencies: the Commission now controls compliance with the GDPR and national regulation laws; also, they can ask for information, documents, and data from companies, emitting opinions, reports, and regulations regarding the matter.

⁷⁵³ Joana Mota and Alexandre Pedral sampaio, 'Regulamento Geral de Proteção de Dados em Portugal – alguns apontamentos à sua lei de execução' [2019] 578-956X(53) Actualidad Jurídica Uría Menéndez 142-148.

3. To which extent is the data protection self-regulated by the private sector in your country?

Portugal has national constitutional privacy and data protection provisions, as article 35 of the Portuguese Constitution. This article protects the right to access personal data, correct it and update it, and it also protects the consent of the owner of the data so it can be used in several situations such as political parties and religious affiliations. Thus, it is safe to say that the GDPR is compatible with the Portuguese Constitution.

As previously stated, in 2018 the General Data Protection Regulation (EU) 2016/679 entered into force in the European Union and, consequently, became applicable in Portugal through the Portuguese Law 58/2019 (The Data Protection Law).

The National Data Protection Commission (NDPC) is an independent administrative entity, with legal personality under public law and with powers of authority, endowed with administrative and financial autonomy, which works with the Assembly of the Republic.

The NDPC controls and inspects compliance with the GDPR, Law no. 58/2019, Law no. 59/2019 and Law no. 41/2004, as well as other legal and regulatory provisions on the protection of personal data, in order to defend the rights, freedoms and guarantees of people when processing their personal data.⁷⁵⁴

NDPC has not issued general guidelines on the protection of personal data. However, it has issued some opinions on the processing of personal data in very specific contexts such as health and telecommunications.

Comparing articles 12 and 13 of Law no. 58/2019, in the private sector there is no obligation to designate data protection officers as in the public sector, except under the conditions of article 13, a) and b).

Regarding the public sector, there are some restrictions and measures regarding data protection:

- Article 23, which refers to the processing of personal data by public entities for purposes other than those determined and which was later unenforced by the Deliberation no. 2019/494 of the NDPC;
- Article 27 on the publication of data in the context of public hiring;
- Article 58, that states that the technical guidelines for the direct and indirect administration of the State are approved by resolution of the Council of Ministers, which can also recommend its application to the State's business sector.

⁷⁵⁴ <<https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/>>.

Therefore, the Resolution of the Council of Ministers no. 41/2018 came to define technical guidelines for the Public Administration in terms of security architecture of networks and information systems related to personal data.

In this way, the private sector enjoys a certain degree of self-regulation and is not subject to as many requirements and measures as the public sector. Nevertheless, there are some regulations in the matter of protection of personal data and privacy in telecommunications (Law no. 41/2004, of the 18th of August) and personal genetic information and health information (Law no. 12/2005, of the 26th of January).

Thus, the system applied arising from Law No. 58/2019 is self-regulating, in which companies and organisations make decisions regarding data processing, with due exceptions previously expressed.⁷⁵⁵

3.1. How do public and private sectors cooperate in this regard?

According to article 8, no. 1 of the Law no. 58/2019, public and private entities must provide their collaboration to NDPC, providing it with all the information requested, in the exercise of its powers.

According to article 8, no. 1 of the Law no. 58/2019, public and private entities must provide their collaboration to NDPC, providing it with all the information requested, in the exercise of its powers.

In addition, 60% of the fines imposed on sanctions related to data protection violations revert to the State and 40% to NDPC, according to article 42 of the Law no. 58/2019.

Due to the Covid-19 pandemic that devastated the world, the Portuguese government drew up a list of recommendations to prevent and control the pandemic, one of which was the controversial installation of the STAYWAY Covid application.

STAYWAY Covid is an application for iOS or Android phones that allows access to location, so that each person who installs it is informed about risk exposures to the disease, by monitoring recent contacts.⁷⁵⁶

This application was developed through a collaboration between a public entity (ISPUP - Public Health and Epidemiology) and private entities (INESC TEC; Keyruptive Technologies and Ubirider), which results from an initiative, carried out under the INCoDe.2030 programme - E.2030 National Digital Skills Initiative, which materialises a

⁷⁵⁵ João Maltez and Filomena Lança, 'Revolução nos dados pessoais está a passar ao lado das PME' [2018] *Jornal de Negócios*

<https://www.telles.pt/xms/files/migrated/Manuais_1/JNeg_GPF_Revolucao-nos-dados-pessoais-esta-a-passar-ao-lado-das-PME_Jan-2018.pdf>

⁷⁵⁶ <<https://stayawaycovid.pt/>>.

strategy for the country's digital development, within the scope of the National Reform Programme initiated by the XXI Constitutional Government and is aligned with the initiative 'Industry 4.0 - National Strategy for the Digitisation of the Economy'.⁷⁵⁷

To regulate the data obtained by users when using this application, the Government manifested itself through Decree-Law no. 52/2020 of the 11th of August, establishing the General-Direction for Health as the entity responsible for processing the app STAYWAY Covid.⁷⁵⁸

The decree-law comes after the National Data Protection Commission (NDPC) determined, in the impact assessment of the app, that it needed a legal framework, in accordance with point no. 93 of the NDPC Deliberation 2020/277. In point no. 94 of the Deliberation in question, NDPC reinforces the voluntary nature of the use of the application by the user.

In article 2 no. 1 of decree-law no. 52/2020, the application '(...) STAYWAY Covid must respect the national and European legislation applicable to data protection, namely Regulation (EU) 2016/679, of the European Parliament and of the Council, of the 27th of April, 2016, Law no. 58/2019, of the 8th of August, and other applicable legislation'.

Thus, through the recommendation of the European Commission that the development and use of mobile applications for notification of individual exposure to risk factors resulting from contact with COVID-19 patients appears important, as 'they can play an important role in the strategy of survey of containment measures, provided that under the responsibility of a health authority, through the exclusive intervention of a doctor and once the protection of personal data, security and privacy is guaranteed',⁷⁵⁹ public and private entities in Portugal worked together and developed an application respecting the rights of its users.

4. What is the process of judicial review of cases of data protection breaches?

4.1. Is the right to data privacy defined in your legal system? If not, is it a part of another right protected by the national law?

In general, the right to privacy is stated in article 26, no. 1 of the Portuguese Constitution and also through article 34, which determines the inviolability of home and

⁷⁵⁷ INCoDe.2030, 'Portugal no contexto europeu: metas a atingir' <<https://www.incode2030.gov.pt/metast>>.

⁷⁵⁸ Karla Pequeno and Filomena Lança, 'DGS responsável pelos dados da app StayAway Covid, que será lançada este mês' [2020] Público <<https://www.publico.pt/2020/07/16/tecnologia/noticia/dgs-responsavel-dados-app-stayaway-covid-sera-lancada-mes-1924720>>.

⁷⁵⁹ Decreto-lei do *Conselho de Ministros* nº52/2020 from 11 August. *Diário da República* n.º 155/2020, Série I.

correspondence. In specific, and before transposing the General Data Protection Regulation (henceforth GDPR), Portugal had five main legal instruments regarding data privacy:

- _ Law no. 67/98 (Law of Data Protection), from the 26th of October, which in turn was originated by the transposition of the Directive no. 95/46/CE, from the European Parliament;
- _ Law Decree no. 131/2014, from the 29th of August, which concerns specifically the protection of sensitive medical data, including genetic data, namely for research purposes;
- _ Law no. 43/2004, from the 18th of August, which relates to the organisation and functioning of the National Data Protection Commission (which is an independent administrative entity in Portugal);
- _ Law no. 1/2005, from the 10th of January, which regulated video surveillance; and
- _ Law no. 5/2004, from the 10th of February, regarding electronic communications, which transposed the Directives no. 2002/19/CE, 2002/20/CE and 2002/21/CE.

Portugal also protected the right to privacy, although with a very limited scope, through Law no. 21/2014, related to clinical research, which guarantees a minimum of protection of the personal data used in medical trials, as well as to its participants.

In this sense, the right to data privacy has been protected in Portugal for more than twenty years, notwithstanding the lack of enforcement and resources of the National Data Protection Commission⁷⁶⁰ (hereafter NDPC), leaving the right to data privacy in a weakened and often forgotten state.

With GDPR's legislative modifications, and consequently with the implementation of Law no. 58/2019, from the 8th of August, on one hand, the previous Law of Data Protection was revoked, and on the other, the Law that regulated the organisation and functioning of the NDPC suffered significant modifications. The other above-mentioned instruments remain in force up to this day.

These legislative changes contributed notably to the protection of the right to data privacy, not only because they allowed public debate to take place and raised awareness about data protection, but also because they provided densification and concretisation of the several elements that compose the right to privacy. This, in turn, allowed national doctrine to prosper and courts to make better decisions on the matter. In addition, since accountability and the fines stipulated increased considerably, companies in general were forced to seek

⁷⁶⁰ NDPC Activity Report [2017-2018], pp. 13, 30, 33-35.

advice from data protection legal counsellors and lawyers, in order to measure the risk of data protection breaches and implement internal procedures to avoid such breaches.

In this sense, although there is still a long way to go in terms of enforcement, the right to data privacy is, in general, duly defined and established in Portugal, in the terms prescribed by the GDPR.

Nevertheless, through Deliberation 2019/494, NDPC clearly stated that the following articles of the implementation Law, among others, wouldn't be enforced due to the fact that they appear to be, in their opinion, contrary to the GDPR and beyond the margin of legislation conferred to the states:

- _ Article 21, which determines the possibility of restriction of information and access rights in the case of a duty of secrecy incumbent upon the controller;
- _ Article 23, which concerns the processing of personal data by public entities and the possibility of transfer between public entities for purposes other than those for which the data were collected;
- _ Article 28, no. 3, a), which states that the worker's consent is not a requirement for the legitimacy of the processing of his/her data if the processing produces a legal or economic advantage for the worker;
- _ Articles 37 and 39, which concern fines in case of infringement of the GDPR. NDPC argues that the fines imposed by the implementation Law are beyond the margin of legislation conferred to the states.

4.2. Can the data subject restrict or object the data processing? What are the circumstances and exceptions to this option?

A European Regulation is mandatory and has direct application in all Member States (article 288 of the Treaty on the Functioning of the European Union). In this sense, as far as the GDPR prescribes the possibility of the data subject to object or restrict data processing, so does National Legislation.

Accordingly, the data subject can object to data processing at any given moment, as stated in article 21 of the GDPR.

When it comes to restricting the data processing, data subjects are entitled to do so, if one of the following conditions is met (article 18 of GDPR):

- _ The accuracy of the personal data is contested by the data subject;
- _ The processing is unlawful, and the data subject opposes the erasure of the personal data (so he can request the restriction of the use instead);
- _ The controller no longer needs the personal data for processing, but the data is required by the data subject for the establishment, exercise, or defence of legal claims;

— The data subject has objected to processing under article 21, no. 1, while the verification of whether the legitimate grounds of the controller override those of the data subject is pending.

Article 23 of the GDPR allowed Member States to legislate exceptions to the objection or restriction to data processing by the data subject, in specific, provided that those exceptions respected fundamental rights and freedoms, as long as they were necessary and proportionate, to safeguard other important values, namely national and/or public security. Portugal, however, has not specified this matter beyond what is stated in the GDPR.

It is also important to mention the right of rectification (article 16 of the GDPR) and erasure (article 17 of the GDPR), which are, inevitably, forms of limitation of the data processing, the latter in the sense that it puts an end to the data processing.

However, data erasure is limited by GDPR itself, in the sense that it is not applicable:

- For exercising the right of freedom of expression and information;
- For compliance with a legal obligation which requires processing to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- For reasons of public interest in the area of public health;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- For the establishment, exercise, or defence of legal claims.

In addition to the above mentioned, the Law no. 58/2019 also reflects these exceptions.

In this sense, the exception of the legal conservation period is stated in article 21, no. 5 of the above-mentioned Law. Therefore, if a legal provision defines a legal conservation period, the data subject is not allowed to exercise its right of erasure. The second exception is described in article 24 and protects freedom of expression and information against erasure. The third concerns publication in official journals, stated in article 25. The last exception is stated in article 31, no. 2 and relates to public interest archives, scientific, or historic research or statistical purposes.

The NDPC was very critical about the scope of article 21, which states the exception of the legal conservation period, since, in its opinion, article 21, no. 3 provides a broad and unlawful justification for the controller to hold personal data for a non-limited period of time. In fact, the article determines that personal data can't be erased, even if requested by the data subject, if the data is still necessary to prove compliance with contractual obligations, while, at the same time, not specifying what contractual obligations means.

On the other hand, NDPC also strongly criticised the text of article 21, no. 5 which clearly indicates that the right to erasure can't be exercised if the legal conservation period is still running. In other words, according to the NDPC, no room is left for erasure even when requested on the grounds of unlawful processing or objection to the data processing for personal reasons, when there is no prevalent legitimate interest, as prescribed by the article 17 of GDPR.

4.3. In case of data protection breaches, what is the process to notify the data subject? Are there any exceptional grounds not to notify the data subject? If such grounds exist, what would be the ideal or optimal balance for necessity and proportionality?

According to article 34 of the GDPR, data breaches must be communicated to the data subject, without disproportionate delay, when it is likely to result in a high risk to the rights and freedoms of natural persons.

Portugal has not issued any specific legislation regarding this matter. However, by recommendation of the NDPC,⁷⁶¹ the Guidelines on personal data breach notification under Regulation 2016/679 from the European Data Protection Board (henceforth EDPB) are applicable. In this sense, the EDPB determines that, in case of data breach, the controller must provide the following information to the data subject: (1) a description of the nature of the breach, (2) the name and contact details of the data protection officer, (3) a description of the likely consequences of the breach and (4) a description of the measures taken by the controller to address the breach.⁷⁶²

It is also stated in the Guidelines that the controller must also provide specific advice to individuals on how to protect themselves from possible adverse consequences of the breach.⁷⁶³ Other recommendations include direct communication with data subjects, transparency, and effective communication, in the sense of using clear and plain language for the data subject to understand.

However, as prescribed in article 34 of the GDPR, this obligation only impedes on the controller if the breach presents a high risk to the rights and freedoms of natural persons. In other words, if we have a low-risk situation, the data subject does not have to be notified of the data breach. In addition, the EDPB Guidelines provide three conditions that, if met, result in the exemption of the obligation of informing data subjects in case of data breaches. Those conditions are the following:

⁷⁶¹ Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 [2017] OJ 2 119/1

⁷⁶² European Data Protection Board, 'Guidelines on Personal data breach notification under Regulation 2016/679' [2018] 20, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> accessed 25th February 2021.

⁷⁶³ *ibid.*

- _ If, prior to the breach, appropriate protective measures were applied (for instance, in order to display personal data unintelligible if accessed by an unauthorised person – namely encryption or tokenization);
- _ If, immediately after the breach, steps were taken to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise (for example, if the unauthorized person was identified and action was taken to ensure that said person won't be able to do anything with the data accessed);
- _ If contacting individuals would involve disproportionate effort. According to the EDPB's Guidelines, it is possible to find a balance between the necessity of notification and proportionality to the risk. For this assessment, elements such as the following must be weighted on the decision.⁷⁶⁴
 - _ Type of breach (for instance, disclosure of data to unauthorized parties vs. loss of data);
 - _ Nature, sensitivity, and volume of the data (in general, the more sensitive the data, the higher the risk of harm will be to the people affected);
 - _ Ease of identification of the individuals through the data;
- _ Severity of consequences for individuals (in the sense of taking into account the potential damages of illicit access and use of the data, such as fraud, physical harm, psychological distress, humiliation, or damage to reputation);
- _ Special characteristics of the individual (for instance, in the case of children or other category of vulnerable individuals);
- _ Special characteristics of the data controller (in relation to the type of data processed. For example, medical organisations have specific characteristics when compared to a mailing list of a newspaper);
- _ The number of affected individuals (generally, the higher the number of individuals affected, the greater the impact of a breach can have).

In conclusion, there are a number of elements that should be considered and analysed when globally assessing the need for notification of the data breach to the data subject, and a balance can be found among the combination of those elements.

5. Does the review constitute effective protection of data privacy?

5.1. Which bodies conduct such review?

The implementation of the Law no. 58/2019 attributed the judicial review of cases in the scope of data protection breaches to the Portuguese Administrative Courts. It was an interesting choice of the legislator as it constitutes a shift of jurisdiction from the Portuguese Court of Competition, Regulation, and Supervision (henceforth CCRS). In

⁷⁶⁴ *ibid*, 22-26.

fact, in the opinion issued by the NDPC concerning the legislative proposal that originated the implementation Law in Portugal⁷⁶⁵, the NDPC points out that, according to the Law of Judicial Organization [previous article 112, no. 1, g)], the appealation of NDPC's decisions was jurisdiction of the CCRS, a specialised court in those matters.

Consequently, with the implementation Law, as the opinion argues, the task of reviewing NDPC's decisions was then given to a different and inexperienced court, from the point of view of the matters involved, instead of maintaining that process in the hands of the CCRS, which in turn had significant experience in data privacy, notwithstanding the new regulation that stepped in. In fact, until 2017, the CCRS had rendered a total of 217 decisions concerning NDPC decisions.⁷⁶⁶

In this sense, it is questionable whether Portuguese Administrative Courts are in position to decide upon these matters, as well as whether they present adequate knowledge when compared to a specialised court with nearly a decade of experience in data privacy and, consequently, if they provide adequate protection of data privacy rights.

Ultimately, judicial review can also be conducted by the Supreme Administrative Court (through appealation) and Constitutional Court, the latter by means of concrete review of the constitutionality of a certain norm, through appealation of the decision of a lower court. In this sense, the case can end up in the Constitutional Court for judicial review if one of the following conditions, among others, is met (article 208 of the Portuguese Constitution and article 70 of the Organic Law of the Constitutional Court):

- _ If the lower court refused to apply any rule on the grounds of its unconstitutionality;
- _ If the unconstitutionality of the rule has been raised during the judicial process and the court decided to apply it.

In other words, if questions of unconstitutionality arise in the Portuguese Administrative Courts, which are Court of Appeals (in the specific case of data privacy), the Constitutional Court will also conduct a judicial review.

5.2. What is the process of judicial review for cases of data protection breaches?

In Portugal, first instance court decisions are not available for consultation. In this sense, and considering that only nearly three years of GDPR implementation have passed, it is hard to draw any conclusions on the process of judicial review of cases in the matter of data privacy, since there's only a handful of decisions to which is possible to have access

⁷⁶⁵ Comissão Nacional de Proteção de dados, Parecer nº 20/2020, Processo no. 6275/2018, <shorturl.at/chkzO> accessed 26th February 2021.

⁷⁶⁶ Miguel Sousa ferro, 'Tribunal da Concorrência, Regulação e Supervisão: uma Análise Jurídico-económica no seu 5º Aniversário' [2017] VI(30) Revista de Concorrência e Regulação 149.

and, of that list, only one was originated by decision of the NDPC, and none had its origin in a data protection breach.

Still, according to the National Paper *Jornal Económico*, since the implementation of the GDPR, and until January of 2021, around 300 data breaches had been notified to NDPC.⁷⁶⁷

5.3. Does the review provide effective remedies to the data protection breaches? If so, please specify. For example, what kind of sanctions are imposed as penalties or what remedies are available?

By the same reasons enunciated in the last question, it is not possible to assess whether or not the reviews provide effective remedies or the extension of the sanctions.

6. What is the process of judicial review of anti-discrimination cases?

Portugal is one of the Member States that most protect people from discrimination according to the EU⁷⁶⁸. However, the Council of Europe and the EU have appointed a very worrisome problem: hate speech, especially in social media and in the media itself. In Portugal, specifically in social media, we see more and more racist speeches against immigrants, refugees, afro-descendants and gypsy communities.⁷⁶⁹ Discrimination is censored by the Portuguese Constitution, namely in article 9, article 13, article 26, article 58, article 59, article 67, article 68, article 69 and article 109.

Portuguese Law differentiates discriminatory behaviours, some as crimes and others as offences according to the seriousness of the situation. Any citizen can report a discriminatory situation even if they are not the victim. In the case of crimes, the discriminatory behaviours are considered what is called *Crimes Públicos* (public crimes), which means that any person can report it to the police or the *Comissão para a Igualdade e Contra a Discriminação Racial* (CICDR).⁷⁷⁰

Article 240, no. 1 of the Portuguese Penal Code states that ‘is punished with a prison sentence anyone who funded or constituted an organisation or developed propaganda

⁷⁶⁷ Mariana Bandeira, 'Regulamento da proteção de dados gerou mais de 272 milhões de euros em multas na Europa', *Regulação e Supervisão: uma Análise Jurídico-económica no seu 5º Aniversário* [2021] *Jornal Económico*

<<https://jornaleconomico.sapo.pt/noticias/regulamento-da-protecao-de-dados-gerou-mais-de-272-milhoes-de-euros-em-multas-na-europa-694111>> accessed 28th February 2021.

⁷⁶⁸ “Crimes de ódio. Portugal é dos países que mais leis tem para combater discriminação” [2018] *Renascença* <<https://rr.sapo.pt/2018/06/21/pais/crimes-de-odio-portugal-e-dos-paises-que-mais-leis-tem-para-combate-r-discriminacao/noticia/116527/>> accessed 11th February 2021.

⁷⁶⁹ Deputy rapporteur: Catarina Marcelino, Report about Racism, xenophobia and ethnic-racial discrimination in Portugal by the Assembleia da República, Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, Subcomissão para a Igualdade e Não Discriminação. Palácio de São Bento, 16 July 2019, page 20 <shorturl.at/hBJ08> accessed 19 February 2021.

⁷⁷⁰ APAV <<https://apav.pt/uavmd/index.php/pt/intervencao/discriminacao>>.

activities that incite discrimination, hate, or violence against a person or a group of people because of their race, colour, ethnic or national origin, ancestry, religion, sex, sexual orientation, gender identity or physical or mental disability, or who encourage it; or who participate or provide assistance for these activities, including their financing”. Number 2 adds that “Is punished with a prison sentence who, publicly, by any means intended for dissemination, provokes violence acts, defames or reviles, threatens, or incite violence or hate (...)”.

Besides the Portuguese Constitution and the Portuguese Penal Code, there is more legislation on discrimination such as the Law no. 93/2017, on the 23 August 2017, relative to prevention, prohibition and combat of discrimination, due to racial and ethnic origin, colour, nationality, ancestry and home territory. Discriminatory behaviours are considered offences in the Law no. 134/99, of the 28th of August 1999 and the Law no. 18/2004, of the 11th of May 2004.

6.1. Which bodies conduct such review? What are the elements that are taken into consideration when such review is conducted?

A judicial review, in Portugal, constitutes ‘an extraordinary means of reviewing a final judicial decision’ intending to avoid an unjust sentence or repair a judicial failure. In Portugal, this review is conducted by the *Supremo Tribunal de Justiça* (The Supreme Court).⁷⁷¹ The purpose of a judicial review in Portugal is to obtain authorisation from the Supreme Court to appreciate again the sentence or absolution, or close the case through a retrial.

This judicial review has two phases: in the first one, the appellant seeks to convince the Supreme Court of the correctness and legality of its position and ask authorisation to review the contested decision; the second phase is when the judicial review is carried out. It is necessary to take into consideration that judicial review has to be justified to be carried out. That justification has to fulfill, at least, one of the elements that are exhaustively listed in article 449 of the Portuguese Penal Procedural Code.^{772, 773}

Although, a judicial review in Portugal can also be conducted by the *Tribunal Constitucional* (the Constitutional Court), which is not only a court but also a constitutional body. As a constitutional body, it has a specific intervention on the constitutional system, namely the declaration of unconstitutionality of legal norms, the powers regarding the President of the Republic, the national and local referendum, and in matters of political parties, political office holders and elections. As a Court, it has the same characteristics as other Courts,

⁷⁷¹ Antas da Cunha Ecija, ‘O Recurso de Revisão e o Advogado’ [2018] <<https://adcecija.pt/en/recurso-revisao-advogado/>> accessed 19th February 2021.

⁷⁷² See Article 449, n° 1 of the Portuguese Penal Procedural Code.

⁷⁷³ Ac. do *Supremo Tribunal de Justiça* (Portuguese Supreme Court) de 12/03/2009, proc. 09P316, <<http://www.dgsi.pt/jsti.nsf/954f0ce6ad9dd8b980256b5f003fa814/48be262b39d71dd78025757b00374745?OpenDocument>> accessed 21 February 2021.

however this one has its composition and competencies directly written in the Constitution.^{774, 775}

The judicial review of the Constitutional Court is one of the mechanisms for the protection of fundamental rights. Although, this protection is not directly applied to the individual when faced with a violation of his/her fundamental rights, since an individual does not have direct access to this court. This means that the Constitutional Court intervenes only to appreciate the decisions of other courts on constitutional matters.

The decisions that can be appealed to the Constitutional Court are specified in the Constitution, namely in article 280, and in the Organic Law of the Constitutional Court, namely in article 70. For there to be a judicial review in this court, an issue of unconstitutionality must have been raised during the process. Nevertheless, the court's decision rests only on the question of unconstitutionality that was raised and does not substitute the contested decision.⁷⁷⁶

6.2. Does the review constitute effective protection against discrimination?

The Portuguese Association for Victim Support (APAV) and the Council of Europe admitted that article 240 of the Portuguese Penal Code is hardly or even never applied in Portugal. Joana Menezes, from the APAV, explained that article 240 is not applied to most cases. It only takes into account crimes with the purpose of public disclosure and hate speech, without regard to private injuries or direct public injuries against another person. This leads to a problem because these last crimes are considered only as injuries, without counting to the statistics of discriminatory crimes. Therefore, for a victim in a situation of discrimination it is extremely difficult to file a complaint, and that is why Portugal needs to act, namely to account for and justly punish discriminatory crimes.

The Council of Europe has criticised Portugal because of a recent report on minorities, between 2013 and 2017, where there was no complaint or conviction under article 240. Portugal has a very limited definition of hate crimes and, as a result, there is an increase in hate speech on the internet and social media because it has become a banality. The Council of Europe calls on the authorities to combat and investigate these types of crimes.^{777, 778}

⁷⁷⁴ See Articles 221, 222, 223 and 224 of the Portuguese Constitution.

⁷⁷⁵ *Tribunal Constitucional* (Portuguese Constitutional Court)

<<https://www.tribunalconstitucional.pt/tc/tribunal-apresentacao.html>> 21th February 2021.

⁷⁷⁶ António Cortes and Teresa Violante, 'Concrete Control of Constitutionality in Portugal: A Means Towards Effective Protection of Fundamental Rights' [2011] 29(4) Penn State International Law Review <<http://elibrary.law.psu.edu/psilr/vol29/iss4/3>> accessed 26th February 2021.

⁷⁷⁷ Nuno Guedes, 'É preciso mudar a lei para saber se somos ou não um país racista' [2020] TSF Rádio Notícias

<<https://www.tsf.pt/portugal/sociedade/e-preciso-mudar-a-lei-para-saber-se-somos-ou-nao-um-pais-racista-11833773.html>> accessed 22 February 2021.

⁷⁷⁸ ECRI Report on Portugal [2018] 13-14.

The truth is that there exists a lot of complaints about racism crimes, but there are very few convictions. Article 240 of the Portuguese Penal Code is not applied by the Portuguese Courts 'because the real cause and motivation of these illegal behaviours is difficult to prove'.⁷⁷⁹ In the year of 2017, there were only 13 convictions for the crime of racial discrimination and most complaints were filed. In Portugal, 'high unemployment levels, low wages, difficulty in accessing education, health, justice and housing are decisive factors for the increase in crime and racism, xenophobia and discrimination'.⁷⁸⁰

A research project entitled '*Combat - O combate ao racismo em Portugal: uma análise de políticas públicas e legislação antidiscriminação*' analysed 106 lawsuits brought by the CICDR between 2016 and 2020. The project coordinator alerted and criticised the lack of timely response, the systematic failures in access to justice and the lack of protection for citizens in bureaucratic processes. Furthermore, she draws attention to the absence of a legal doctrine and jurisprudence in the context of racial discrimination.⁷⁸¹

With this information, it can be said that there is a lack of protection against discrimination in justice and that cases do not even reach the *Supremo Tribunal de Justiça*. However, discrimination at work has been very protected by the courts, including the Supreme Court. There are a lot of judicial reviews on discrimination at work, mostly between women and men, concerning gender equality, equal pay, equal opportunities and moral harassment.

Regarding the *Tribunal Constitucional* (Portuguese Constitutional Court), critics acknowledge that fundamental rights are not effectively protected because it is impossible to bring a direct action to this Court.⁷⁸² Furthermore, in practice, most discriminatory cases are closed because of the conflict or collision between fundamental rights, and the tension between constitutional rights and principles. On the one hand, there is freedom of speech, freedom of the press and freedom of artistic creation protected constitutionally and

⁷⁷⁹ Ana Rita Duarte de Campos e Pedro Barosa, partners at Abreu Advogados (Portuguese Law Firm). Frederico Pedreira, 'Queixas por racismo são muitas mas e as condenações? São poucas' [2020] ECO <<https://eco.sapo.pt/especiais/queixas-por-racismo-sao-muitas-mas-e-as-condenacoes-sao-poucas/>> accessed 22 February 2021.

⁷⁸⁰ *ibid.* Raquel Caniço, barrister at Caniço Advogados (Portuguese Law Firm).

⁷⁸¹ Lusa, 'Racismo: 80% processos acabam arquivados' [2020] Público <<https://www.publico.pt/2020/02/27/sociedade/noticia/racismo-tres-quatro-processos-acabam-arquivados-1905706>> accessed 22 February 2021.

⁷⁸² António Cortes and Teresa Violante, 'Concrete Control of Constitutionality in Portugal: A Means Towards Effective Protection of Fundamental Rights' [2011] 29(4) Penn State International Law Review <<http://elibrary.law.psu.edu/psilr/vol29/iss4/3>> accessed 26 February 2021.

internationally⁷⁸³; on the other hand, with the same protection, there is the right to equality and the protection of diversity, out of respect for the dignity of the human person.⁷⁸⁴

The question is: towards public manifestations, presented as an exercise of these freedoms, allegedly as a mere exhibition of opinion, criticism or even entertainment and humour, despite showing contempt for certain social groups and contributing to stereotypes, must they be combated using speech and debate, or can they be limited and held accountable by the courts? The answer to this question must meet the commitments of the Portuguese State in the construction of a just, solidary and egalitarian society based on the dignity of the human person.

If we check closed cases, when there is a conflict between freedom of expression/press and the right to equality, the understanding prevails that freedoms cannot be limited, since it can be considered censorship. However, the Portuguese Constitution expressly states that these liberties are not unlimited.⁷⁸⁵ The *Tribunal Constitucional* itself says that any form of censorship is prohibited, but it 'is lawful to suppress abuses of freedom of expression'.⁷⁸⁶ In practice, this is very difficult because of the trivialisation of behaviours.

Therefore, although the rights under analysis are protected at international and constitutional levels, their implementation and legal protection are still insufficient to provide them with the necessary protection in the face of the reproduction of stereotypes, acts of discrimination and violence.⁷⁸⁷

6.3. What is a considered role of the technical aspects that result in discrimination (such as algorithmic bias)? How are these problems tackled?

There was a study promoted by Google in partnership with *Fundação Francisco Manuel dos Santos* (Francisco Manuel dos Santos Foundation) and coordinated by João Castro⁷⁸⁸ about artificial intelligence in Portugal and the result was very positive. Portugal is betting mainly on health and retail areas. On the other hand, the banking sector appears more apprehensive and conservative when it comes to artificial intelligence, although there are already some examples.

⁷⁸³ See Article 10 of the European Convention on Human Rights and article 37 and 38 of the Portuguese Constitution.

⁷⁸⁴ See Article 13 of the Portuguese Constitution, the preamble and article 1 to 10 of the Universal Declaration of Human Rights and Article 14 and protocol 12 of the European Convention on Human Rights.

⁷⁸⁵ See article 37, n° 3 and 39 of the Portuguese Constitution.

⁷⁸⁶ Portuguese Constitutional Court, Process n° 949/15, 1st Section, Rapporteur: Conselheiro João Pedro Caupers, 20/09/2016. Available in : <<http://www.tribunalconstitucional.pt/tc/acordaos/20160496.html>> accessed 28 February 2021.

⁷⁸⁷ Isabella Ribeiro Liquer, Report under the project 'Vulnerabilidade e diversidade: direitos fundamentais em contexto' 'Non-discrimination for gender and sexual orientation', CIJE from FDUP, 28-34.

⁷⁸⁸ Professor at NOVA SBE, Portugal.

João Castro is very clear about the differences between Europe and America. Europe is trying to orient itself by the General Data Protection Regulation (GDPR), while America is guided by capitalism.⁷⁸⁹ Nevertheless, Portuguese people are also targeted by Facebook, Instagram, Zoom, Twitter, Tinder and so many other apps when it comes to discrimination. Therefore, although in Portugal those who work in this area seek to make the processing of personal data with caution and legal guarantees, it is important to have mechanisms of protection against discrimination in technology.

In Portugal, there exists an independent administrative entity called *Comissão Nacional de Proteção de Dados* (National Data Protection Commission) that controls and monitors compliance with the GDPR, Law no. 58/2019, Law no. 59/2019, Law no. 41/2004, as well as other legal and regulatory provisions on the protection of personal data. The main goal of the NDPC is to defend people's rights, freedoms and guarantees in the context of the processing of their personal data.

A person who sees his/her rights, freedoms and guarantees being violated in the context of the processing of their personal data, can ask for information or clarification and make complaints or reports with the NDPC.⁷⁹⁰

7. Does your country have any specific regulations on advanced digital technologies, such as big data, Artificial Intelligence (AI), Internet of Things (IoT) and/or encryption?

At the present moment, there are no regulations on advanced digital technologies such as big data, Artificial Intelligence, Internet of Things and encryption. The Portuguese regulatory frameworks for advanced digital technologies are still in a preliminary stage, and as of now any provisions that concern these topics are scattered across sector-specific regulations. Portugal is strongly influenced by international developments, particularly at the European Union level.

7.1. Please specify any existing or proposed legislation. If none is in place, are there any initiatives introduced by private actors or NGOs?

In this regard, an Action Plan for Digital Transition⁷⁹¹ has been approved, concerning the development of new digital technologies such as cloud computing, Internet of Things, among others. A Resolution from the Ministers' Council no. 29/2020, which concerns the establishment of regulatory frameworks, has been approved in April 2020. It lays down the

⁷⁸⁹ Sara Sá, 'Deepfakes e algoritmo do Facebook é o que os Portugueses mais temem na IA' [2021] Visão <<https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2021-02-11-deepfakes-e-algoritmo-do-facebook-os-portugueses-mais-temem-na-ia/>> accessed 28 February 2021.

⁷⁹⁰ National Data Protection Commission <<https://www.cnpd.pt>> accessed 28 February 2021.

⁷⁹¹ Resolution of the Council of Ministers, n°. 78/2020.

general principles for the creation and regulation of Free Technological Zones. It also establishes the objective of developing a regulatory framework that promotes and facilitates new technologies' testing, services, products and innovative processes, thus encouraging its development. Additionally, it sets a goal to develop a specific treatment and legal framework for each technology, in line with the work of the European Union.

Furthermore, in May 2021, the 'Charter of Fundamental Rights in the Digital Era' was approved. The aim is to 'innovate, clarify and bind State powers'⁷⁹² through 23 articles, with an innovative 'right to a good use of AI and robots' (concerning algorithms and the creation and use of robots). It establishes that use of Artificial Intelligence must be guided by principles such as the respect for fundamental rights, security, transparency, accountability and explicability, while the use and creation of robots must observe, *inter alia*, the principles of beneficence, non-maleficence, the principle of respect human autonomy and justice, non-discrimination and tolerance⁷⁹³. This Charter also enshrines several other noteworthy rights, such as a 'right to net neutrality', a 'right to cybersecurity' and a 'right to be forgotten'.⁷⁹⁴

Some of the issues posed by big data are addressed in the data protection regulatory framework. Law no. 58/2019⁷⁹⁵ has transposed the EU General Data Protection Regulation (GDPR)⁷⁹⁶ to the Portuguese legal system. This Regulation entered into force in 2016, becoming applicable in Portugal as of the 25th of May 2018. This law specifies some of the Regulation's general provisions, changes some of its requirements, and regulates situations the latter has not expressly provided for, such as the treatment of data arising from video vigilance systems. In addition, Law no. 32/2008⁷⁹⁷ transposes Directive 2006/24/CE with regard to the conservation of data generated or treated in the context of services of electronic communications, while Law no. 12/2005 of the 26th of January concerns personal genetic information and health information.

7.2. To what extent are the external legislative developments influential on your country's regulation of this area?

As a Member State of the European Union, Portugal is strongly impacted by the European Union's normative acts. European Union regulations are directly applicable in Member States, its Directives bind the results to be achieved by national legislation, and other agreements that are legally binding have the strongest legal effects. These are followed by

⁷⁹² Law n.º 27/2021 Official Journal n.º 95/2021, Series I 2021-05-17.

⁷⁹³ *ibid*, art. 9.

⁷⁹⁴ *ibid*, art. 10, 15 and 13 respectively.

⁷⁹⁵ Law n.º 58/2019 8th August, Official Journal n.º 151/2019, Série I de 2019-08-08.

⁷⁹⁶ General Data Protection Regulation)[2016] OJ L 119.

⁷⁹⁷ Law no. 32/2008 17th July.

recommendations and opinions.⁷⁹⁸ It is laid down in article 8 of the Portuguese Constitution that Treaty provisions and EU norms are applicable in the Portuguese legal system. In fact, Portuguese authorities cannot apply national norms contrary to EU Law, as established by settled European Court of Justice case-law.

As a result, the national provisions that are related to the effects of these new technologies in different fields often derive from the transposition of European Directives.⁷⁹⁹ For instance, this was the case with Law no. 30/2020, which transposes Directive (EU) 2015/1535⁸⁰⁰ regarding the information procedures in the field of technical regulations and rules concerning Information Society services.

Regarding the regulation of digital advanced technologies in particular, Portugal is closely following the European Union's legislative developments. In the field of Artificial Intelligence, Portugal signed the Declaration on Cooperation on Artificial Intelligence in April 2018.⁸⁰¹ This is one of many milestones in the context of the European Commission's Artificial Intelligence Strategy in 2018, with a human-centric approach. This has led to a publication of a White Paper on AI in February 2020, and an upcoming legislative proposal, which is expected to take place in 2021.⁸⁰²

With regards to big data, the European Commission has published a proposal for a Regulation on European Data Governance⁸⁰³ with the aim to increase trust in data intermediaries and reinforce data-sharing mechanisms across the Union, in order to stimulate the availability of data. The aforementioned General Data Protection Regulation is comprehensive, but it only concerns personal data. In addition, a regulation is being developed to replace the ePrivacy Directive, concerning the processing of data and privacy in the electronic communications sector.⁸⁰⁴

Furthermore, Portugal integrates other international intergovernmental organisations with stances on advanced digital technologies, such as the World Commerce Organization, the

⁷⁹⁸ Article 288, Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, 171–172.

⁷⁹⁹ Alexandre Dias Pereira, *'Direito da Informática, Estudos'* [2017] 7.

⁸⁰⁰ General Data procedure for the Formation in the field of technical regulations and of rules on Information Society services Protection Regulation [2015] OJ 2 241/1.

⁸⁰¹ Commission, 'Declaration on Artificial Intelligence' [2018] <<https://ec.europa.eu/jrc/communities/sites/jrccties/files/2018aideclarationatdigitaldaydocxpdf.pdf>> accessed 22 February 2021.

⁸⁰² Artificial Intelligence <<https://ec.europa.eu/digital-single-market/en/artificial-intelligence>> accessed 22 February 2021.

⁸⁰³ Proposal for a Regulation on European data governance (Data Governance Act) [2020] <<https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-ac>> accessed 22 February 2021.

⁸⁰⁴ European Commission 'Proposal for an ePrivacy Regulation' <<https://ec.europa.eu/digital-single-market/en/proposal-privacy-regulation>> accessed 26 February 2021.

United Nations Educational Scientific and Cultural Organization, among others. Portugal is also a member of the Organisation for Economic Co-operation and Development (OECD), that has adopted several of these instruments in the field of advanced digital technologies: the OECD Principles on Artificial Intelligence⁸⁰⁵ in 2019 as well as the Recommendation concerning Guidelines for Cryptography Policy⁸⁰⁶ in 1997 which is regularly reviewed. While its recommendations are not legally binding, they are influential and taken into consideration when developing national legislation.

It is expected that regulations that are specific to each new technology (Artificial Intelligence, Big Data, among others) will be developed by the European Union and any national legislative development will be in accordance with the orientations and norms that the EU sets. It is expected also that the efforts taking place across the world by international bodies and industry stakeholders to fill these gaps, although not binding, will be taken into account particularly when building new regulatory frameworks from scratch.

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?

Society is facing, for a few years already, an age of fierce developments in all fronts when we talk about Artificial Intelligence (from now on, named AI), which has been changing and affecting our life in general – for both good and bad –, as well as our personal, and public relations.⁸⁰⁷ Globalisation, highly impelled by the technologies and the utopia of a connected online world, has been extinguishing frontiers, namely geographic and legal ones, which can represent a huge advantage; but it also has a paradoxical effect, namely the dependency on the demanding of digital life.⁸⁰⁸ This – as Aldous Huxley⁸⁰⁹ would say – Brave New World is changing our ways of communication and interaction with others, being our time, more than ever, dependent on AI, as well as other technologies, constantly appearing and changing our perspectives. This demands a fundamental and necessary reflection on the achievement of legislation - an improvement of legislation.⁸¹⁰

If, as we know, law origins are the human relations and the human interaction, and if they are, as we said, more than ever, so dependent on technologies, the way of law acts is highly challenged by the disruptive nature of AI, which – we can say – has already some years in

⁸⁰⁵ OECD/Legal/0449, adopted 25th December 2019.

<<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>> accessed 26 February 2021.

⁸⁰⁶ Recommendation of the Council concerning Guidelines for Cryptography Policy, OECD/Legal/0289, adopted 27 March [1997] <<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289>>.

⁸⁰⁷ Henrique Antunes, *Direito e Inteligência Artificial* (1st ed., Universidade Católica Editora, 2020), 7-8.

⁸⁰⁸ Maria Esteves, 'A Utopia Transhumanistas fundada nas ilimitadas possibilidades das tecnociências – uma ameaça à dimensão axiológica do humano, constitucionalmente acolhida e merecedora de tutela penal' (eds), *Criminologia Integrativa* (Editora D'Plácido 2018), 651.

⁸⁰⁹ Aldous Huxley was an English writer, a humanist and pacifist, more known for his novel *Brave New World*.

⁸¹⁰ Henrique Antunes, *Direito e Inteligência Artificial* (1st ed., Universidade Católica Editora, 2020).

advance of legislation capability, that is highly misfit, having in consideration the technological evolution.⁸¹¹ The so known and promised 4th Industrial Revolution, that even challenges the own idea of what we establish as human beings, can't be defined through only one set of technologies that can be extinguished in themselves, nor even a hegemony of an exact type of technology, resulting instead in a constant interaction between physical, virtual, biologic and juridic realities.⁸¹²

The huge and fierce technological developments have started a cultural extraordinary change, in which penal and procedural law are not an exception, in their juridic, epistemological and ethical ways, as we have the growing use of AI on court,⁸¹³ fostering a debate on the opposition between the crescent use of digital proof and the guarantee of private life, foresaw as a human right through article 12 of the Universal Declaration of Human Rights⁸¹⁴ (from now on, named UDHR), which foresees that no one shall be subjected to arbitrary⁸¹⁵ interference with his/her privacy. We can assume that, in one hand, the resource to technological and AI devices brings, besides what we established before, undeniable advantages to procedural law, for example when we talk about saving time and charges; in the other hand, it comes to show and polarize the differences between social classes, already economically separated, and challenging the procedure fundamental rights.⁸¹⁶

In Portugal, the use of digital proof and encrypted personal messages can be used under some circumstances, namely in the event of Cybercrimes, but not only; actually, it can become relevant to use digital proofs in barely any crime, being, without disregarding what said before, this use, subject of some criteria, as well as some concepts, not being clear which ones. Before we continue, and for the correct understanding of the following essay, it is important to distinguish electronic from digital proof. Electronic proof is a widest concept than digital proof, being included in the first one proofs obtained through both digital and analogic – from photography and photographic roll – ways⁸¹⁷; digital proof is a product of data in an informatic format – in a binary form – that is manipulated, stored and communicated through any kind of tech device, computer, informatic system or even

⁸¹¹ *ibid*, 7-8.

⁸¹² Anabela Miranda Rodrigues, *A Inteligência Artificial no Direito Penal* (1st ed, Almedina, 2020), 129.

⁸¹³ *ibid*.

⁸¹⁴ The full UDHR body is available here <<https://www.un.org/en/universal-declaration-human-rights/>> accessed 27 February 2021.

⁸¹⁵ Arbitrary is an important part of the article, giving United Nations, through this word, to states a wiggle room for they can act in consideration with their domestic legislations.

⁸¹⁶ Rodrigues (n 813), 129-130.

⁸¹⁷ Electronic proof is foreseen in articles 1st, 11th, n° 1 c), 18th, n° 1, b) and 20th of Cybercrime Portuguese Law.

transmitted through a network system,⁸¹⁸ which includes encrypted personal messages⁸¹⁹ that can give information about personal diaries, localisation data, between others.

8.1. Specify the circumstances in which such decryption may be conducted? What are the potential or real consequences of such requirement?

As we have established, access to digital proof, which includes the decryption of personal messages, is composed by a logic sequence of *bits* that exists independently of the material support; digital proof can be usually found in some places, only through specific tools and under specific circumstances. Domestic legislation foresees its admissibility through articles 187, 188 and 189 of the Penal Procedural Code, and Law no. 109/2009 of the 15th of September (Cybercrime Law).⁸²⁰

The Penal Procedural Code (from now on PPC) foresees, through its article 187, the interception and the record of conversations and telephonic communication. This can only be authorised during inquiry - “*Inquérito*” -⁸²¹ and only if there is enough evidence and reasons to believe that this diligence - this interference in the suspect’s personal life – is imperative to find the truth or, if the proof wouldn’t be found in any other way, being that it can only happen by a duly justified order from a specific judge – “*juíz de instrução*”⁸²² – and by a requirement from the Public Prosecution Service (from now on, named PPS) – “*Ministério Público*”. These articles establish that this possibility can only happen in crimes whose minimum penalty is three years, in relation to what is foreseen on the paragraphs of its numbers 1 and 2.⁸²³ In an attempt to restrict the excessive, avoiding its trivialisation use of this invasion, the PPS established a set of formal and material conditions and requirements through which the access to private digital information can happen, under nullity penalty of the proof.

⁸¹⁸ The possibility to appeal in court to digital proof is foreseen in article 189th of the Portuguese Processual Penal Code (from now on, named PPC).

⁸¹⁹ Rodrigues (n 813), 130-132.

⁸²⁰ The full Cybercrime Law body is available in

<http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis> accessed 29th February 2020. Results this law from a transposition into the domestic legal order Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems in consensus with the Convention on the European Council on Cybercrime, that Portugal signed in 2001. Lately the Council Framework Decision was changed by the Directive N. ° 32/2008, 17th July.

⁸²¹ The Inquiry process is foreseen in article 262nd CPP. The full CPP body is available at <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=199A0187&nid=199&tabela=leis&ficha=1&nversao=>> accessed 29 February 2021.

⁸²² The function of the “*juíz de instrução*” is foreseen in article 17th CPP. The full CPP body is available at <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=199A0187&nid=199&tabela=leis&ficha=1&nversao=>> accessed 29 February 2020.

⁸²³ The full CPP body is available at <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=199A0187&nid=199&tabela=leis&ficha=1&nversao=>> accessed 29 February 2021.

The foreseen on the interception and record of conversations and telephonic communication – article 187 PPC - mentioned above is applicable and extended to any technological device that may have information, e-mails and other ways of data transmission by telematics, as is foreseen by article 189 PPC. In this way, we can conclude that Penal Procedural Law foresees the limitation of right to privacy, namely through interception of telecommunications.

8.2. Does this requirement (in general or in practice) provide the authorised body with too much power? Clarify your answer.

As *Schwab* would say, this fourth stage of industrialisation is not only a new stage of technological development, predicting a truthful change of paradigm, and this, as we have foreseen, also includes a structural change in the common accessions and realities of the law and courts system.⁸²⁴ These aggressive changes are reflected in the omnipresence of technology in our social life as well as the risks for the fundamental rights – right to a fair trial⁸²⁵ and right to privacy -, democracy and Rule of Law. To avoid these attempts, there are normative instruments from the European Union Law and Domestic Law that, working with a common aim, are applicable on courts and administrative authorities; being an example of this, the Cybercrime Law, whose interpretation and application is made in consensus with other domestic laws on cybercrime and digital proof. Its application has raised doubts on Portuguese jurisprudence and doctrine, especially in the articulation between Cybercrime Law and the PPC,⁸²⁶ being also important to have in mind the interference between the juridic domestic interpretation on data obtained and treated in Portuguese courts⁸²⁷ and in the European Union.⁸²⁸

Expanding the proof means that, with resource to AI and decryption, the fine line between what is conceded by law and what is not can easily be transcended, attempting against a multiplicity of human and fundamental rights, which can reflect an excessive – and also uncontrolled – power to the authorised body, which can include courts, “*Ministério Público*”, “*Juíz de Instrução*”, among others.⁸²⁹

⁸²⁴ Rodrigues (n 813), 130-137.

⁸²⁵ Article 8th UDHR - The full UDHR body is available at <<https://www.un.org/en/universal-declaration-human-rights/>>, accessed 27 February 2021.

⁸²⁶ Francisco Pacheco de Andrade, *et al.*, “Relatório Cibersegurança em Portugal: Ética & Direito” <https://www.cncs.gov.pt/content/files/relatorio_etica.direito2020__observatoriociberseguranca_cncs.pdf> accessed 28 January 2021.

⁸²⁷ Stablished through N.º 32/2008, 17th July Law. The full body of the law is available at <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=selected&nid=1264&tabela=leis&pagina=1&ficha=1&nversao=>> accessed 28 January 2021.

⁸²⁸ The European Commission moved a formal procedure against Portugal about the wrong transposition of the Directive N.º 32/2008, 17th July, relative to the attacks against the information systems.

⁸²⁹ Rodrigues (n 813), 137.

Following this line of thought, the right to speak, the right to the protection of one's image, the right to privacy, the right to informational self-determination, as well as the right to integrity and trust on the legal systems and, at its extreme, to celerity on the right to a fair and impartial defence of the accused, are only some of the rights highly at risk when we allow the resource to encrypted messages and information during trials. From this chapter of the essay we can conclude that there are two different dimensions of the use of decryption: in one hand, we have the right to privacy and, in the other hand, the right to a fair and impartial defence, both of which can be easily alienated and curtailed in this scenario.⁸³⁰

8.3. What level of protection does your country's legislation provide to the individuals in the circumstances mentioned above?

In Portugal, the right to privacy is foreseen by Constitutional Law, but having in consideration the developments of investigation methods – highly stimulated by the 4th Industrial Revolution –, this constitutional protection has created a mechanism that intends to answer to this new paradigm. Doctrine and jurisprudence have been, in the last few years, the motors that stimulated and defined the limits and demands of the right to informational self-determination – article 35 of the Portuguese Constitution -. This right foresees that any citizen has the right to decide, himself, when and under which circumstances they want their personal data and messages revealed. This right works as a guarantee of the right to privacy, protecting – or at least, intending to protect – the individuals against the State's accesses, through AI and decryption, to communications and stored data⁸³¹. Having in consideration the timeline between law and technology developments, the notion of what we consider as 'private life' on article 34 of the Portuguese Constitution has to be redefined, being that today's concepts as 'domicile' – something physically – and 'correspondence' – something corporal – doesn't represent the essence of individual privacy, being most of our information in technological devices.⁸³²

The access to encrypted information can be highly offensive and that's why law tries to be exhaustive in this point because, having in consideration the characteristics of new technologies, the disproportionate interference on the private life of, not only the accused, but also of suspects or third parties is very tempting. There is also a concern about the protection of private messages between the accused and his defendant – the lawyer,⁸³³ and the interception of encrypted messages is only authorised and valid as a proof for a maximum of three months, being after that renewed for the same time if the judge

⁸³⁰ *ibid.*

⁸³¹ *ibid.*, 137-139.

⁸³² *ibid.*, 139.

⁸³³ Foreseen by article 187th, n. 5 CPP.

considers⁸³⁴, being subjected to its use the formalities foreseen by article 188 PPC. Procedural Law and Constitutional Law, stimulated by jurisprudence, have been trying to avoid this paradigm, densifying and expanding the traditional guardianship of pre-existing fundamental rights⁸³⁵. In this way, and in respect to the fragile nature of right to privacy, besides the cases expressly foresaw by law, the intromission to privacy is protected by insurmountable prohibition of proof, as the own European Court of Human Rights predicted through its sentences and also the EU established by the Regulation (EU) 2016/679 of the European Parliament and of the Council of the 27th of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.⁸³⁶

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online? If applicable, specify how the situation in your country is perceived externally (by other countries/ members of the economic/political bloc, international organizations, etc).

According to a report presented by OECD on the countries that are making the best progress on the topic of digital governance, Portugal ranks 9th. The index consists of a measurement tool that monitors the adoption of a strategic approach, policy levers, mechanisms for implementing and monitoring digital government policies in OECD member countries and partner countries.⁸³⁷

Still, according to the European Investment Bank, Portugal is the third strongest country in the digitisation index. The European Investment Bank's Investment Research Digitization Index (EIBIS, in its acronym in English), groups the countries of the European Union according to the assessment of companies in terms of digitisation: pioneers, strong, moderate and modest.

EIBIS prepared the report in 2020, with the objective of understanding what are the main problems for companies when it comes to the adoption of digital technologies. In

⁸³⁴ *ibid.*

⁸³⁵ Human rights enjoy a dynamic nature, meaning that it is not necessary a previous legislative intervention to expand themselves. - Rodrigues (n 813), 141.

⁸³⁶ The full GDPR body is available here

<<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PT>> accessed 2 March 2021.

⁸³⁷ Organisation for Economic Co-operation and Development, Digital Government Index 2019

<<http://www.oecd.org/gov/digital-government-index-4de9f5bb-en.htm>> accessed 16 February 2021.

particular, the document highlights how access to management, skilled labor and the regulatory environment affect the digitisation of European companies.⁸³⁸

Thus, we can observe that Portugal presents itself as a country that is concerned with the balance between human rights online and digital advances, while increasingly investing to make this balance happen as soon as possible.

10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the coming 5 years? Incorporate the answers you have given to the previous questions, and the main results of your research.

As a part of the INCoDe.2030 Program, which is an integrated public policy initiative aimed at enhancing digital competences, with valances that include AI and data privacy, Portugal has shown that it is committed to cooperating with the EU when it comes to policy making and updating.⁸³⁹

On the other hand, the European Commission made very clear the importance of making ‘What’s illegal offline illegal online’.

Accordingly, enormous efforts have been put into place in order to identify the risks of technologies, as well as the menace it presents to human rights, and solutions have been proposed in the last years, either by scholars, regulation entities and digital rights protection associations, in order to guarantee protection of those who use technology as final consumers (users). In this sense, the expectation is that in the following five years, legislation will suffer significant densification and concretisation, besides the implementation of new regulation that will impose additional obligations for technological companies and create innovative legal frameworks.

As described in the present report, legislation concerning data privacy is the one that, so far, offers better protection to individuals, although further concretisation for monitoring and enforcement is still required.

Another major evolution that has been pointed out as probable might be related to the creation of new regulation and supervision entities, which in turn has consequences in legislation and hopefully grants protection of the individual’s human rights.⁸⁴⁰

⁸³⁸ European Investment Bank, ‘Who is prepared for the new digital age? - Evidence from the EIB Investment Survey’; <<https://www.eib.org/en/publications/who-is-prepared-for-the-new-digital-age>> accessed 16 February 2021.

⁸³⁹ The program can be consulted through <<https://www.incode2030.gov.pt/en/action-lines>> accessed 16 February 2021.

⁸⁴⁰ Recommendation, Council of Europe Commissioner for Human Rights ‘Artificial Intelligence: 10 Steps to protect human rights’ [2019] 10.

It is also predictable that some new Regulation will be approved, which will be applicable to Portugal. The major change in discussion in the European Parliament is the Digital Services Act (DSA) and the Digital Markets Act (DMA).

In specific, the DSA promises to look out for individual's rights by imposing, among others, the following measures:⁸⁴¹

- _ Measures to counter illegal goods, services or content online, (for instance, mechanisms for users to flag such content);
- _ New obligations on traceability of business users in online marketplaces, in order to identify sellers of illegal goods;
- _ Effective safeguards for users, regarding content moderation process and decisions;
- _ Transparency measures for online platforms;
- _ Obligations for very large platforms (meaning the ones that reach more than 10% of the EU's population) to prevent abuse of their systems;
- _ Codes of conduct and technical standards for the online platforms;
- _ Application of these new rules to all online intermediaries offering their services in the single market, regardless of their location (inside or outside the EU);
- _ Enhanced supervision and enforcement by the Commission and a new European Board for Digital Services.

Another set of initiatives is taking place, namely concerning ethical questions and principles in AI (regarding its development, implementation and utilisation), which inevitably will have an impact on human rights online, as well as legal framework for liability for AI conduct, which in turn will, predictably, provide remedy mechanisms in case of violation of human rights. Accordingly, the European Commission is committed to proposing new AI legislation.⁸⁴² Although its exact terms are not yet known, its discussion and approval is expected to occur over the next five years.

These initiatives will allow the adoption of regulations by the Member States, and consequently the uniformisation of obligations, either for the public or private sector, when it comes to technology usage. These obligations are, in general, related to transparency and protection of the rights of the users (which include protection against discrimination, protection of the individual's self-determination, minimisation of the use of personal data, remedies in case of violation of rights, among others).

⁸⁴¹ Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), COM/2020/842 final and https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_en accessed 16 February 2021.

⁸⁴² <https://www.europarl.europa.eu/news/en/headlines/eu-affairs/20201208STO93329/coming-up-eu-spearheads-efforts-for-recovery-in-2021#:~:text=In%20early%202021%2C%20the%20Commission,at%20the%20forefront%20of%20developments> accessed 16 February 2021.

As mentioned, Portugal established lines of action through the INCoDe.2030 Program. Through this program, on the 1st of February 2019, the program AI Portugal 2030 was launched, with the purpose of outlining an innovation and growth strategy to foster Artificial Intelligence in Portugal in the European context. In this initiative, the importance of ethics is highlighted,⁸⁴³ meaning that legislation to come must obey ethical principles, not only in the European context but also specifically in internal Laws.

Accordingly, the initiative mentions transparency (in the sense of ability to explain the decisions) and auditability (the ability to trace the flow of decisions and actions from humans to algorithms) as two strong pillars in promoting safety and compliance with ethical principles, including privacy protection and fairness.

Also, the Action Plan for Digital Transition has been approved, concerning the development of new digital technologies such as cloud computing, Internet of Things, among others. A Resolution from the Ministers' Council no. 29/2020, which concerns the establishment of regulatory frameworks, has been approved in April 2020. It lays down the general principles for the creation and regulation of Free Technological Zones. It also establishes the objective of developing a regulatory framework that promotes and facilitates new technologies' testing, services, products and innovative processes, thus encouraging its development. Additionally, it sets a goal to create a specific treatment and legal framework for each technology, in line with the work of the European Union.

The European Commission has also published a proposal for the Regulation on European Data Governance⁸⁴⁴ with the aim of increasing trust in data intermediaries and reinforcing data-sharing mechanisms across the Union, in order to stimulate the availability of data. The aforementioned General Data Protection Regulation is comprehensive, but it only concerns personal data. In addition, a Regulation is being developed to replace the ePrivacy Directive, concerning the processing of data and privacy in the electronic communications sector.⁸⁴⁵

The last major legislative change that should be noted is the modifications expected to occur in Law no. 1/2005, from the 10th of January, which regulates the use of video camera surveillance systems by security forces and services in public places. Although the

⁸⁴³ AI Portugal 2030, Portuguese National Initiative on DIGI, Coordination Office of INCoDe.2030 Initiative, Portuguese Science and Technology Foundation (FCT), The Portuguese Innovation Agency (ANI), Ciência Viva and the Portuguese Agency for Administrative Modernisation (AMA), page 35 <https://www.incode2030.gov.pt/sites/default/files/julho_incode_brochura.pdf> accessed 15 February 2021.

⁸⁴⁴ Proposal for a Regulation on European data governance (Data Governance Act) [2020] <<https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-ac>>.

⁸⁴⁵ European Commission 'Proposal for an ePrivacy Regulation' <<https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>> accessed 26 February 2021.

initiative has not yet been discussed in the Portuguese Parliament, the Portuguese Minister of Intern Administration already stated that it will introduce significant changes in the legal framework, namely by imposing the use of body cams in police officer's uniforms. Allegedly, the NDPC will be heard on the matter when the proposal is concluded and sent for the Parliament for discussion and approval, a process also expected to take place within the next five years.

Conclusions

Throughout this report, several legal frameworks associated with different rights were described. In this sense, the report seeks to understand how human rights associated with technologies are protected at a national level through legislation as well as at an international and European level.

It is clear that, as a Member State of the European Union, Portugal is strongly impacted by the European Union's normative acts. On one hand, European Union Regulations are directly applicable in Member States, and on the other, its Directives are transposed to national legislation, which must comply with them. These types of acts are followed by recommendations and opinions, which help in specifying and densifying legal concepts and respective legal frameworks.

In general, and besides specific legislation mentioned throughout the report, many concerns are expressed regarding technology and privacy in the Portuguese Constitution, for instance, among many, in article 35 which determines the protection of citizens against the processing of computerised personal data, as well as highlights that the use of data processing is prohibited in some specific cases, where it could even be a threat to human rights. The article also guarantees minimum guidelines with which the data should be treated.

However, concerns about the impact of technology on human rights are also described in the e.2030 Digital Skills National Initiative (Portugal INcoDe.2030), published in 2017, which is an integrated public policy program that focuses on promoting digital skills, which seeks to protect human rights as described by the International Convention on economic, social and cultural rights. In turn, these are listed as the right to work in fair and favourable conditions, the right to social protection, an adequate standard of living and the highest attainable standards of physical and mental well-being, the right to education and to enjoy the benefits of cultural freedom and scientific progress.

In this regard, data privacy is by far the right that is most studied and protected in Portuguese Law, not only by means of existent legislation before GDPR, but also due to its direct application and implementation through the Law no. 58/2019. Also, in terms of

monitoring and enforcement, the National Data Protection Commission has also contributed to this protection, being an independent administrative entity, with powers of authority, endowed with administrative and financial autonomy, while also working with the Portuguese Parliament advising and consulting on the matter when needed. Additionally, the NDPC issues opinions on non-consensual matters, which helps clearing out any doubts regarding data privacy.

In this sense, in Portugal, the private sector enjoys a certain degree of self-regulation and is not subject to as many requirements and measures as the public sector. Nevertheless, there are some regulations that apply equally to all entities, regardless of their nature, such as in the case of protection of personal data and privacy in telecommunications (Law no. 41/2004, of the 18th of August) and personal genetic information and health information (Law no. 12/2005, of the 26th of January).

However, and according to article 8, no. 1 of the Law no. 58/2019, public and private entities must provide their collaboration to NDPC, providing all the information requested by it, in the exercise of its powers.

Up to date, there aren't many examples of cooperation between the private and public sector in matters of data privacy. However, during the pandemic, ISPUP - Public Health and Epidemiology (public entity) and INESC TEC, Keyruptive Technologies and Ubrider (private entities) came together to develop the application "STAYAWAY Covid", a controversial app, in terms of data privacy. Notwithstanding the critics and concerns of the NDPC, the Portuguese government repeatedly and strongly recommended its installation on the populations' mobile phones.

However, in matters of data privacy it is still unclear on how effective existent legislation is, as well as what kind of process takes place when Administrative Courts conduct judicial review of cases and whether or not they provide adequate remedies. In specific, opinions issued by the NDPC must be taken into account when analysing the legal framework of data privacy in Portugal, as they provide important information on the vulnerabilities of the implementation of Law no. 28/2019.

When it comes to protection against discrimination, Portugal is one of the Member States that most protect people from discrimination according to the EU. However, many problems are still pointed out in this report, regarding this matter.

On one hand, hate speech, especially in social media and in the media itself is increasing. Specifically, in Portugal, hate speech against minorities, such as immigrants, refugees, afro-descendants and gypsy communities is visibly expanding each day.

On the other hand, judicial review of anti-discrimination cases appears to be somewhat ineffective. A judicial review in Portugal, unlike in other countries, constitutes ‘an extraordinary means of reviewing a final judicial decision’, intending to avoid an unjust sentence or repair a judicial failure. In general, this review can be conducted by the Supreme Court or Constitutional Court. In the first case, the purpose is to obtain authorisation from the Supreme Court for new appreciation of the lower courts’ decision or to close the case through a retrial. The second case is a mechanism for the protection of fundamental rights. However, in this circumstance, an individual, when faced with a violation of a fundamental right, does not have direct access to the Constitutional Court, since its intervention only occurs when an appreciation of the decision of a lower court on constitutional matters is needed (in the terms prescribed by article 240 of the Portuguese Constitution).

In this sense, and notwithstanding the fact that hate speech is visible in Portugal and considered a crime, under article 240 of the Portuguese Penal Code, according to APAV (Victim Support Portuguese Association) and the Council of Europe, between 2013 and 2017, there was no complaint or conviction under article 240, due to the very limited definition of hate crime.

A research project entitled ‘*Combat - O combate ao racismo em Portugal: uma análise de políticas públicas e legislação antidiscriminação*’, which analysed 106 lawsuits between 2016 and 2020, concluded that the above described was also a result of lack of timely response, the systematic failures in access to justice and the lack of protection for citizens in bureaucratic processes, as well as the absence of a legal doctrine and jurisprudence in the context of racial discrimination.

Therefore, although the rights under analysis are protected at the international and constitutional levels, their implementation and legal protection are still insufficient to provide them with the necessary protection.

At the present moment, in Portugal, there are no regulations on advanced digital technologies such as big data, Artificial Intelligence, Internet of Things and encryption. In this regard, an Action Plan for Digital Transition has been approved, concerning the development of new digital technologies such as cloud computing, Internet of Things, among others. Portugal is also closely following the European Union’s legislative developments, having signed the Declaration on Cooperation on Artificial Intelligence in April 2018.

Regarding digital proof and encrypted personal messages, its use in criminal cases is allowed. However, specific conditions must be met. For instance, the interception and the record of conversations and telephonic communication must be properly authorised and

justified by the judge, during the investigation (*Inquérito*) and only if there is enough evidences and reasons to believe that this diligence - this interference in suspects' personal lives – is imperative to find the truth and provided there is no other way to obtain that evidence. Also, this type of proof can only be used if the framework of the crime that is being investigated determines a minimum of three years of jail time if convicted. The use of communications is also restricted by a set of formal conditions and requirements through which the access to private digital information can happen.

In conclusion, although Portugal is committed to the protection of human rights, the legal framework still shows some flaws, both in terms of adapting to changes in society itself, in all its dynamics, advances and rapid evolution, and in terms of ensuring effective monitoring and adequate remedies in cases of violation of rights.

As the European Union intends to make the decade of 2020-2030 the Digital Transformation Decade, and Portugal, as a state member, must comply with any new Regulations, as well as transpose all the approved Directives, these adaptations are expected to occur soon. It is also expected that these flaws will be reviewed, mitigated and/or corrected in the near future, starting with the Digital Services Act (DSA) and the Digital Markets Act (DMA), and complementing with the new Regulation on AI that is currently in discussion, the ePrivacy Directive as well as any other Regulations that result from the Action Plan for Digital Transition and Resolution from the Ministers' Council no. 29/2020, which concerns the establishment of regulatory frameworks.

Table of legislation

Provision in portuguese	Corresponding translation
Constituição da República Portuguesa Artigo 35.º (Utilização da informática) 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja	Constitution of the Portuguese Republic Article 35 (Use of information technology) 1. Every citizen has the right of access to all computerised data that concerns him, which he may require to be corrected and updated, and the right to be informed of the purpose for which they are intended, as laid down by law. 2. The law shall define the concept of personal data, together with the terms and conditions applicable to its automatised treatment and its linkage, transmission and use, and shall guarantee its protection, particularly by means of an independent administrative entity. 3. Information technology may not be used to treat data concerning philosophical or political convictions, party or trade union affiliations, religious faith, private life or ethnic origins, save with the express consent of the data subject, or with an authorisation provided for by law and with guarantees of nondiscrimination, or for the purpose of processing statistical data that are not individually identifiable. 4. Third-party access to personal data is prohibited, save in exceptional cases provided for by law. 5. The allocation of a single national number to any citizen is prohibited. 6. Everyone is guaranteed free access to public-use information technology networks. The law shall define the regime governing cross-border data flows, and the appropriate

salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei.	means for protecting both personal data and other data whose safeguarding is justified in the national interest. 7. Personal data contained in manual files enjoy the same protection as that provided for in the previous paragraphs, as laid down by law.
Declaração Universal dos Direitos Humanos Artigo 12.º Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.	Universal Declaration of Human Rights Article 12 No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Bibliography

English titles

Legislation

Declaration of Human Rights

Constitution of the Portuguese Republic

Law no. 67/98, from the 26th of October, the Law “On the Protection of Personal Data”

Law no. 58/2019, from the 8th of August, implementation, in the national legal order, of Regulation (EU) 2016/679 “On protection of individuals with regard to the processing of personal data and the free movement of such data”

Law no. 41/2004, of the 18th of August and Law no. 12/2005, of the 26th of January “On protection of personal data and privacy in telecommunications”

Reports

European Commission against Racism and Intolerance (ECRI) Report on Portugal 2018

NDPC Activity Report 2017-2018

Portuguese titles

Legislation

Constituição da República Portuguesa

Lei n.º 67/98, de 26 de Outubro, transpõe para a ordem jurídica portuguesa a Dir. n.º 95/46/CE, do PE e do Conselho, 24/10/95, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados

Lei n.º 58/2019 de 8 de Agosto, Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

Lei n.º 41/2004, de 18 de Agosto transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas

Reports

European Commission against Racism and Intolerance (ECRI) Report on Portugal 2018

NDPC Activity Report 2017-2018

ELSA ROMANIA

Contributors

National Coordinator

Iulia Mitrache

National Researchers

Alexandra Grieb

Ana-Anca Sampetean

Antonia Pîslariu

Bianca Elena Isache

Cătălin Panțiru

Diana Firincă

Raluca Crețu

Alexandra Rebeca Manea

National Linguistic Editors

Maria Duminică

Brândușa Enișor

National Technical Editors

Andreea Iordache

Raluca Elena Irimia

Introduction

The impact of the advanced digital technologies on human rights is of utmost importance as nowadays its implications are more and more present. Among current examples on ADT are: artificial intelligence, agents, speech and handwriting recognition, virtual reality and 3D visualisation, smart cards, real-time collaboration, enhanced user authentication, data mining, and knowledge management. Artificial Intelligence (AI)-driven technology is the one having the most impactful effects on human rights, therefore this report will refer mostly to it. ADT is entering everyone's everyday life: multiple new gadgets are being implemented by public authorities to monitor people's state of health, certain skills or to allocate resources. Innovation must be developed responsibly and taking the safeguard of fundamental rights in AI development must be the primary goal, as making decisions without prior knowledge can have multiple serious consequences for the human rights of individuals.

What one may wonder is whether AI is beneficial or harmful, as many technologies involving AI are still in their early stages and more time is needed in order to assess the implications thoroughly. Taking this into account, one shall start by presenting what AI is, keeping in mind that its development should be inspired by some strong principles such as: proportionality, responsibility, participation of people or transparency.

Currently, there is no agreed definition of 'Artificial Intelligence', therefore^[A1] one will illustrate a few for the purposes of this report in the following lines. 'AI is a broad field encompassing a variety of approaches that attempt to emulate human cognitive skills' Algorithms need not be software-in the broadest sense, they are encoded procedures for transforming input data into a desired output, based on specified calculations.⁸⁴⁶ The procedures name both a problem and the steps by which it should be solved.' (Gillespie 2014:167) Algorithms are thus perceived as 'a series of steps undertaken in order to solve a particular problem or accomplish a defined outcome.' (Diakopoulos 2015:400).⁸⁴⁷

Taking all these into consideration, this report will display the current relation between human rights and technology in Romania, given the following questions.

1. Which human rights issues does Advanced Digital Technologies(ADT) pose in your country?

⁸⁴⁶ "Artificial intelligence and data protection - Conseil de l'Europe."

<<https://edoc.coe.int/en/artificial-intelligence/8254-artificial-intelligence-and-data-protection.html>> accessed 16 February 2021.

⁸⁴⁷ "Algorithms and human rights - Study on the human rights"

<<https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html>> accessed 16 February 2021.

A common ‘Declaration on Cooperation on Artificial Intelligence’⁸⁴⁸ was adopted by The European Union member states in 2018. This Declaration emphasises the achievements and investments of Europe in AI as well as the progress towards the creation of a Digital Single Market. The Member States agree to cooperate on: Boosting Europe's technology and industrial capacity in AI and its uptake, including better access to public sector data; innovative business models and also creating economic growth and new qualified jobs; Addressing socio-economic challenges, such as the transformation of the labour markets and modernising Europe's education and training systems, including upskilling & reskilling EU citizens; Ensuring an adequate legal and ethical framework, building on EU fundamental rights and values, including privacy and protection of personal data, as well as principles such as transparency and accountability.

In 2019, the Council adopted the Coordinated Plan on Artificial Intelligence, stating the coordinates of the EU strategy regarding AI. Following these, Romania implemented the given directions in the Coordinated Plan on Artificial Intelligence in April 2019, regulating some draft documents that can be used by non-specialised persons, also giving some explanations on how to comply with such needs and hurdles, but online storage was not found.^{849, 850}

It is worth mentioning that Romania took part in organising the Digital Assembly in 2019, this forum being considered the most important European digital event of the year. Launching a European initiative on AI aims to prepare countries for socio-economic changes, to boost the EU's technological and industrial capacity with AI and to ensure an appropriate ethical and legal framework.

Non-compliant development and implementation of AI systems may lead to liability issues. Romania passed the Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Even though GDPR does not use the term ‘Artificial Intelligence’, an extensive interpretation of Article 22 could be used in that sense.^{851 852}

⁸⁴⁸ ‘EU Declaration on Cooperation on Artificial Intelligence | JRC’
<<https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence>> accessed 16 February 2021.

⁸⁴⁹ ‘Conclusions on the coordinated plan on artificial ... - European Union.’
<<https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf>>, accessed 22 May 2021.

⁸⁵⁰ Decision no. 15 (3 April 2019) <<http://legislatie.just.ro/Public/DetaliuDocument/212417>>, accessed 22 May 2021.

⁸⁵¹ Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679
<<https://www.dataprotection.ro/servlet/ViewDocument?id=1685>>, accessed 22 May 2021.

⁸⁵² GDPR, art. 22.

When discussing human rights in relation to Advanced Digital Technologies (ADT), Art. 22 of the General Regulation on Data Protection an example of regulations concerning AI. Article 22 forbids a machine to make a decision for a human being when juridical consequences may occur; it gives people the right to contest a decision and to ask for human assistance; Art. 22 as well as Articles 71-72 protect against the possible discrimination AI might make, assuring that AI can be implemented while avoiding an unwanted impact on human rights; these articles also protect children. Art. 13 states that one can ask about the technical process behind the algorithm and what the given protection is.⁸⁵³

The main instrument of the EU fundamental rights framework applicable to the use of AI is the Charter of Fundamental Rights of the European Union, together with the unwritten general principles of EU law. Fundamental rights can be also found in the European Convention on Human Rights. In the EU, Article 2 of the Treaty on the European Union (TEU) provides that non-discrimination is one of the fundamental values of the EU and Article 10 of the Treaty on the Functioning of the European Union (TFEU) requires the Union to combat discrimination on a number of grounds. Moreover, several EU non-discrimination directives regard more specific and detailed provisions, such as: the Employment Equality Directive (2000/78/EC), the Racial Equality Directive (2000/43/EC), the Gender Goods and Services Directive (2004/113/EC), and the Gender Equality Directive (2006/54/EC).

Using ADT may lead to human rights violations. As systems are becoming more complex and various connections are being established between machines, humans tend to be scared of the amount of new information, not knowing whether it is a beneficial growth or a harmful one. Human dignity, fair trial and due process, privacy and data protection, freedom of expression, healthcare, social rights and access to public services, consumer protection or the right to free elections are just some domains which can be affected when using AI. As an example, people need to be informed about the automated decisions that are being made, as they do not feel comfortable being subject to biometric identification systems. Freedom of expression or the right to free elections need to be granted as people need to think and shape their opinions in a free manner. Discrimination is also a very sensitive subject as the main purpose of ADT is to categorise, classify and separate. This process needs to be achieved without unjustified, unfair or differential treatment.⁸⁵⁴

⁸⁵³ The 'right to an explanation' under EU data protection law
<<https://medium.com/golden-data/what-rights-related-to-automated-decision-making-do-individuals-have-under-eu-data-protection-law-76f70370fcd0>>, accessed 22 May 2021.

⁸⁵⁴ Algorithms and human rights - Study on the human rights dimensions of automated data processing techniques and possible regulatory implications
<<https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html>>, accessed 22 May 2021.

2. How is personal information protected in your national legislation?

Personal data protection remains a new matter not only for the Romanian legal system, but for the European Union as well. On the 4th of May 2016, two normative acts were published in the Official Journal of the European Union. The first one was the EU Regulation no. 2016/679 regarding general data protection regulation and the free circulation of data with which the Regulation 95/46/CE was repealed (General Regulation concerning data protection). Furthermore, the EU Regulation no. 2016/679 updates the principles established two decades ago by Directive 95/46/EC. The second one is Directive no. 2016/680 dedicated to data protection within the specific activities of law enforcement authorities. As mentioned in the EU Regulation no. 2016/679, it is ‘intended to contribute to the accomplishment of an area of freedom, security and justice [...] to the strengthening and the convergence of the economies within the internal market, and to the wellbeing of natural persons’.⁸⁵⁵

In Romania, within the effect of Law no. 2005/102, the National Authority for the Supervision of Personal Data was established and its purpose is to guarantee the observance of the fundamental rights to privacy and the protection of personal data, established especially by Art. 7 and Art. 8 of the Charter of Fundamental Rights of the European Union, Art. 16 of the Treaty on the Functioning of the European Union (TFEU) and Art. 8 of the European Convention for Human Rights and Fundamental Freedoms.

The General Regulation on the Protection of Personal Data has direct applicability in all EU member states since the 25th of May 2018. Consequently, the Parliament of Romania passed Law no. 2018/190 which came into operation with the purpose of applying the EU Regulation mentioned above. It sets the necessary measures for the implementation at the national level, mainly, of the provisions of Art. 6 para. (2), Art. 9 para. (4), Art. 37-39, 42, 43, Art. 83 para. (7) and Art. 87-89 of the General Regulation on data protection. The law no. 2018/190 regulates, for example, work relationships, obligations arising from economic operators which use personal data, relations between a hospital unit, whether private or public, and a natural person *et caetera*.

In the beginning, Law 2018/190 provides definitions to terms and expressions such as national identification number, remediation plan, remedial measure, fulfilling a task that serves a public interest and so on. The second chapter (Special rules for the processing of certain categories of personal data) regulates aspects such as processing of genetic data, biometric data or health data. In this case, it is permitted only with the explicit consent of the data subject or if processing is carried out on the basis of express legal provisions, with

⁸⁵⁵ EU Regulation 2016/679, art. 2.

establishment of appropriate measures for the protection of rights, freedoms and legitimate interests of the data subject. Furthermore, the processing of certain categories of personal data cannot be performed later for other purposes by third parties.

The processing of a national identification number, including by collecting or the disclosure of the documents containing it can be made in the provided situations of Art. 6 para. (1) of the General Data Protection Regulation. The processing of a national identification number for the purpose provided in Art. 6 para. (1) let. f) of the General Regulation on data protection, respectively of implementing legitimate interests pursued by the operator or a third party, shall be carried out with the establishment of the following guarantees: the implementation of appropriate technical and organisational measures for compliance - in particular - with the principle of data minimisation, as well as to ensure security and confidentiality of data processing with personal information, according to the provisions of Art. 32 of the General Regulation on data protection; the appointment of a data protection officer, in accordance with the provisions of Art. 10 of this law; establishing storage deadlines depending on the nature of the data and the purpose of processing, as well as specific deadlines, in which personal data must be deleted or revised for deletion; regular training on the obligations incumbent on persons who, under the direct authority of the operating manager, processes personal data.

When it comes to processing personal data in the context of work relationships, it is allowed only when the legitimate interests pursued by the employer are duly justified and prevail over the interests or rights and freedoms of data subjects; the employer should make the mandatory prior information complete and in a manner explicit to the employees; the employer should consult the union or, as the case may be, the employees' representatives before the introduction of monitoring systems. Other less intrusive forms and ways to achieve the goal pursued by the employer have not previously proven effective; the duration of storage of personal data is proportional to the purpose of processing, but not more than 30 days, except in express cases regulated by law or duly justified cases.

As for the processing of personal and special data in the context of fulfilling a task that serves a public interest, if necessary, it should respect Art. 6 para. (1) let. e) and Art. 9 let. g) of the General Data protection regulation. This is done by the operator or by the third party in the following situations: the implementation of appropriate technical and organisational measures for observance of the principles listed in Art. 5 of the General Regulation on data protection, in particular data minimisation, respectively the principle of integrity and confidentiality. A data protection officer is appointed, if necessary, in accordance with Art. 10 of this law. They are in charge of setting storage deadlines depending on the nature of the data and the purpose of processing, as well as specific deadlines in which personal data must be deleted or revised with a view to deletion.

The only accepted exception is processing of personal data for journalistic purposes or for the purpose of academic, artistic or literary expression. In order to ensure a balance between the right to data protection, freedom of expression and the right to information, processing for journalistic purposes or for the purpose of academic, artistic or literary expression may be carried out if it concerns personal data which has been made public by the data subject or which is closely related to the quality of public personhood belonging to the data subject, the public nature of the matters in which they are involved, by way of derogation from the following chapters of the General Data Protection Regulation: Principles; The rights of the data subject; The operator and the person authorised by the operator; Transfers of personal data to third countries or international organisations; Independent supervisory authorities; Cooperation and coherence; Provisions regarding specific processing situations.

Regarding the processing of personal data for the purpose of scientific or historical research, for statistical purposes or for purposes of archiving for public interest, Articles 15, 16, 18 and 21 of the General Regulation on protection details do not apply. Derogations are necessary for the fulfillment of these purposes. Articles 15, 16, 18, 19, 20 and 21 of the General Regulation on data protection do not apply where personal data is processed for archiving purposes in the public interest, to the extent that the rights mentioned in these articles are likely to make it impossible or seriously affect the achievement of specific objectives and these derogations are necessary for the fulfillment of these purposes.

In order to ensure that proportionality and a balance between the right to protection of personal data and special data and processing of such data by political parties and citizens' organisations belonging to national minorities and non-governmental organisations will be achieved by: informing the data subject about the processing of personal data, guaranteeing the transparency of information, guaranteeing the right of rectification and deletion. Also, the processing of personal and special data is allowed to the parties, political organisations and citizens' organisations belonging to national minorities and non-governmental organisations, in order to achieve their objectives, without the express consent of the data subject, but provided that the guarantees correspond to the ones referred to in the preceding paragraph.

Operators and individuals authorised by the operator shall designate a responsible person for data protection in the situations and conditions provided in Art. 37-39 of the General Data Protection Regulation. If the operator or the person authorised by the operator is a public authority or a public body, as defined in Art. 2 para. (1) lit. a), a data protection officer may be appointed, unique for several of these authorities or bodies, taking into account organisational structures and their size. The activity and tasks of the data

protection officer shall be performed with compliance to the provisions of Art. 38 and 39 of the General Regulation on data protection and applicable national legal regulations.

Accreditation of certified bodies provided in Art. 43 of the General regulation on data protection is made by the Association of Accreditation from Romania - RENAR, as a national body of accreditation, in accordance with Regulation (EC) no. 765/2008 of the European Parliament and of the Council on the 9th of July 2008 establishing accreditation and market surveillance requirements with respect to marketing of products and repealing the Regulation (EEC) no. 339/93, published in the Official Journal of the European Union, series L, no. 218 from the 13th of August 2008, as well as in accordance with Government Ordinance no. 23/2009 regarding the accreditation activity of the evaluation bodies of compliance, approved with amendments by Law no. 256/2011. The certification bodies will be accredited according to the legal regulations applicable, in accordance with the European Standard-International Organization for Standardisation (EN-ISO)/International Electrotechnical Commission (IEC) 17065 standard and the requirements established by the National Supervisory Authority, as well as with compliance to the provisions of Art. 43 of the General Protection Regulation data.

When it comes to coercitive measures and sanctions, violation of the provisions listed in Art. 83 para. (4) - (6) of the Regulation data protection is a misdemeanor. The main contravention sanctions are the warning and the fine. Violation of the provisions of Art. 3-9 of this law constitutes a contravention and is sanctioned under the conditions provided in Art. 83 para. (5) of the Regulation general data protection law. The National Supervisory Authority in accordance with the provisions is competent to find the contraventions provided by the present law and apply the contravention sanctions, as well as other corrective measures provided by Art. 58 of the General Regulation on data protection. The general regulation on data protection, of Law no. 102/2005 on the establishment, organisation and functioning of the National Authority of Supervision of Personal Data Processing, with modifications and subsequent additions, and of this law.

As for authorities and public bodies, in case of finding a violation of the provisions of the General Regulation on protection of data and of this law by public authorities or bodies, the National Supervisory Authority shall draw up a report of the finding and sanctioning the contravention. The remediation term is established according to the associated risks processing, as well as the steps which are necessary to be performed for insurance processing conformities. Within 10 days from the date of expiry of the remediation period, the National Supervisory Authority may regain control. The responsibility for fulfilling the remedial measures rests with the public authority or body which, according to the law, bears the responsibility contravention for the facts found. The model of the remediation plan is annexed to the main body of this law.

If following the control provided in Art. 13 para. (3) it is found that public authorities have not fully implemented the measures provided in the remediation plan, the National Supervisory Authority - depending on the circumstances of each case - may apply a fine, taking into account the criteria set out in Art. 83 para. (2) of the General Data Protection Regulation. The violation by the public authorities or bodies constitutes a contravention of the following provisions of the General Data Protection Regulation, relating to the obligations of the operator and of the person empowered by the operator in accordance with the provisions of Art. 8, Art. 11, Art. 25-39, Art. 42 and 43; the obligations of the certification body in accordance with Art. 42 and 43; the obligations of the monitoring body in accordance with Art. 41 para. (4). The violation by the public authorities or bodies constitutes a contravention of the provisions of art. 3-9 of this law. The contraventions provided in par. (2) and (3) shall be sanctioned with a fine from 10.000RON up to 100.000RON. The violation by the public authorities constitutes a contravention of the following provisions of the General Data Protection Regulation, relating to the basic principles for processing, including the conditions regarding the consent, in accordance with Art. 5-7 and Art. 9; the rights of the persons concerned in accordance with Art. 12-22; transfers of personal data to a recipient in a third party country or an international organisation, in accordance with Art. 44-49; any obligations under national law adopted under chapter IX. Non-compliance with a decision or a temporary or permanent limitation on the processing or suspension of data flows, issued by the National Supervisory Authority pursuant to Art. 58 para. (2), or not granting access, by violating the provisions of Art. 58 para. (1). By derogation from the provisions of art. 8 para. (2) lit. a) of the Ordinance Government no. 2/2001 on the legal regime of contraventions, approved with amendments and completions by Law no. 180/2002, with modifications and subsequent completions, the contraventions presented in par. (5) shall be sanctioned with a fine from 10.000RON to 200.000RON. The infringement by public authorities or bodies is a contravention of a decision issued by the National Supervisory Authority in accordance with Art. 58 para. (2) in conjunction with Art. 83 para. (2) of the General Regulation on data protection. By derogation from the provisions of Art. 8 para. (2) lit. a) of the Ordinance Government no. 2/2002, as subsequently amended and supplemented, contraventions shown in para. (7) shall be sanctioned with a fine of 10.000RON up to 200.000RON.

In applying the provisions of Art. 58 para. (2) lit. b) of the General Regulation on data protection, Art. 142 para. (1) of Law no. 102/2005 regarding establishment, organisation and functioning of the National Supervisory Authority of Personal Data Processing, published in the Official Gazette of Romania, Part I, no. 391 on the 9th of May 2005, with amendments and completions, subsequent amendments shall stipulate as follows: the main penalties imposed by the National Supervisory Authority, according to Art. 58 para. (2) let.

b) and i) of the general data protection regulations are the warning and the fine. The application of the fine is made under the conditions of Art. 83 of the General Regulation on data protection.’

3. To which extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard?

Even though GDPR is still somewhat new in the Romanian legal system, its regulation in the national system had a great impact. Whether one considers the applications they download on the phone, the websites they access, be they public or private, prior consent of the processing of personal data is required everywhere. On the contrary, it would be at least bizarre that, by providing some of their personal data, one would not be asked for consent to their processing. For example, when one needs medical services, they are always asked for consent for the processing of personal data (phone number, ID card, email address etc.). Among the most common forms by which the authorities, institutions, economic operators *et caetera* request the agreement regarding the processing of personal data is the signing of a contract by which the natural person offers their consent, usually by handwritten signature.

Another example would be the moment an individual accesses a website and a pop-up notification with the so-called ‘cookie policy’ appears. By this notification, the site administrator notifies them that they need their express consent regarding the use of cookies. By agreeing, they give access to the particular site to install this so-called cookie, which aims to facilitate navigation on the site, browser and so on, as well as personalisation of a user's preferences. An example would be, of course, the agreement that applications require when one enters certain personal data. For example, social media applications, which require the user's consent regarding the terms and conditions, along with the notice detailing how personal data will be used.

Some more concrete examples of how the data protection is self-regulated in the private sector would be Law 506/2004 concerning data protection and private life protection in the electronic communications sector; Law 363/2018 on the protection of individuals regarding the processing of personal data by the competent authorities for the purpose of preventing, detecting, investigating, prosecuting and combating crimes or the execution of punishments, educational and security measures, as well as on their free movement data.

Law 2004/506 establishes the specific conditions for guaranteeing the right to privacy with regard to the processing of personal data in the electronic communications sector. The provisions of this law apply to the processing of personal data related to the provision of

electronic communications services to the public through public electronic communications networks, including public electronic communications networks involving data collection and identification devices. Even so, Law 2004/506 does not apply to the processing of personal data carried out within the activities in the field of national defense and national security, carried out within the limits and with the restrictions established by law or within the activities of combating crimes and maintaining public order, as well as within other activities in the field of criminal law, carried out within the limits and with the restrictions established by law.

Law 2018/363 aims to protect the fundamental rights and freedoms of individuals, in particular the right to protection of personal data.

4. What is the process of judicial review in cases of data protection breaches?

The right to data privacy in Romania is first and foremost instituted in our Constitution, as part of Article 26 dedicated to ‘Private and Family Life’. While no clear definition is given, due to its vast and complex nature and given the fact that the Constitution’s role is not to offer such definitions, this right was eventually nuanced in 2016, with the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council on the 27th of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).⁸⁵⁶

The Regulation grants multiple rights, so as to offer individuals efficient protection of their data: the right of access, the right to rectification, the right to erasure (also known as ‘the right to be forgotten’), the right to restriction of processing, the right to data portability, the right to object and last but not least, the right to avoid automated decision-making, including profiling. As a result of Romania being a Member State of the European Union, these rights are acknowledged in the national law system, due to EU Regulations being directly applicable. Hence, the data subject is given the possibility to restrict or object data processing, with the exception of certain situations, in which certain restrictions to these rights may apply. However, such restrictions must abide by certain prerequisite conditions, according to article 23 of the Regulation. First of all, the essence of the fundamental rights

⁸⁵⁶ Mihai Constantinescu, Antonie Iorgovan, Ioan Muraru, Elena Simina Tănăsescu, *The Constitution of Romania revised – comments and explanations* (ALL BECK Publishing, 2004) 49.

and freedoms must be ensured and respected. Second of all, such measures must be necessary and proportionate in a democratic society. Third of all, they must be imposed only to safeguard one or more of the fields expressly mentioned in the Regulation, such as national and public security, defence, enforcement of civil law claims and so on. Lastly, any restrictions imposed through legislation must ensure adequate provisions, regarding, but not limited to, the purpose or categories of processing, the scope of the restriction, safeguards to prevent abuse or even storage periods.

Furthermore, a personal data breach, according to Art. 4 para. 12 of the Regulation, is considered to be a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. 'Destruction' is to be understood as the situations in which the personal data does not exist anymore, while 'damage' indicates there was an alteration, corruption of the personal data in case, or that it is no longer complete. 'Loss' refers to the cases in which personal data still exists, but it is no longer in the possession of the natural or legal person, public authority, agency or other body which determines the purposes and means of its processing. Lastly, unauthorised or unlawful processing includes the disclosure of such personal data to recipients who are not authorised to receive or access it, or other methods of processing which are not in accordance with General Data Protection Regulation (GDPR).⁸⁵⁷ It must be noted that such breaches may be accidental, in which case the controller shall still be held liable.

Furthermore, we shall keep in mind that any personal data breach is a type of a security incident, but not all security incidents are necessarily a personal data breach.⁸⁵⁸ The distinction lies in whether or not there is a breach of personal data and is important as only breaches which refer to such data fall under the provisions of Articles 33 and 34 of the GDPR, whereas 'regular' security incidents do not. Moreover, a security incident is not to be restrictively understood as an external intrusion, but also includes incidents from internal processing that breach security principles.⁸⁵⁹

Thus, in case of a 'personal data breach', the controller shall notify, first of all, the supervisory authority that is competent, without delay and no later than 72 hours after having become aware of a breach regarding personal data. In Romania, this authority is the National Supervisory Authority for Personal Data Processing. The moment when a controller becomes 'aware' of a breach that could likely result in a risk to the rights and freedoms of natural persons will highly depend on the specific circumstances of each

⁸⁵⁷ Guidelines on Personal data breach notification under Regulation 2016/679 by the Article 29 Data Protection Working Party.

⁸⁵⁸ Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018 Brussels, 24.1.2018 COM (2018) 43 final.

⁸⁵⁹ Guidelines on Personal data breach notification under Regulation 2016/679 (n 858).

incident. However, controllers are granted a limited amount of time to investigate whether or not it is the case to take further action and notify the competent authority. Even more so, if a company or organisation is merely a processor, then it must notify each and every data breach to the data controller without undue delay.

Furthermore, Article 34 of the Regulation states that ‘when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject’. This rule is also subject to a few exemptions: the breach is unlikely to result in a high risk for the rights and freedoms of data subjects, due to subsequent measures taken by the controller; appropriate technical and organisational protection were in place at the time of the incident and in regards to the data in case; or this would suppose disproportionate efforts and would rather be a form of public communication or another effective measure of informing data subjects. Great caution and examination must be taken so as the responsible individuals with data processing do not abuse these exemptions. Under no circumstance should they be interpreted as an excuse in order to bypass GDPR requirements, but rather a way to make requirements flexible and facile to put in practice.

Finally, in order to bring a personal data breach case before a national court, we must take into consideration the ‘data processor or controller’, as well as ‘the data subject’. On the one hand, from the perspective of the former stakeholders, Law no. 102/2005 on the set up, organisation and functioning of the National Supervisory Authority for Personal Data Processing in Articles 17 and 23, grants the possibility to challenge the ‘reports of the finding/sanctioning and/or the decision to apply the corrective measures, as the case may be’ issued by the National Supervisory Authority for Personal Data Processing before the competent national court. On the other hand, the data subject may stand before national courts in order to defend their data privacy rights, which have been infringed, as an alternative to addressing a complaint to the National Supervisory Authority (further referred to as ‘the NSA’)⁸⁶⁰ or in case of non-observance of its duties by the NSA, after addressing a complaint.⁸⁶¹ Additionally, the data subject acquires the quality of claimant, should they approve the action notified by the NSA in accordance with the provisions of article 22 or should they suffer any material or non-material damage as a result of an

⁸⁶⁰ Law no. 102/2005 on the set up, organisation and functioning of the National Supervisory Authority for Personal Data Processing - Republished, art. 24 (1).

⁸⁶¹ Law no. 102/2005 on the set up, organisation and functioning of the National Supervisory Authority for Personal Data Processing (n 861), art. 21 (6).

infringement of the rights protected under GDPR, in order to receive compensation, this being the only way to do so.^{862 863}

5. Does the review constitute effective protection of data privacy?

The Charter of Fundamental Rights of the European Union (further referred to as ‘the Charter’) protects all rights enshrined in the European Convention on Human Rights (further referred to as ‘the Convention’) and even certain additional ones. As Romania is both a member of the European Union and the Council of Europe, both the Charter and the Convention are binding. However, regarding the enforcement of those rights, there are certain relevant differences which must be brought into attention. The European Court of Human Rights in Strasbourg is the specific court mandated to ensure that states comply with the obligations deriving from the Convention. Individuals who deem one of their rights under the Convention has been violated can apply directly to the Court, if certain conditions of admissibility are satisfied. For the Charter, then again, there is no comparable international court. There is no possibility for EU citizens to apply directly to an international court, should they consider any right of theirs, which is protected under the Charter, has been violated. Moreover, even the preamble of the Charter expressly refers to the Convention and to the jurisprudence of the European Court of Human Rights, stating that the Charter reaffirms the rights resulting from the Convention. Furthermore, the Charter also states that it must not be interpreted as limiting rights which are guaranteed by the Convention, thus making the latter a minimum standard.⁸⁶⁴

For all the aforementioned reasons and bearing in mind the possibilities of standing in court of both the processor/controller and the data subject presented above, in Question 4, they shall be examined in light of the European Court of Human Rights Case-Law on Article 6 § 1 and Article 13 of the Convention, which grant the ‘right to a fair trial’, respectively the ‘right to an effective remedy’.

First of all, in accordance with Article 13, which stands as a *lex generalis*, the remedy must be capable of directly elucidating the impugned situation, for it to be considered effective.⁸⁶⁵ Moreover, the term ‘effective’ means that the remedy must be sufficient and accessible,

⁸⁶² ‘...following the exercise of its legal powers, the National Supervisory Authority considers that any of the rights of the data subjects guaranteed by the legal regulations in the field of personal data protection have been infringed, it may notify the competent court, according to the law.’

⁸⁶³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Article 82 and repealing Directive 95/46/EC (General Data Protection Regulation) in conjunction with articles 1349, 1357, 1358, 1382, 1385, 1386 of the Romanian New Civil Code.

⁸⁶⁴ Holger Hembach, The difference between the ECHR and the EU Charter of Fundamental Rights, <<https://www.youtube.com/watch?v=3Q4i1ev4fI4>>, accessed 15 May 2021.

⁸⁶⁵ *Pine Valley Developments Ltd. And Others v Ireland* App no 12742/87 (Commission Decision, 3 May 1989).

fulfilling the obligation of promptness.⁸⁶⁶ In the Romanian legislation, there are no excessively restrictive requirements and the remedies are facile for the person concerned, bearing in mind the interests of each party involved. *Post hoc* remedies may suffice to be fruitful, such in the case of *M.S. v. Sweden*, which concerned the disclosure without the patient's consent of confidential personal and medical data by one public authority to another.⁸⁶⁷

A realistic account must be taken not only of the existence of formal remedies in the legal system of the country, as the remedy required by Article 13 must be 'effective' in practice as well as in law.^{868, 869}

Second of all, Article 6 § 1 of the Convention is a *lex specialis* in relation to Article 13 which, as a rule, is not applicable where the alleged violation of the Convention has taken place in the context of judicial proceedings, with the only exception of the right to trial within a reasonable time.⁸⁷⁰ Thus the correct interpretation of Article 13 is that that provision guarantees an effective remedy before a national authority for an alleged breach of the requirement under Article 6 § 1 to hear a case within a reasonable time.⁸⁷¹ A very important principle instituted through Article 6 is 'the right to court', which implies that the claims must be capable of being submitted to a judge for an effective judicial review, a principle which is respected in this specific case. Both the organisation and composition of the court, and the conduct of the proceedings. In sum, the whole makes up the right to a fair hearing.^{872, 873}

Hence, the efficacy of the remedy remains to be assessed *in concreto*, as each case may vary, depending on the circumstances. Therefore, at least *prima facie*, the judicial remedies provided by the Romanian legislation appear to be effective in law, as they are capable of directly solving various and specific situations.⁸⁷⁴ This is also reflected in the sanctions and penalties provided in the Regulation, which are directly applicable in the national law.⁸⁷⁵ In addition, alongside the constant adaptation to GDPR, the aforementioned penalties seem to appear more and more in the practical world. However, they are mainly applied by the National Security Agency (NSA), since not many organisations seem to challenge reports, nor do data subjects claim infringements in their rights, most likely due to the novelty of this field. There is indeed an interesting case-law in which the national court granted the

⁸⁶⁶ *Çelik and İmret v. Turkey* App no 44093/98 (ECtHR, 5 October 2004) [59].

⁸⁶⁷ App no 20837/92 (Commission Decision, 27 August 1997) [55-56].

⁸⁶⁸ *A.B. v. the Netherlands* App no 37328/97 (ECtHR, 8 January 2002) [98].

⁸⁶⁹ *İlhan v. Turkey [GC]* App no 22277/93 (ECtHR, 27 June 2000) [97].

⁸⁷⁰ *Menesheva v. Russia* App no. 59261/00 (ECtHR, 9 March 2006) [105].

⁸⁷¹ *Kudła v. Poland* App no. 30210/96 (ECtHR, 26 October 2000) [156].

⁸⁷² *Fayed v. The United Kingdom* App no. 17101/90 (ECtHR, 21 September 1994) [65].

⁸⁷³ *Golder v. The United Kingdom* App no. 4451/70 (ECtHR, 21 February 1975) [36].

⁸⁷⁴ *Colozza and Rubinat v. Italy* App nos 9024/80 & 9317/81 (Commission decision, 9 July 1982).

⁸⁷⁵ GDPR, art. 83.

claimant a little over 2.000€ in compensation for having personal data, such as their address and their ID card data posted on a company's website.⁸⁷⁶ Hence, penalties seem to be applied effectively, proportionally and dauntingly, with a yet to expand case-law.⁸⁷⁷

6. What is the process of judicial review of anti-discrimination cases?

6.1. Which bodies conduct such reviews

There are multiple bodies that are responsible for reviewing discrimination cases, depending on the purpose of the complaint (what the result that the complainant wants to obtain is) and on the areas where discrimination may occur. For example, work-related discrimination issues could be addressed to the labour inspection. If any kind of behaviour which could be qualified as incitement to hatred has been broadcasted, the National Audiovisual Council of Romania may be noticed and be in charge of reviewing the respective matter.

The most important bodies are the National Council for Combating Discrimination, the People's Advocate (the Romanian Ombudsman) and the courts.

The National Council for Combating Discrimination is an autonomous state authority, under parliamentary control. It was established through the Government Order no. 137/2000 with the purpose of establishing the right order when it comes to anti-discrimination. Its role is to guarantee the observance and application of the principle of non-discrimination, in accordance with the domestic legislation in force and with the international documents Romania is a part of.⁸⁷⁸ Besides the reviewing of discrimination cases, the Council is responsible for the Government's policy in the field of discrimination. Its most important attribution is to investigate, find and sanction acts of discrimination. In order to analyse cases as correctly as possible and to take decisions in the case of received petitions or self-referrals, the Board of Directors has at their disposal measures to investigate cases, followed by whether it finds the existence of discrimination and, if necessary, its sanction. The Council also monitors the repercussions of discrimination cases through the subsequent supervision of the parties involved.⁸⁷⁹

Since said acts of discrimination, as described by the previously mentioned law, may attract the disciplinary liability of the perpetrator, the Council can impose fines from 1.000 to 30.000RON for natural persons and 2.000 to 10.000RON for legal entities.⁸⁸⁰

⁸⁷⁶ Sector 5 Bucureşti Civil Court decision no. 747/2019.

⁸⁷⁷ GDPR, art. 84.

⁸⁷⁸ The Government Ordinance no. 137/2000, art. 19.

⁸⁷⁹ 'General presentation' <<https://www.cncd.ro/despre-cncd-prezentare-general/>>, accessed 5 March 2021.

⁸⁸⁰ The Government Ordinance no.137/2000, art. 26.

Mediation of discrimination cases is made in the presence of the representatives of the National Council for Combating Discrimination (NCCD) and the parties involved in the case. The National Council for Combating Discrimination seeks to reduce and eliminate acts of discrimination and not to impose fines.

The People's Advocate is organised and operates in Romania exercising a general mandate of defence of the rights and freedoms of individuals in their relations, especially with public authorities. Hence, a person will address the People's Advocate in regards with a discrimination case arising from their relations with a public authority.

The People's Advocate is accountable only to the Parliament, a responsibility that materialises through the obligation to submit reports. It exercises its duties either *ex officio* or at the request of the persons aggrieved in their rights and freedoms, within the limits established by law. The Constitution obliges the public authorities to provide the People's Advocate with the necessary support in the exercise of its duties. The Ombudsman's work is complementary to that of the courts. Unlike courts, the Ombudsman draws on its experience dealing with individual complaints to identify and report systemic problems in the public administration.

Although both NCCD and the People's Advocate provide effective protection against discrimination by sanctioning either natural or legal entities and public authorities, in order for the subjects of discrimination to get civil remedies such as: compensation, restoration of the previous situation or to order the cancellation of the situation that was established through discrimination, they still need to address the courts. Discriminated people have the right to address the court and to request the previously mentioned remedies on the basis of the rules regarding tort liability, established through the Civil Code.^{881 882} The previous submission of a referral to the National Council for Combating Discrimination is not needed in order to address the courts but the Council will be *subpoena*-ed *ex officio* by the court.

6.2. What are the elements that are taken into consideration when such review is conducted?

According to the article 2(1) of the Governance Order no. 137/2000, discrimination means any difference, exclusion, restriction or preference based on race, nationality, ethnicity, language, religion, social category, sex, sexual orientation, age, disability, chronic non-communicable disease, HIV infection, membership in a disadvantaged category, as well as any other criteria that has, as its purpose or effect, the restriction, removal of the recognition, use of exercise on equal terms, of human rights and fundamental freedoms or

⁸⁸¹ <<https://www.antidiscriminare.ro/instanta-de-judecata>>, accessed 5 March 2021.

⁸⁸² Romanian Civil Code, artt. 1349.

of rights recognised by law, in the political, economic, social and cultural sphere or in any other sphere of public life. Thus, according to the NCCD, discrimination is a differentiation based on a criteria which jeopardises a right.

The elements that are taken into consideration when such review is conducted are: the comparison between two situations and the positive relationship between the criteria claimed by the complainant and the facts reported.⁸⁸³

6.3. Does the review constitute effective protection against discrimination?

According to the European Commission against Racism and Intolerance (ECRI) report for 2019, the Romanian legislation provides easily reachable legal proceedings, including conciliation, in matters regarding discrimination.⁸⁸⁴ The 2019 activity report of the National Council for Combating Discrimination shows that the number of referrals has increased annually since 2017.⁸⁸⁵ Nonetheless, the same ECRI report that was previously mentioned shows that the victims of hate speech are rather pessimistic about the legal assurances and the competence of institutions when it comes to having their cases investigated. Therefore, although there are multiple bodies that can address discrimination cases, the referrals are easy to submit and the number of them increases annually, the review is not currently perceived by the most victims of discrimination as being an effective legal protection because it is either not trusted or not prominent enough. These issues, as ECRI concludes, could be solved only by means of educating the right holders.

6.4 What is a considered role of the technical aspects that result in discrimination (such as algorithmic bias)? How are these problems tackled?

There is still no information available regarding the implementation of artificial intelligence or other kinds of technology-driven machines by Romanian legal entities or public authorities in fields such as employment, that could eventually lead to discrimination of any kind. When it comes to discrimination and artificial intelligence, an example presented in the 2019 study⁸⁸⁶ made by the Council of Europe - 'Discrimination, artificial intelligence, and algorithmic decision-making' - could make us better understand what discrimination resulting from the use of technology could look like, that of an automated recruitment process, that could lead to consequential discrimination against certain disadvantaged

⁸⁸³ Government Ordinance no. 137/2000, art. 1(3).

⁸⁸⁴ ECRI Report on Romania <<https://rm.coe.int/fifth-report-on-romania/168094c9e5>>, accessed 5 March 2021.

⁸⁸⁵ Activity Report, National Council for Combating Discrimination <<https://www.cncd.ro/wp-content/uploads/2021/01/activity-report-cncd-2019.pdf>>, accessed 5 March 2021.

⁸⁸⁶ Frederik Zuiderveen Borgesius, *Discrimination, artificial intelligence, and algorithmic decision-making* (Directorate General of Democracy © Council of Europe 2018) <<https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>>, accessed 5 March 2021.

groups, making it harder for them to fulfill the criteria imposed by the employer, in comparison to other people. The intention of the employer in the given example was not that of discrimination between certain groups of people but rather that of objectively selecting the best qualities of an employee, such as ‘not being late for work’. This automatically resulted in the outcome that people from immigrant neighbourhoods were never selected for a job, because of their neighbourhoods being far away from the economical centre of the city. As previously stated, we haven’t yet implemented algorithmic decision-making (or, at least, this fact is not publicly known), therefore there is no data of discrimination based on technical aspects.

7. Does your country have any specific regulations on advanced digital technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?

7.1. Please specify any existing or proposed legislation. If none is in place, are there any initiatives introduced by private actors or NGOs?

Advanced digital technologies represent a real challenge for the legislative branch all over the world because of their constant changes and fast evolution, but more importantly since it is one of the youngest fields of research. Therefore, the pieces of legislation get constantly amended as the everyday groundbreaking discoveries of new technologies need to be regulated so that any abuses or infringements of human rights are avoided, as was the case with Cambridge Analytica.⁸⁸⁷

Romania’s case is not far from this reality. There is a significant lack of political will to actively regulate the use of advanced digital technologies, particularly because it does not represent a top priority in the legislative agenda. Most regulations that currently exist in Romania are amendments of the current legislation, statements that indicate the alignment of Romania’s stance in this manner with the one of the European Union, and the legislation that is adopted in the EU and implemented in all member states, as it happened with the GDPR.⁸⁸⁸

When it comes to the Internet of Things (IoT), we could easily say that there is a scarcity of legislation, particularly for two reasons. The first would be the high level of digital illiteracy that exists in Romania, which makes the population doubt the benefits of fast digitalisation in society. As a side analysis, 40% of the Romanian population sees the

⁸⁸⁷ The Guardian, ‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’ <<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>>, accessed 5 March 2021.

⁸⁸⁸ Decision no. 28 (9 September 2021) <<http://legislatie.just.ro/Public/DetaliuDocument/229861>>, accessed 22 May 2021.

implementation of 5G technology in the country with a high level of skepticism. The second reason would be from a social and economical perspective. Since the vast majority of the Romanian population has a small or average family income, and the IoT is a quite expensive technology, only 4% of the population used this kind of technology, and only 22% of them heard about the IoT.⁸⁸⁹ Therefore, the IoT is currently unappealing to Romanian society, and therefore, not calling out for urgent regulation.

However, the Romanian Government was not completely absent in this regard. In 2019 the 'Romanian Strategy for the implementation of 5G' was created, together with an inter-institutional workgroup. This Group has the purpose to identify and propose solutions to ensure the long-term development of the electronic communications network. One of the first regulations in regards to Big Data was Law no. 677 of the 21st of November 2001, which had stipulations regarding the processing of personal data and the free movement of such data.⁸⁹⁰ However, we cannot assume that it was implemented explicitly to create a legal framework for the use of data by artificial intelligence or international corporations. This law served as a preventive element since it was rather designed to serve as a tool for the protection of the private life of individuals at that time, a right which is explicitly stipulated both in the Romanian Constitution and in the European Convention of Human Rights.

This law was revoked in 2018, when the General Data Protection Regulation entered into force, which is currently the most important piece of legislation in Romania in the matter of Big Data.

The methodology from the 22nd of December 2017 of cryptographic products establishes the general framework for the evaluation and certification, ensuring unity in this process. Its main purpose is to establish the level of trust in the security functions of cryptographic products and systems. To achieve this, the following cryptographic solutions are subject to evaluation: hardware, software, firmware components and other components necessary for the realisation of the testing infrastructure.

Encryption is also vaguely regulated in the 362nd Article of the Romanian Criminal Code: 'Disruption of the functioning of information systems' which generally states that the unrighteous disruption of any information system, including encryptions, is punishable with 2 to 7 years of imprisonment.

⁸⁸⁹ Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM), '34% of the population knows what 5G is, and 22% have heard about the Internet of Things (IoT)' <<https://www.ancom.ro/34-din-populatie-stie-ce-este-5g-iar-22-a-auzit-de-internetul-obiectelor-iiot- 6080>> accessed 4 March 2021.

⁸⁹⁰ Law no. 677/2001.

In 2019, Law no. 30/2019 entered into force and completed the new Fiscal Code by adding regulations regarding virtual currencies among others.⁸⁹¹ The first amendment that is relevant for this report modifies Article no. 114 - 'Defining revenues from other sources in the tax code' by adding the revenues that came from cryptocurrency transactions. The second one adds to Article 116 the following stipulation 'Earnings below the level of 200 RON/transaction are not taxed only if the total earnings in a fiscal year do not exceed the level of 600 RON'.

The Research Institute for Artificial Intelligence was created in 2002, after the Government Ordinance no. 695 from 2002 entered into force, under the subordination of the Romanian Academy, fact that changed in 2012, when another Government Ordinance was created with the purpose to change the name of the institution from the aforementioned one into 'The Research Institute for Artificial Intelligence "Mihai Drăgănescu"'. This institution conducts research into the following key areas: 1) artificial intelligence - machine learning, natural language processing and conceptual and cognitive modelling, intelligent agents and the likewise; 2) society knowledge - knowledge management, modelling of infrastructures and processes of society, based on knowledge and cognitive scenarios; 3) new computer network architectures - self-organising systems.⁸⁹²

Aside from this Institution, in Romania there are certain legislative initiatives that have the final goal to crystallise and enforce the legal framework of Artificial Intelligence, such as AI4RO and Open Legislation.

The AI4RO appeared at the initiative of from Dragoș Preda, the Secretary of State for Communications and aims to support the development of Artificial Intelligence in Romania, by encouraging advanced research in the field of AI and the development of it in a responsible manner, weighting the upsides and the downsides of large-scale implementation of this technology without infringing the fundamental human rights and freedoms of individuals.

AI4RO revolves around a couple of fundamental principles. Those principles include constant consideration for the risks of AI that may affect fundamental human rights and freedoms, introducing and promoting the concept of digital data governance, extensive attention to the side effects of AI for the Romanian labor market, and the capitalisation of Romania's advantages in the technological field, such as a consistent base of hardware and software engineers, and the advanced internet infrastructure.

The working group of this project stands for the creation of a whitepaper on Artificial Intelligence in Romania, building the foundation of a national AI strategy for the country.

⁸⁹¹ Law no. 30/2019.

⁸⁹² <<http://legislatie.just.ro/Public/DetaliiDocument/37314>>, accessed 5 March 2021.

Another project which aims to have a significant impact in the domain of AI comes this time from an NGO, more specifically, from ELSA Bucharest. Open Legislation seeks to bring to the attention of the public eye the notion of ‘artificial intelligence’ and to prove the significant impact it has on our daily lives.

Having as a final goal to create a legislative draft that would be subsequently proposed to the political alliances in the Romanian Parliament, Open Legislation will bring together some of the best 20 law students with some influential private entities that have high expertise in this and other related fields.

7.2 To what extent are the external legislative developments influential on your country’s regulation of this area?

As a member of the European Union, both primary and derived law of the Union has a significant influence on national law, especially since derivative law prevails over national rules.

But if in other areas of interest we could see an overlap between the national interests and the ones of the EU, in the field of Artificial Intelligence the Romanian Government has generally integrated the stance of the organisation in its own national stance.

One event that shows Romania’s commitment to the Union’s mission to reach excellency in this domain is the adoption of the Decision No. 51 of 19 September 2018.

This decision is important as it proves that the Romanian Government understands the importance of evaluating the initiatives of the European Commission in this area, considering that the Artificial Intelligence could have substantial effects over areas of huge interest for the European Union such as energy, education, automation of the workplace, competition law and its possible destructive effect to be used in order to create deep fakes.⁸⁹³

On a similar note, Government’s decision No. 28 of 09 September 2020 supplemented the previous one, but this time with a particular and extremely relevant focus on human rights and consumers rights, on how the civil society can be supported in order to create more initiatives that could familiarise the general population with this technology, and on how more hubs that could the exchange of information between private actors.

⁸⁹³ What is a deepfake? <<https://www.businessinsider.com/what-is-deepfake>>, accessed 15 May 2021.

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?

8.1. Code of Criminal Procedure

Romania's Code of Criminal Procedure was adopted on the 15th of July 2010, which makes it new enough to provide rules regarding informational surveillance and computer tracking, but old enough to not provide rules regarding the many situations that the informational surveillance can now take form in, including the decryption of personal messages.

In the 5th Title of the General Part of the Romanian Code of Criminal Procedure entitled 'Evidence, means of proof and probative procedures' we find article 138, which provides the general analysis of the special procedures of surveillance such as the interception of communications or any type of remote communication and the access to an informational system. The Code doesn't specify which type of communication or informational system we can apply it to or if it excludes personal messages, so it is necessary to use a larger form of interpretation and assume it applies to all forms of communications by using the principle of '*ubi lex non distinguit, nec nos distinguere debemus*' ('where law does not distinguish, neither should we distinguish'). The Code specifies in Article 139 in which cases this technical surveillance can be requested by the prosecutor and ordered by the judge: crimes against national security; drug or other psychoactive substances trafficking; offences relating to non-compliance with the weapon regime, ammunition, nuclear materials, explosive materials; terrorism; human trafficking; money laundering and counterfeiting; crimes committed through informational systems; rape; blackmail; deprivation of liberty; corruption; tax evasion or any other crime to which the law provides a prison sentence of five years or more. This technical surveillance can be ordered by the judge of rights and freedoms at the request of the prosecutor during the prosecution. The judge can take the decision to order technical surveillance only if there is a reasonable suspicion about the preparation or perpetration of a criminal offence; the measure must be proportionate to the restriction of this fundamental right or freedom and the evidence could not be obtained otherwise or obtaining it would entail particular difficulties that would prejudice the investigation or there would be a danger to the safety of persons or valuables. This measure can be taken for a maximum of 30 days during the prosecution, but it can be extended if motivated. The prosecutor can order this measure as well, but only for 48 hours and only if the urgency is motivated. Criminal investigators can make copies of all information and communications received. The supervised person must be informed of the technical surveillance at least ten days after the measure ended and the defendant can also ask to see all the evidence that the prosecutor received after the supervision. The judge of rights and freedoms can, as well, order the preservation of personal data from

public providers of communications networks. Everything mentioned above applies to the informational search that is described in Article 168.

We can observe that an inter-institutional control is exerted between the prosecutor and the judge of rights and freedoms, as well as an authority control whenever the supervised person uses an appeal to remove the evidence extracted by technical surveillance, if the evidence was illegally or unfairly administered.

8.2. Inter-Institutional cooperation protocol

In 2006 and 2016, *Parquetul de pe lângă Înalta Curte de Casație și Justiție* ('The Public Prosecutor's Office attached to the Supreme Court') signed a cooperation protocol with *Serviciul Român de Informații* ('The Romanian Intelligence Service') where agents of the Romanian Intelligence Service were allowed to make procedural acts in place of the prosecutors. Both were partially declared unconstitutional by *Curtea Constituțională a României* ('Romanian Constitutional Court') because prosecutors are not allowed to delegate the power of issuing procedural acts to authorities that are not already empowered by law to issuing them, affecting the principle of separation of powers in the state (only the Parliament is allowed to give such delegations). However, prosecutors are allowed to delegate the power of making administrative acts to the intelligence agents. The Constitutional Court concluded that this legal matter will be judged case by case to see if the evidence administered is illegally obtained or not.⁸⁹⁴

What is relevant to this case is the position that the Public Prosecutor's Office took. Its arguments were based on the advanced technologies that the Romanian Intelligence Service uses in listening to and interpreting different types of communications. It was argued that the prosecution would be simplified if the intelligence agents' abilities and their devices were to be used in listening and understanding the communications and the messages of different defendants.

The protocol signed in 2016 is still in force, but with the amendments added by the Constitutional Court.

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?

9.1. Introduction

The Internet and its accessibility are not yet officially considered to be part of human rights, however both national and international legislatures regard it as a contemporary

⁸⁹⁴ Decision of the Romanian Constitutional Court no. 26/2019.

condition and catalyst for freedom of expression and access to information. So, countries nowadays have to face the challenge of allowing digital and technological progress but, at the same time, ensuring the adjustment and protection of human rights in the online world. In order to analyse this matter in regards to its efficiency and balance in Romanian legislation, we will first address the digital development over the past years in Romania, and secondly, the implementation of human rights safeguarding regulations regarding IT domains.

9.2. Digital Advancement in Romania

The Digital Economy and Society Index (DESI) is a marker created by the European Commission that sums up the most important factors regarding Europe's digital conduct and tracks the development of EU Member States, across five domains: 'Connectivity, Human Capital, Use of Internet, Integration of Digital Technology, Digital Public Services'.⁸⁹⁵

In 2020, Romania scored 40 on The Digital Economy and Society Index, whereas the European Average had an average of 52,6- ranking Romania the 26th out of 28 EU Member states.

As indicated by the DESI report in 2020, Romania's state was the same in four of the five DESI estimated measurements (based on information prior to the COVID-19 pandemic). This is because of the slow digital advancement overall, intensified by the political turn of events, as Romania has had four distinct governments in the course of the last 3 years. Romania performs best on the Connectivity measurement (Romania's score: 56.2, EU score: 50.1), thanks to the great take-up of ultrafast broadband and the wide accessibility of fixed high-capacity networks, particularly in urban regions. As much as 49% of Romanian homes buy into ultrafast broadband, the fifth most elevated figure in the EU. Be that as it may, digitalisation of the economy falls behind, right around one fifth of Romanians have never utilised the web, and not even a third have at any rate essential digital abilities. Romania is very well situated in regards to Information and Technology (ICT) graduates, as it positions fifth, with 5.6% of all its graduates, whereas the EU has an average of 3.6% graduates. However, on Digital public services and on Use of internet services, Romania has the most reduced execution among the EU Member States.⁸⁹⁶

9.3. Protection of human rights online

9.3.1. Access and non-discrimination

⁸⁹⁵ European Commission, DESI Report 2020,

<<https://ec.europa.eu/digital-single-market/en/scoreboard/romania>>, accessed 5 March 2021.

⁸⁹⁶ *ibid.*

Access to the Internet is a significant means for people to exercise their rights and freedoms and to participate in democracy. Internet access ought to be affordable and non-discriminatory. Everyone should therefore have access to the Internet, unless decided otherwise by a court.

According to the National Strategy for the Romania Digital Agenda 2020 (put in order by the Government Decision no. 245 on the 7th of April 2015), one of the main goals was for over 60% of the population to use the Internet regularly - a goal which according to the DESI report might have been reached, as only 20% of the population has never used the Internet.^{897, 898}

9.3.2. Freedom of expression and information

Seeking, receiving and sharing information and ideas without interference and regardless of frontiers should be seen as a modern fundamental right. People should have the possibility and liberty to express themselves online and to access information and the opinions of others. Censorship may only occur with information or content which promotes hatred, discrimination or violence. While freedom of expression and information are guaranteed by the Constitution or by national legislation, their protection and censorship are not as particularly regulated. There is no specific policy concerning issues such as cyberbullying, hate speech censorship, fake news censorship, not even mentioning the lack of monitoring of the algorithmic predictions of user preferences by search engines which might create informational 'bubbles' amongst various groups of people.

9.3.3. Freedom of assembly, association and participation

People have the right to peacefully gather with others on the World Wide Web. People also ought to have the right to protest in a civilised and respectful manner online. Nonetheless, Internet-users should ensure that their online assemblies do not prompt blockages, disruption of network or harm the property of others.

9.3.4. Privacy and data protection

One has the right to their private life on the Internet which contains the protection of their personal information, data and correspondence, in regard to their confidentiality.⁸⁹⁹

⁸⁹⁷ National Strategy for the Romania Digital Agenda 2020, <<https://www.comunicatii.gov.ro/agenda-digitala-pentru-romania-2020/>>, accessed 5 March 2021.

⁸⁹⁸ European Commission, DESI Report 2020 (n 896).

⁸⁹⁹ EU Regulation no. 2016/679.

There is an obligation, for both public authorities and privately-owned companies, to respect specific standards and procedures when they process personal data.⁹⁰⁰ Therefore, personal data can only be processed when explicitly allowed by users.

An individual's personal data should only be processed when specifically stated by law or when they have expressed their consent.

GDPR clauses (such as the ones contained in the EU Regulation no. 679/2018) have been transposed into national legislation within Law no. 190 from the 18th of July 2018.

Looking at the number of GDPR-related complaints and fines in Romania from 2019 and 2020, one might conclude that these clauses are well respected and protected, as there have been 6193 complaints in 2019 and 5480 in 2020 - resulting in a quantum of 2.339.291RON (approximately 480.000€) worth of fines in 2019 and 892.115RON (approximately 180.000€) in 2020.⁹⁰¹

9.3.5. Education and literacy

Another human right also facilitated by the Internet is the right to education, including access to knowledge.

People should have online access to education and to cultural, scientific, scholarly and other content in their respective languages.

These rights and liberties are pursued by the Romanian Government in the aforementioned National Strategy for the Romania Digital Agenda 2020 (put in order by the Government Decision no. 245 on the 7th of April 2015), as another goal is to implement and support 'TIC Programmes' (Technology of Information and Communication) through online platforms. These programmes cover areas such as education and culture.

9.3.6. Protection of children and young people

Children and young people are entitled to special protection and guidance while using the Internet.

They ought to be granted unique protection from interference with their physical, mental and moral welfare, specifically regarding sexual manipulation and abuse on the Internet.

⁹⁰⁰ *ibid.*

⁹⁰¹ REPORT from 11.02.2021 summary of the activity for the year 2020, <https://gdprcomplet.ro/lista-amenzi-gdpr-romania/#III_RAPORTUL_din_11022021_sinteza_a_activitatii_pentru_anul_2020>, accessed 5 March 2021.

Unfortunately, cybercrimes such as cyberbullying, online luring and internet-based sex crimes are not well regulated in regards to internet policies. Also, children are sometimes exposed to disturbing content, due to the lack of age proofing tools. However, the Romanian Civil Code regulates some of these before aforementioned issues in general.⁹⁰²

10. Based on your analysis, how do you believe the legislation regarding on the area of protecting human rights online will develop in the coming 5 years?

Based on our analysis, Romania's situation concerning the regulatory system for artificial intelligence has not yet reached a status satisfactory for the existent challenges in the field. While Romania remains one of the countries with significant prospects in this area, no substantial actions have been performed by authorities in regards to assuring the necessary protection of human rights when using AI technologies. As provided in our research, there are no specific regulations related to potential breaches of human rights by AI systems. Therefore, when deciding in certain cases, courts base their ruling on general provisions such as the Romanian Criminal Code or the Romanian Civil Code, general principles of law or on European acquis. As these practices continue to occur, directions in jurisprudence regarding protections of human rights when interacting with AI technologies are still to be established on a case-to-case basis.

Although AI technology is developing at a rapid pace, existing gaps in the regulatory framework still need to be analysed before any actions in this regard may be taken.

As no specific, sustainable steps have been made towards this goal, neither by the public authorities, nor by the non-governmental organisations, we may presume that Romanian regulations regarding the protection of human rights online will follow the directions set by the European Union.

Therefore, Romania is expected to take a set of measures, as well as set certain criteria that may impact various areas of its social and cultural system, aligning with the European framework and transposing various regulations into our national legislation.

When implementing EU legislation, human rights requirements and values need to be taken into consideration, including in the field of financial services, migration or responsibility of online intermediaries.

⁹⁰² Council of Europe Portal, Guide to Human Rights for Internet Users, <[https://www.coe.int/en/web/freedom-expression/guide-to-human-rights-for-internet-users#{"34618061](https://www.coe.int/en/web/freedom-expression/guide-to-human-rights-for-internet-users#{)> accessed 5 March 2021.

Romania has also signed the Declaration of Cooperation on Artificial Intelligence in May of 2018,⁹⁰³ which grants a certain degree of predictability to the Romanian regulatory framework on AI in the next few years. However, it is important to mention that EU legislation still has to address the issue of whether it can be adequately enforced upon the risks that AI technologies and systems create.

According to our analysis, certain domains will benefit from particular attention within the AI regulatory framework, as presented below.

10.1. Financing

Artificial Intelligence is envisaged to impact our lives and ease our work in various domains, from Energy to Business Administrations, Agriculture, Public Administration, Travel, Environment and other Industrial systems, including Cybersecurity. The Romanian regulatory system demands sector-specific rules, relevant for the various applications of AI. Taking into consideration the aforementioned directions in which AI systems may be developed, Government policies shall ensure that these sectors are receiving enough funding for the development of new technologies, as well as create sector specific rules to offer sufficient warranties with regard to Consumer Protection, Equal Treatment in employment and occupation or Financial Services. Although the regulatory framework must leave room for further developments, national market operators shall perform in an environment that does not leave room for any algorithmic exploitation of consumer behaviour, as well as any other possible violations of human rights. Such violations shall be punished accordingly.

10.2. Education

More and more countries and institutions address the need for AI education among people. While Romanian education systems still do not provide neither basic education on human rights compliance, nor AI courses before university, one can assert that future policies and projects may provide training programs for young students and, more importantly, for teachers. Understanding the impact of artificial intelligence technologies and the challenges they create on the environments we live in is essential, firstly for learning methods of how to use AI for implementing various concepts and, subsequently, for learning how to use these systems efficiently and ethically.

Such projects and policies may also be extended to broader audiences, once their success is proven within the school system.

⁹⁰³ EU Declaration on Cooperation on Artificial Intelligence
<<https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence>>, accessed 5 March 2021.

10.3. Research and development

AI technologies proved serious potential related to improving people's day - to - day lives, especially in regards to healthcare systems. While further discoveries that may increase the wellbeing of people are deeply encouraged, future policies, as well as some regulatory framework, shall tackle key issues such as the training of data used on AI systems taking into consideration EU rules and values, including fundamental rights. Further development of artificial intelligence shall find an equilibrium between the minimum requirements regarding safety, representativity, privacy and non-discrimination.

Conclusion

It is quite obvious that ADT promises considerable benefits in many fields, but the protection of human rights and fundamental freedoms remains essential. Some of the main principles of the correct approach are the following: lawfulness, fairness, proportionality, transparency, responsibility and demonstration of accountability or security of every step.

It is well known that keeping a balance is of utmost importance when discovering and implementing new ideas. Legislating ADT has to be done gradually, as people will cross a process of adapting to the changes in their lives, the transition starting to be more and more visible every day.

The EU has developed some strong strategies and encourages the contribution of all the member states, as only by cooperating and following the given rules the independence of people remain unharmed. Only by regulating the domain of ADT, the development of it can continue in a safe manner. Considering the given report, Romania, with no doubt, is supporting the initiative.

The purpose of ADT, the description of it or the impact on population can be found in various codes of ethics (ACM Code of Ethics and Professional Conduct), standards (Standards for AI Governance: International Standards to enable global coordination in AI Research & Development), guidelines (Guidelines on Data Protection Impact Assessment-DPIA) etc. However, EU countries promise further development, testing and continuing ongoing projects, evaluating and sharing the progress, contributing to a better tomorrow.

As Dave Waters said, 'The potential benefits of artificial intelligence are huge, but so are the dangers'. Only by thoughtful regulation can human rights remain safe.

Table of legislation

Provision in Romanian language	Corresponding translation in English
Constituția României Articolul 26 - Viața intimă, familială și privată (1) Autoritățile publice respectă și ocrotesc viața intimă, familială și privată. (2) Persoana fizică are dreptul să dispună de ea însăși, dacă nu încalcă drepturile și libertățile altora, ordinea publică sau bunele moravuri.	The Constitution of Romania Article 26 - Private and Family Life (1) Public authorities shall respect and protect private and family life. (2) Every person is free to dispose of themselves, as long as they do not violate the rights and freedoms of other persons, public order, or the standards of public morality.
LEGEA nr. 102 din 3 mai 2005 (republicată) privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal Articolul 17 (1) Împotriva procesului-verbal de constatare/sancționare și/sau a deciziei de aplicare a măsurilor corective, după caz, operatorul sau persoana împuternicită de operator poate introduce contestație la secția de contencios administrativ a tribunalului competent, în termen de 15 zile de la înmânare, respectiv de la comunicare. Hotărârea prin care s-a soluționat contestația poate fi atacată numai cu apel. Apelul se judecă de curtea de apel competentă. În toate cazurile, instanțele competente sunt cele din România. (2) Procesul-verbal de constatare/sancționare sau decizia președintelui Autorității naționale de supraveghere necontestată în termen de 15 zile de la data înmânării, respectiv comunicării, constituie titlu executoriu fără vreo altă formalitate. Introducerea contestației prevăzute la alin. (1) suspendă numai plata amenzii, până la pronunțarea unei hotărâri judecătorești definitive.	Law no. 102/2005 on the set up, organisation and functioning of the National Supervisory Authority for Personal Data Processing - Republished Article 17 (1) The data controller or processor may file an appeal against the report of the finding/sanctioning and/or the decision to apply the corrective measures, as the case may be, with the administrative contentious section of the competent court, within 15 days from handing, respectively from communication. The decision can only be appealed against. The appeal is judged by the competent court of appeal. In all cases, the competent courts are those in Romania. (2) The report of finding/sanctioning or the decision of the president of the National Supervisory Authority unchallenged within 15 days from the date of handing, respectively the communication, constitutes an enforceable title without any other formality. Introducing the appeal provided in paragraph (1) suspends only the payment of the fine, until a final court decision is issued. (3) The fine payment deadline is 15 days from the date of handing, respectively from the

(3) Termenul de plată a amenzii este de 15 zile de la data înmânării, respectiv de la data comunicării procesului-verbal de constatare/sanționare sau a deciziei președintelui Autorității Naționale de Supraveghere.	communication date of the finding/sanctioning minutes or of the decision of the president of the National Supervisory Authority.
Articolul 21 (1) Procedura de soluționare a plângerilor se reglementează prin decizie a președintelui Autorității naționale de supraveghere, publicată în Monitorul Oficial al României, Partea I. (2) Autoritatea națională de supraveghere informează persoana vizată cu privire la admisibilitatea plângerii, în termen de cel mult 45 de zile de la înregistrare. În cazul în care se constată că informațiile din plângere sau documentele transmise sunt incomplete sau insuficiente, Autoritatea națională de supraveghere solicită persoanei vizate să completeze plângerea pentru a putea fi considerată admisibilă în vederea efectuării unei investigații. Un nou termen de cel mult 45 de zile curge de la data completării plângerii. (3) Autoritatea Națională de Supraveghere informează persoana vizată în legătură cu evoluția sau cu rezultatul investigației întreprinse în termen de 3 luni de la data la care s-a comunicat acesteia că plângerea este admisibilă potrivit alin. (2). Informarea va cuprinde și calea de atac împotriva Autorității naționale de supraveghere. (4) Dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu alte autorități de supraveghere în conformitate cu art. 57 alin. (1) lit. f) din Regulamentul general privind protecția datelor, Autoritatea națională de supraveghere informează persoana vizată în legătură cu evoluția investigației, din 3	Article 21 (1) The procedure for handling complaints is regulated by decision of the president of the National Supervisory Authority, published in the Official Journal of Romania, Part I. (2) The national supervisory authority shall inform the data subject about the admissibility of the complaint, within 45 days from the registration. If it is found that the information in the complaint or the documents transmitted are incomplete or insufficient, the National Supervisory Authority requests the data subject to complete the complaint in order to be considered admissible for the purpose of carrying out an investigation. A new deadline of no more than 45 days starts from the date of filing the complaint. (3) The National Supervisory Authority shall inform the data subject about the progress or outcome of the investigation, within three months from the date on which they were notified that the complaint is admissible in accordance with paragraph (2). The information will also include the remedy against the National Supervisory Authority. (4) If a more detailed investigation or coordination with other supervisory authorities is required in accordance with Article 57 paragraph (1) letter f) of the General Data Protection Regulation, the National Supervisory Authority shall inform the data subject about the progress of the

în 3 luni, până la finalizarea acesteia. Rezultatul investigației se aduce la cunoștință persoanei vizate în termen de cel mult 45 de zile de la finalizarea acesteia. (5) În cadrul procedurii de soluționare a plângerilor, investigațiile se efectuează în conformitate cu dispozițiile art. 14-19. (6) În cazul nerespectării dispozițiilor alin. (2)-(4), persoana vizată se poate adresa secției de contencios administrativ a tribunalului competent, după parcurgerea procedurii prealabile prevăzute de Legea contenciosului administrativ nr. 554/2004, cu modificările și completările ulterioare. Recursul se judecă de curtea de apel competentă. În toate cazurile, instanțele competente sunt cele din România.	investigation, every three months, until it is finalised. The outcome of the investigation shall be brought to the attention of the data subject within 45 days from the finalisation of the investigation. (5) Within the procedure for solving complaints, investigations are carried out in accordance with the provisions of Articles 14-19. (6) In case of non-observance of the provisions of paragraphs (2) - (4), the data subject may address the administrative contentious section of the competent court, after having completed the preliminary procedure provided by the Law of the administrative contentious no. 554/2004, as subsequently amended and supplemented. The appeal is judged by the competent court of appeal - in all cases, the competent courts are those in Romania.
Articolul 22 (1) Dacă în urma exercitării atribuțiilor sale legale, Autoritatea națională de supraveghere apreciază că au fost încălcate oricare dintre drepturile persoanelor vizate garantate de reglementările legale din domeniul protecției datelor personale, poate sesiza instanța competentă, potrivit legii. Persoana vizată dobândește de drept calitatea de reclamant, urmând a fi citată în această calitate. Dacă persoana vizată își însușește acțiunea, încetează calitatea procesuală activă a Autorității naționale de supraveghere. Dacă persoana vizată nu își însușește acțiunea formulată de Autoritatea națională de supraveghere, instanța anulează cererea potrivit Codului de procedură civilă.	Article 22 (1) If, following the exercise of its legal powers, the National Supervisory Authority considers that any of the rights of the data subjects guaranteed by the legal regulations in the field of personal data protection have been infringed, it may notify the competent court, according to the law. The data subject acquires the quality of a claimant and shall be cited as such. If the data subject approves this action, the active quality of the National Supervisory Authority shall cease. If the data subject does not approve the action taken by the National Supervisory Authority, the court will cancel the application according to the Civil Procedure Code. (2) The actions and requests, including those for the exercise of ordinary or extraordinary

(2) Acțiunile și cererile, inclusiv cele pentru exercitarea căilor de atac ordinare sau extraordinare, formulate de Autoritatea națională de supraveghere, sunt scutite de la plata taxelor judiciare de timbru. (3) Dispozițiile alin. (2) se aplică și persoanei vizate care își însușește acțiunea formulată de Autoritatea națională de supraveghere în condițiile alin. (1).	remedies, formulated by the National Supervisory Authority, are exempt from the payment of stamp court fees. (3) The provisions of paragraph (2) also apply to the data subject who appropriates the action formulated by the National Supervisory Authority under the conditions of paragraph (1).
Articolul 23 (1) Contestarea actelor emise de Autoritatea națională de supraveghere în activitatea de control și de soluționare a plângerilor se efectuează potrivit art. 17 și 21. (2) Actele administrative emise de Autoritatea națională de supraveghere în exercitarea atribuțiilor legale, altele decât cele prevăzute la alin. (1), pot fi contestate la secția de contencios administrativ a tribunalului competent. (3) Dispozițiile prezentei legi se completează cu prevederile Legii nr. 554/2004, cu modificările și completările ulterioare, în măsura în care prezenta lege nu dispune altfel.	Article 23 (1) Challenging of the documents issued by the National Supervisory Authority in the activity of control and handling of the complaints is carried out according to Articles 17 and 21. (2) The administrative documents issued by the National Supervisory Authority in the exercise of the legal tasks, other than those provided in paragraph (1), can be appealed to the administrative litigation section of the competent court. (3) The provisions of this law are supplemented by the provisions of Law no. 554/2004, as subsequently amended and supplemented, to the extent that this law does not provide otherwise.
Lege nr. 287 din 17 iulie 2009 privind Codul civil	Law no. 287/2009 on the Civil Code
Articolul 1349 - Răspunderea delictuală (1) Orice persoană are îndatorirea să respecte regulile de conduită pe care legea sau obiceiul locului le impune și să nu aducă atingere, prin acțiunile ori inacțiunile sale, drepturilor sau intereselor legitime ale altor persoane. (2) Cel care, având discernământ, încalcă această îndatorire răspunde de toate prejudiciile cauzate, fiind obligat să le repare integral.	Article 1349 – Liability (1) Everyone has the duty to comply with the rules of conduct which the law or habit of the place requires and shall not prejudice, through their actions or inactions, the rights or legitimate interests of other persons. (2) One who, having discernment, violates this duty shall be liable for all the damage caused, being obliged to repair them in full.

(3) În cazurile anume prevăzute de lege, o persoană este obligată să repare prejudiciul cauzat de fapta altuia, de lucrurile ori animalele aflate sub paza sa, precum și de ruina edificiului. (4) Răspunderea pentru prejudiciile cauzate de produsele cu defecte se stabilește prin lege specială.	(3) In the specific cases provided by law, a person is obliged to repair the damage caused by the deed of another, by the things or animals under their guard, as well as by the ruin of the edifice. (4) The liability for damage caused by defective products shall be established by special law.
Articolul 1357 - Condițiile răspunderii (1) Cel care cauzează altuia un prejudiciu printr-o faptă ilicită, săvârșită cu intenție sau din culpă, este obligat să îl repare. (2) Autorul prejudiciului răspunde pentru cea mai ușoară culpă.	Article 1357 - Conditions of liability (1) A person who causes damage to another by an unlawful act, committed with intent or culpability, shall be obliged to repair it. (2) The perpetrator of the damage shall be liable for the slightest culpability.
Articolul 1358 - Criterii particulare de apreciere a culpei Pentru aprecierea culpei se va ține seama de împrejurările în care s-a produs prejudiciul, străine de persoana autorului faptei, precum și, dacă este cazul, de faptul că prejudiciul a fost cauzat de un profesionist în exercițiul activității sale.	Article 1358 - Private criteria for the assessment of fault In the scope of fault assessment, an account shall be taken of the circumstances in which the damage occurred, alien to the person responsible for the offence and, where appropriate, of the fact that the damage was caused by a professional in the course of their business.
Articolul 1382 - Răspunderea solidară Cei care răspund pentru o faptă prejudiciabilă sunt ținuti solidar la reparație față de cel prejudiciat.	Article 1382 – Solidarity liability Those who are responsible for an injurious act are held in solidarity with the injured.
Articolul 1385 - Întinderea reparației (1) Prejudiciul se repară integral, dacă prin lege nu se prevede altfel. (2) Se vor putea acorda despăgubiri și pentru un prejudiciu viitor dacă producerea lui este neîndoielnică. (3) Despăgubirea trebuie să cuprindă pierderea suferită de cel prejudiciat, câștigul pe care în condiții obișnuite el ar fi putut să îl realizeze și	Article 1385 – Reach of repairs (1) The damage shall be fully repaired, unless otherwise provided by law. (2) Damages may also be granted for future damage if its production is undeniable. 3. The compensation must include the loss suffered by the injured person, the gains which they could have achieved under normal circumstances and were deprived of, and the

de care a fost lipsit, precum și cheltuielile pe care le-a făcut pentru evitarea sau limitarea prejudiciului. (4) Cu toate acestea, dacă fapta ilicită a determinat și pierderea șansei de a obține un avantaj, reparația va fi proporțională cu probabilitatea obținerii avantajului, ținând cont de împrejurări și de situația concretă a victimei.	costs they have incurred in order to avoid or limit the damage. (4) However, if the unlawful act has also caused the loss of an opportunity to obtain an advantage, the reparation will be proportionate to the likelihood of obtaining the advantage, taking into account the circumstances and the actual situation of the victim.
Articolul 1386 - Formele reparației (1) Repararea prejudiciului se face în natură, prin restabilirea situației anterioare, iar dacă aceasta nu este cu puțință ori dacă victima nu este interesată de reparația în natură, prin plata unei despăgubiri, stabilită prin acordul părților sau, în lipsă, prin hotărâre judecătorească. (2) La stabilirea despăgubirii se va avea în vedere, dacă prin lege nu se prevede altfel, data producerii prejudiciului. (3) Dacă prejudiciul are un caracter de continuitate, despăgubirea se acordă sub formă de prestații periodice. (4) În cazul prejudiciului viitor, despăgubirea, indiferent de forma în care s-a acordat, va putea fi sporită, redusă sau suprimată, dacă, după stabilirea ei, prejudiciul s-a mărit, s-a micșorat ori a încetat.	Article 1386 – Forms of repair (1) Repair of the damage shall be done in kind, by restoring the previous situation, and if this is not possible or if the victim is not interested in the compensation in kind, by payment of compensation, established by agreement of the parties or, failing that, by judicial decision. (2) When establishing the compensation, an account shall be taken of the date of the damage, unless otherwise provided by law. (3) Where the damage is of a continuity nature, compensation shall be granted in the form of periodic benefits. (4) In the case of future damage, compensation, regardless of the form in which it was granted, may be increased, reduced or suppressed if, after its establishment, the damage has increased, decreased or ceased.
Ordonanța de Guvern nr. 137/2000	The Government Ordinance no. 137/2000
Articolul 1 (1) În România, stat de drept, democratic și social, demnitatea omului, drepturile și libertățile cetățenilor, libera dezvoltare a personalității umane reprezintă valori supreme și sunt garantate de lege. (2) Principiul egalității între cetățeni, al excluderii privilegiilor și discriminării sunt	Article 1 (1) In Romania, as a democratic and social state governed by the rule of law, human dignity, citizens' rights and freedoms, free development of human personality represents supreme values and shall be guaranteed. (2) The principle of equality among citizens, the elimination of all privileges and

garantate în special în exercitarea următoarelor drepturi: a) dreptul la un tratament egal în fața instanțelor judecătorești și a oricărui altui organ jurisdicțional; b) dreptul la securitatea persoanei și la obținerea protecției statului împotriva violențelor sau maltratărilor din partea oricărui individ, grup sau instituție; c) drepturile politice, și anume drepturile electorale, dreptul de a participa la viața publică și de a avea acces la funcții și demnități publice; d) drepturile civile, în special: (i) dreptul la libera circulație și la alegerea reședinței; (ii) dreptul de a părăsi țara și de a se întoarce în țară; (iii) dreptul de a obține și de a renunța la cetățenia română; (iv) dreptul de a se căsători și de a-și alege partenerul; (v) dreptul de proprietate; (vi) dreptul la moștenire; (vii) dreptul la libertatea de gândire, conștiință și religie; (viii) dreptul la libertatea de opinie și de exprimare; (ix) dreptul la libertatea de întrunire și de asociere; (x) dreptul de petiționare; e) drepturile economice, sociale și culturale, în special: (i) dreptul la muncă, la libera alegere a ocupației, la condiții de muncă echitabile și satisfăcătoare, la protecția împotriva șomajului, la un salariu egal pentru muncă egală, la o remunerație echitabilă și satisfăcătoare; (ii) dreptul de a înființa sindicate și de a se afilia unor sindicate;	discrimination shall be guaranteed, in particular with regard to the exercise of the following rights: a) the right to equal treatment before courts and any other jurisdictional bodies; b) the right to personal security and to be granted state protection against violence and mistreatment perpetrated by any individual, group or institution; c) political rights, namely electoral rights, the right to take part in public life and the right to access to public positions; d) other civil rights, in particular: (i) the right to freedom of movement and of choosing one's residence; (ii) the right to leave and return to one's country; (iii) the right to obtain the Romanian citizenship; (iv) the right to marry and to choose one's partner; (v) the right to property; (vi) the right to inheritance; (vii) the right to freedom of thought, conscience and religion; (viii) the right to freedom of expression and opinion; (ix) the right to freedom of peaceful meeting and association; (x) the right to file a petition. e) economic, social and cultural rights, in particular: (i) the right to work, to freely choose an occupation, to fair and satisfactory working conditions, to protection against unemployment, to equal pay for equal work, to fair and satisfactory wages; (ii) the right to establish and to join trade unions; (iii) the right to housing;

(iii) dreptul la locuință; (iv) dreptul la sănătate, la îngrijire medicală, la securitate socială și la servicii sociale; (v) dreptul la educație și la pregătire profesională; (vi) dreptul de a lua parte, în condiții de egalitate, la activități culturale și sportive; f) dreptul de acces la toate locurile și serviciile destinate folosinței publice. (3) Exercițarea drepturilor enunțate în cuprinsul prezentului articol privește persoanele aflate în situații comparabile.	(iv) the right to health, medical assistance, social security and social services; (v) the right to education and to professional training; (vi) the right to take part in cultural activities in conditions of equality; f) the right of access to all public places and services. (3) The exercise of the rights provided by the present article regards the persons found in comparable situations.
Articolul 2 (1) Potrivit prezentei ordonanțe, prin discriminare se înțelege orice deosebire, excludere, restricție sau preferință, pe bază de rasă, naționalitate, etnie, limbă, religie, categorie socială, convingeri, sex, orientare sexuală, vârstă, handicap, boală cronică necontagioasă, infectare HIV, apartenență la o categorie defavorizată, precum și orice alt criteriu care are ca scop sau efect restrângerea, înlăturarea recunoașterii, folosinței sau exercitării, în condiții de egalitate, a drepturilor omului și a libertăților fundamentale sau a drepturilor recunoscute de lege, în domeniul politic, economic, social și cultural sau în orice alte domenii ale vieții publice.	Article 2 (1) In accordance with the ordinance herein, discrimination encompasses any difference, exclusion, restriction or preference based on race, nationality, ethnicity, language, religion, social category, beliefs, gender or sexual orientation, age, handicap, non contagious chronic disease, HIV infection, belonging to a disfavoured category, as well as any other criterion aiming to or resulting in the restriction or elimination of the recognition, use or exercise, in conditions of equality, of human rights and fundamental liberties or of rights granted by law in the political, economic, social and cultural field or in any other domains of public life.
Articolul 19 (1) În vederea combaterii faptelor de discriminare, Consiliul își exercită atribuțiile în următoarele domenii: a) prevenirea faptelor de discriminare; b) medierea faptelor de discriminare; c) investigarea, constatarea și sancționarea faptelor de discriminare;	Article 19 (1) As regards the combating of discrimination deeds, the National Council for Combating Discrimination is exercising its duties in the following fields: a) prevention of all forms of discrimination; b) mediation of discrimination deeds;

d) monitorizarea cazurilor de discriminare; e) acordarea de asistență de specialitate victimelor discriminării.	c) investigation, ascertaining and sanctioning of discrimination deeds; d) monitoring the discriminatory cases; e) providing specialised assistance to victims of discrimination.
Articolul 26 (1) Contravențiile prevăzute la art. 2 alin. (2), (4), (5) și (7), art. 6 - 9, art. 10, art. 11 alin. (1), (3) și (6), art. 12, 13, 14 și 15 se sancționează cu amendă de la 1.000 lei la 30.000 lei, dacă discriminarea vizează o persoană fizică, respectiv cu amendă de la 2.000 lei la 100.000 lei, dacă discriminarea vizează un grup de persoane sau o comunitate.	Article 26 (1) The contraventions provided under articles 2 paragraph (5) and (7), 5-8, 10, 11 paragraphs (1), (3) and (6), 12, 13 paragraph (1), 14 and 15 of the ordinance herein shall be sanctioned with a 1.000 to 30.000 RON fine if perpetrated against a natural entity or with 2.000 to 100.000 RON fine if perpetrated against a group of persons or a community.
Hotărârea nr. 695/2002 privind înființarea Institutului de Cercetări pentru Inteligență Artificială	Decision No. 695/2002 on the establishment of the Research Institute for Artificial Intelligence
(1) Se înființează Institutul de Cercetări pentru Inteligență Artificială prin reorganizarea Centrului pentru Cercetări Avansate în Învățarea Automată, Prelucrarea Limbajului Natural și Modelare Conceptuală din subordinea Academiei Române, care se desființează. (2) Institutul de Cercetări pentru Inteligență Artificială desfășoară activități de cercetare fundamentală în domeniile: a) inteligenței artificiale - învățarea automată, prelucrarea limbajului natural și modelare conceptuală și cognitivă, agenți inteligenți și altele asemenea; b) societății cunoașterii - managementul cunoștințelor, modelarea infrastructurilor și a proceselor societății, bazată pe cunoștințe și scenarii cognitive; c) noilor arhitecturi de rețele de calculatoare - sisteme cu autoorganizare.	(1) The Research Institute for Artificial Intelligence is founded by the reorganisation of the Center for Advanced Research in Automatic Learning, Natural Language Processing and Conceptual Modeling under the Romanian Academy, which is abolished. (2) The Research Institute for Artificial Intelligence conducts fundamental research activities in the fields of: a) artificial intelligence – automatic learning, natural language processing and conceptual and cognitive modeling, intelligent agents and the like; b) knowledge society – knowledge management, shaping of society's infrastructures and processes, based on knowledge and cognitive scenarios; c) new architectures of computer networks – systems with self-organisation.
Codul de Procedură Penală	Code of Criminal Procedure.
Articolul 138	Article 138

(1) Constituie metode speciale de supraveghere sau cercetare următoarele: a) interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță; b) accesul la un sistem informatic; c) supravegherea video, audio sau prin fotografiere; d) localizarea sau urmărirea prin mijloace tehnice; e) obținerea datelor privind tranzacțiile financiare ale unei persoane; f) reținerea, predarea sau percheziționarea trimiterilor poștale; g) utilizarea investigatorilor sub acoperire și a colaboratorilor; h) participarea autorizată la anumite activități; i) livrarea supravegheată; j) obținerea datelor de trafic și de localizare prelucrate de către furnizorii de rețele publice de comunicații electronice ori furnizorii de servicii de comunicații electronice destinate publicului. (2) Prin interceptarea comunicațiilor ori a oricărui tip de comunicare se înțelege interceptarea, accesul, monitorizarea, colectarea sau înregistrarea comunicărilor efectuate prin telefon, sistem informatic ori prin orice alt mijloc de comunicare. (3) Prin acces la un sistem informatic se înțelege pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe. (4) Prin sistem informatic se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate ori aflate în relație funcțională, dintre care unul sau mai multe asigură	(1) The following are surveillance or investigation special methods: a) wiretapping of communications or of any type of remote communication; b) accessing a computer system; c) video, audio or photo surveillance; d) tracking or tracing with the use of technical devices; e) obtaining data regarding the financial transactions of individuals; f) withholding, delivery or search of mail deliveries; g) use of undercover investigators and informants; h) authorised participation in specific activities; i) controlled delivery; j) obtaining data generated or processed by providers of public electronic communication networks or by providers of electronic communication services intended for the public, other than the content of communications, stored by these under the special law on storing data generated or processed by providers of public electronic communication networks and by providers of electronic communication services intended for the public. (2) Wiretapping of communications or of any type of messages designates the wiretapping, accessing, monitoring, collection or recording of communications via phone, computer system or any other communication device. (3) Accessing a computer system designates the penetration of a computer system or of other data storage device either directly or from a distance, through specialised programs or through a network, for the purpose of identifying evidence.

prelucrarea automată a datelor, cu ajutorul unui program informatic. (5) Prin date informatice se înțelege orice reprezentare de fapte, informații sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic. (6) Prin supraveghere video, audio sau prin fotografiere se înțelege fotografierea persoanelor, observarea sau înregistrarea conversațiilor, mișcărilor ori a altor activități ale acestora. (7) Prin localizare sau urmărire prin mijloace tehnice se înțelege folosirea unor dispozitive care determină locul unde se află persoana sau obiectul la care sunt atașate. (8) Prin percheziționarea trimerilor poștale se înțelege verificarea, prin mijloace fizice sau tehnice, a scrisorilor, a altor trimiteri poștale sau a obiectelor transmise prin orice alt mijloc. (9) Prin obținerea datelor privind tranzacțiile financiare ale unei persoane se înțelege operațiunile prin care se asigură cunoașterea conținutului tranzacțiilor financiare și al altor operațiuni efectuate sau care urmează să fie efectuate prin intermediul unei instituții de credit ori al altei entități financiare, precum și obținerea de la o instituție de credit sau de la altă entitate financiară de înregistrări ori informații aflate în posesia acesteia referitoare la tranzacțiile sau operațiunile unei persoane. (10) Prin utilizarea investigatorilor sub acoperire și a colaboratorilor se înțelege folosirea unei persoane cu o altă identitate decât cea reală în scopul obținerii de date și	(4) A computer system is any device or combination of devices interconnected between them or in a functional relation, one or more of which provide the automatic data processing by means of a computer program. (5) Computer data is any representation of facts, information or concepts in a form appropriated for processing in a computer system, including a program able to determine the performance of a function by a computer system. (6) Video, audio or photo surveillance is the taking of pictures of persons, the observation or recording of their conversations, gestures or other activities. (7) Tracking or tracing with the use of technical devices is the use of devices that establish the location of the person or the object to which such devices are attached. (8) Search of mail deliveries designates the inspection, through physical or technical methods, of letters or other mail deliveries or objects transmitted through any other means. (9) Obtaining of data regarding the financial transactions of individuals designates operations that provide knowledge of the contents of financial transactions and other operations performed or to be performed through a credit institution or through other financial entity, as well as the obtaining from a credit institution or other financial entities of documents or information held by it referring to the transactions or operations of a person. (10) Use of undercover investigators and informants designates the use of a person with an identity other than their real one, for the purpose of obtaining data and information regarding the commission of an offense.

informații cu privire la săvârșirea unei infracțiuni. (11) Prin participarea autorizată la anumite activități se înțelege comiterea unei fapte similare laturii obiective a unei infracțiuni de corupție, efectuarea de tranzacții, operațiuni sau orice fel de înțelegeri privind un bun sau privind o persoană despre care se bănuiește că ar fi dispărută, că este victima traficului de persoane ori a unei răpiri, efectuarea de operațiuni privind droguri, precum și prestarea unui serviciu, desfășurate cu autorizarea organului judiciar competent, în scopul obținerii de mijloace de probă. (12) Prin livrare supravegheată se înțelege tehnica de supraveghere și cercetare prin care se permit intrarea, circulația sau ieșirea de pe teritoriul țării a unor bunuri în privința cărora există o suspiciune cu privire la caracterul ilicit al deținerii sau obținerii acestora, sub supravegherea ori cu autorizarea autorităților competente, în scopul investigării unei infracțiuni sau al identificării persoanelor implicate în săvârșirea acesteia. (13) Prin supraveghere tehnică se înțelege utilizarea uneia dintre metodele prevăzute la alin. (1) lit. a)-d).	(11) Authorised participation in specific activities means the commission of acts similar to the objective component of a corruption offense, the performance of transactions, operations or any other kind of arrangements related to an asset or to a person who is presumed missing, a victim of trafficking in human beings or of kidnapping, the performance of operations involving drugs, as well as the providing of services, based on an authorisation from the judicial bodies of competent jurisdiction for the purpose of obtaining evidence. (12) Controlled delivery designates a surveillance and investigation technique allowing for the entry, transit or exit from the territory of the country of goods in respect of which there is a suspicion related to the illicit nature of their possession or obtaining, under the surveillance of or based on an authorisation from the competent authorities, for the purpose of investigating an offense or of identifying the persons involved in its commission. (13) Electronic surveillance is the use of any of the methods listed under par. (1) items a) - e).

Articolul 139 (1) Supravegherea tehnică se dispune de judecătorul de drepturi și libertăți atunci când sunt îndeplinite cumulativ următoarele condiții: a) există o suspiciune rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni dintre cele prevăzute la alin. (2); b) măsura să fie proporțională cu restrângerea drepturilor și libertăților fundamentale, date fiind particularitățile cauzei, importanța informațiilor ori a probelor ce urmează a fi obținute sau gravitatea infracțiunii; c) probele nu ar putea fi obținute în alt mod sau obținerea lor ar presupune dificultăți deosebite ce ar prejudicia ancheta ori există un pericol pentru siguranța persoanelor sau a unor bunuri de valoare. (2) Supravegherea tehnică se poate dispune în cazul infracțiunilor contra securității naționale prevăzute de Codul penal și de legi speciale, precum și în cazul infracțiunilor de trafic de droguri, de efectuare de operațiuni ilegale cu precursori sau cu alte produse susceptibile de a avea efecte psihoactive, infracțiunilor privind nerespectarea regimului armelor, munițiilor, materialelor nucleare, al materiilor explozive și al precursorilor de explozivi restricționați, de trafic și exploatarea persoanelor vulnerabile, acte de terorism, de spălare a banilor, de falsificare de monede, timbre sau de alte valori, de falsificare de instrumente de plată electronică, în cazul infracțiunilor care se săvârșesc prin sisteme informatice sau mijloace de comunicare electronică, contra patrimoniului, de șantaj, de viol, de lipsire de libertate în mod ilegal, de evaziune fiscală, în cazul infracțiunilor de corupție și al infracțiunilor asimilate	Article 139 (1) Electronic surveillance is ordered by the Judge for Rights and Liberties when the following requirements are cumulatively met: a) there is a reasonable suspicion in relation to the preparation or commission of one of the offenses listed under par. (2); b) such measure is proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or evidence that are to be obtained or the seriousness of the offense; c) evidence could not be obtained in any other way or its obtaining implies special difficulties that would harm the investigation, or there is a threat for the safety of persons or of valuable goods. (2) Electronic surveillance may be ordered in case of offenses against national security stipulated by the Criminal Code and by special laws, as well as in case of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism, money laundering, counterfeiting of currency or securities, counterfeiting electronic payment instruments, offenses against property, blackmail, rape, deprivation of freedom, tax evasion, corruption offenses and offenses assimilated to corruption, offenses against the European Union's financial interests, offenses committed by means of computer systems or electronic communication devices, or in case of other offenses in respect of which the law sets forth a penalty of no less than 5 years of imprisonment. (3) The recordings set forth by this chapter, done by the parties or by other persons, represent evidence when they concern their

infracțiunilor de corupție, infracțiunilor împotriva intereselor financiare ale Uniunii Europene ori în cazul altor infracțiuni pentru care legea prevede pedeapsa închisorii de 5 ani sau mai mare. (3) Înregistrările prevăzute în prezentul capitol, efectuate de părți sau de alte persoane, constituie mijloace de probă când privesc propriile convorbiri sau comunicări pe care le-au purtat cu terții. Orice alte înregistrări pot constitui mijloace de probă dacă nu sunt interzise de lege. (4) Raportul dintre avocat și persoana pe care o asistă sau o reprezintă nu poate forma obiectul supravegherii tehnice decât dacă există date că avocatul săvârșește ori pregătește săvârșirea unei infracțiuni dintre cele prevăzute la alin. (2). Dacă pe parcursul sau după executarea măsurii rezultă că activitățile de supraveghere tehnică au vizat și raporturile dintre avocat și suspectul ori inculpatul pe care acesta îl apără, probele obținute nu pot fi folosite în cadrul niciunui proces penal, urmând a fi distruse, de îndată, de către procuror. Judecătorul care a dispus măsura este informat, de îndată, de către procuror. Atunci când apreciază necesar, judecătorul dispune informarea avocatului.	own conversations or communications with third parties. Any other recordings may constitute evidence unless prohibited by law. (4) The relation between a counsel and a person assisted or represented by them may be subject to electronic surveillance only when there is information that the counsel perpetrates or prepares the commission of any of the offenses listed under par. (2). If during or after the performance of such measure it results that the activities of electronic surveillance also targeted the relations between the counsel and the suspect or defendant defended by the former, the evidence obtained this way may not be used in a criminal proceeding, and shall be destroyed forthwith by the prosecutor. The judge having ordered such measure shall be informed forthwith by the prosecutor. When deemed necessary, the judge may order the information of the counsel.
Articolul 168 (1) Prin percheziție în sistem informatic sau a unui suport de stocare a datelor informatice se înțelege procedeul de cercetare, descoperire, identificare și strângere a probelor stocate într-un sistem informatic sau suport de stocare a datelor informatice, realizat prin intermediul unor mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea.	Article 168 (1) A computer system search or a computer data storage medium search designates the procedure for the investigation, discovery, identification and collection of evidence stored in a computer system or in a computer data storage medium, performed by means of adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these.

(2) În cursul urmăririi penale, judecătorul de drepturi și libertăți de la instanța căreia i-ar reveni competența să judece cauza în primă instanță sau de la instanța corespunzătoare în grad acesteia în a cărei circumscripție se află sediul parchetului din care face parte procurorul care efectuează sau supraveghează urmărirea penală poate dispune efectuarea unei percheziții informatice, la cererea procurorului, atunci când pentru descoperirea și strângerea probelor este necesară cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice. (3) Procurorul înaintează cererea prin care se solicită încuviințarea efectuării percheziției informatice împreună cu dosarul cauzei judecătorului de drepturi și libertăți. (4) Cererea se soluționează în camera de consiliu, fără citarea părților. Participarea procurorului este obligatorie. (5) Judecătorul dispune prin încheiere admiterea cererii, atunci când aceasta este întemeiată, încuviințarea efectuării percheziției informatice și emite de îndată mandatul de percheziție. (6) Încheierea instanței trebuie să cuprindă: a) denumirea instanței; b) data, ora și locul emiterii; c) numele, prenumele și calitatea persoanei care a emis mandatul; d) perioada pentru care s-a emis mandatul și în cadrul căreia trebuie efectuată activitatea dispusă; e) scopul pentru care a fost emis; f) sistemul informatic sau suportul de stocare a datelor informatice care urmează a fi percheziționat, precum și numele suspectului sau inculpatului, dacă este cunoscut;	(2) During a the criminal investigation, the Judge for Rights and Liberties of the court that would have the competence of jurisdiction to examine the case in first instance or of the court corresponding to its level under whose territorial jurisdiction the premises of the prosecutors' office with which the prosecutor conducting or supervising the criminal investigation is working are located may order the conducting of a computer search, upon request by the prosecutor, when the investigation of a computer system or of a computer data storage medium is necessary for the discovery and collection of evidence. (3) The prosecutor shall submit an application requesting the approval of a computer search together with the case file to the Judge for Rights and Liberties. (4) Such application is ruled on in chambers, without summoning the parties. The prosecutor's attendance is mandatory. (5) The judge orders, through a court resolution, to sustain the application, when this is well-grounded, to approve the computer search, and issues a search warrant forthwith. (6) Such court resolution has to contain: a) name of the court; b) date, time and place of issuance; c) surname, first name and capacity of the person who issued the warrant; d) the time frame for which the warrant was issued and within which the ordered activity has to be performed; e) purpose for which it was issued; f) the computer system or computer data storage medium that is to be subject to search, as well as the name of the suspect or defendant, if known;

g) semnătura judecătorului și ștampila instanței. (7) Încheierea prin care judecătorul de drepturi și libertăți se pronunță asupra cererii de încuviințare a efectuării percheziției informatice nu este supusă căilor de atac. (8) În cazul în care, cu ocazia efectuării percheziției unui sistem informatic sau a unui suport de stocare a datelor informatice, se constată că datele informatice căutate sunt cuprinse într-un alt sistem informatic ori suport de stocare a datelor informatice și sunt accesibile din sistemul sau suportul inițial, procurorul dispune de îndată conservarea, copierea datelor informatice identificate și va solicita de urgență completarea mandatului, dispozițiile alin. (1)-(7) aplicându-se în mod corespunzător. (9) În vederea executării percheziției dispuse, pentru asigurarea integrității datelor informatice stocate pe obiectele ridicate, procurorul dispune efectuarea de copii. (10) Dacă ridicarea obiectelor care conțin datele informatice prevăzute la alin. (1) ar afecta grav desfășurarea activității persoanelor care dețin aceste obiecte, procurorul poate dispune efectuarea de copii, care servesc ca mijloc de probă. Copiile se realizează cu mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea. (11) Percheziția în sistem informatic sau a unui suport de stocare a datelor informatice se efectuează în prezența suspectului ori a inculpatului, dispozițiile art. 159 alin. (10) și (11) aplicându-se în mod corespunzător. (12) Percheziția în sistem informatic ori a unui suport de stocare a datelor informatice se efectuează de un specialist care funcționează în	g) signature of the judge and stamp of the court. (7) A court resolution through which the Judge for Rights and Liberties decides upon an application for the approval of a computer search is not subject to avenues of appeal. (8) In the event that, on the occasion of a search of a computer system or of a computer data storage medium, it is found that the sought computer data are stored in a different computer system or a computer data storage medium, and are accessible from the initial system or medium, the prosecutor shall immediately order the preservation and copying of the identified computer data and shall request the issuance of a warrant on an emergency basis. The stipulations of par. (1) - (7) shall apply accordingly. (9) In conducting the ordered search, in order to ensure integrity of the computer data stored on the seized objects, the prosecutor shall order the making of copies of them. (10) If the seizure of objects containing computer data is set under par. (1) seriously hinders the performance of activities by the persons holding such objects, the prosecutor may order the making of copies of them, which would serve as methods of proof. Copies are made with adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these. (11) A computer system or computer data storage medium search is conducted in the presence of a suspect or a defendant, and the provisions of Art. 159 par. (10) and (11) shall apply accordingly. (12) A computer system or computer data storage medium search is conducted by a

cadrul organelor judiciare sau din afara acestora, în prezența procurorului sau a organului de cercetare penală. (13) Procesul-verbal de percheziție informatică trebuie să cuprindă: a) numele persoanei de la care a fost ridicat sistemul informatic sau suporturile de stocare a datelor informatice ori numele persoanei al cărei sistem informatic este cercetat; b) numele persoanei care a efectuat percheziția; c) numele persoanelor prezente la efectuarea percheziției; d) descrierea și enumerarea sistemelor informatice ori suporturilor de stocare a datelor informatice față de care s-a dispus percheziția; e) descrierea și enumerarea activităților desfășurate; f) descrierea și enumerarea datelor informatice descoperite cu ocazia percheziției; g) semnătura sau ștampila persoanei care a efectuat percheziția; h) semnătura persoanelor prezente la efectuarea percheziției. (14) Organele de urmărire penală trebuie să ia măsuri ca percheziția informatică să fie efectuată fără ca faptele și împrejurările din viața personală a celui la care se efectuează percheziția să devină, în mod nejustificat, publice. (15) Datele informatice identificate cu caracter secret se păstrează în condițiile legii. (16) În cursul judecății, percheziția informatică se dispune de către instanță, din oficiu sau la cererea procurorului, a părților ori a persoanei vătămate, în cazurile prevăzute la alin. (2). Mandatul de efectuare a percheziției	specialist working with the judicial bodies or an external one, in the presence of the prosecutor or of the criminal investigation bodies. (13) A computer search report has to contain: a) name of the person from whom a computer system or computer data storage media is seized or name of the person whose computer system is subject to search; b) name of the person having conducted the search; c) names of the persons present during the search conducting; d) a description and list of the computer systems or computer data storage media against which search was ordered; e) a description and list of the performed activities; f) a description and list of the computer data discovered on the occasion of the search; g) signature or stamp of the person having conducted the search; h) signature of the persons present during the search conducting. (14) Criminal investigation bodies have to take steps in order to make sure that the search is conducted without making facts and circumstances of the private life of the person subject to search public in an unjustified manner. (15) Computer data of a secret nature identified during such search is kept under the law. (16) During the trial, computer search is ordered by the court, ex officio or upon request by the prosecutor, by the parties or the victim, in the situations set by par. (2). A warrant for a computer search ordered by the

informatică dispuse de instanță se comunică procurorului, care	court shall be communicated to the prosecutor, who shall act as per par. (8) - (15).

Bibliography

English titles

Legislation

Declaration on Cooperation on Artificial Intelligence

The Coordinated Plan on Artificial Intelligence

Directive 95/46/EC (General Data Protection Regulation)

European Convention on Human Rights

Employment Equality Directive (2000/78/EC)

The Racial Equality Directive (2000/43/EC)

The Gender Goods and Services Directive (2004/113/EC)

The Gender Equality Directive (2006/54/EC)

Treaty on the European Union

Treaty on the Functioning of the European Union

Charter of Fundamental Rights of the European Union

National Strategy for the Romania Digital Agenda 2020, Government Decision no. 245 on the 7th of April 2015

Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Reports

FRA- European Union Agency for Fundamental Rights- Getting the future rights- Artificial Intelligence and Fundamental Rights

Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications prepared by the Committee of experts on Internet Intermediaries (msi-net)

Unboxing Artificial Intelligence: 10 steps to protect human rights (2019)- Commissioner for Human Rights

REPORT from 11.02.2021 summary of the activity for the year 2020, regarding Romanian GDPR related fines

The Digital Economy and Society Index- European Commission

Council of Europe, Guide to Human Rights for Internet Users

Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018 Brussels, 24.1.2018 COM(2018) 43 final

Digital resources

Holger Hembach, The difference between the ECHR and the EU Charter of Fundamental Rights, <<https://www.youtube.com/watch?v=3Q4i1ev4fl4>>, accessed 15 May 2021

Case law

Pine Valley Developments Ltd. And Others v Ireland App no 12742/87 (Commission Decision, 3 May 1989)

Çelik and İmret v. Turkey App no 44093/98 (ECtHR, 5 October 2004)

M.S. v. Sweden, App no 20837/92 (Commission Decision, 27 August 1997)

A.B. v. the Netherlands App no 37328/97 (ECtHR, 8 January 2002)

İlhan v. Turkey [GC] App no 22277/93 (ECtHR, 27 June 2000)

Colozza and Rubinat v. Italy App nos 9024/80 & 9317/81 (Commission decision, 9 July 1982)

Menesheva v. Russia App no. 59261/00 (ECtHR, 9 March 2006)

Kudła v. Poland App no. 30210/96 (ECtHR, 26 October 2000)

Fayed v. The United Kingdom App no. 17101/90 (ECtHR, 21 September 1994)

Golder v. The United Kingdom App no. 4451/70 (ECtHR, 21 February 1975)

Romanian titles

Legislation

Code of Criminal Procedure

Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)

Law no. 102/2005 on the set up, organisation and functioning of the National Supervisory Authority for Personal Data Processing – Republished

Law no. 287/2009 on the Civil Code

Books

Constantinescu M, Iorgovan A, Muraru I, Tănăsescu ES, *The Constitution of Romania revised – comments and explanations* (ALL BECK Publishing, 2004)

Case law

Sector 5 Bucureşti Civil Court decision no. 747/2019

ELSA SERBIA

Contributors

National Coordinator

Andela Bakula

National Researchers

Ana Memeti

Denis Knežević

Jelena Branković

Katarina Bakula

Milica Cvetković

Tatjana Kovačević

Tea Mladenov

Introduction

Technology is an integral part of people's lives, it is developing more and more and permeates all spheres. Unfortunately, an indispensable part of the development of technology is the violation of human rights, and there is a need for greater legal regulation of this issue. Every country on the globe, as well as the international community, has a very important task - to resolve this issue and to ensure the protection of fundamental human rights.

In this report we will try to present a picture of the real situation in the Republic of Serbia, where we are with the regulation, what are the advantages and disadvantages of our legal system and what awaits us in the future.

1. Which human rights issues do Advanced Digital Technologies pose in your country?

The Republic of Serbia does not have a procedure for human rights impact assessments, therefore, the issue that is the subject of consideration in this matter is not directly regulated by national regulations. However, our legislation regulates a significant range of human rights related to this topic.

In previous years, a massive decline in employees was recorded in Serbia due to the inflexibility of the labour market. The development of technology and a highly productive economy has made it known that adult education is at the core of the socio-economic transformation towards new tendencies based on technological development. Recording this, the Republic of Serbia passed The Law on the Fundamentals of the Education System.⁹⁰⁴ Modernity and development of artificial intelligence have led to the adoption of the Strategy for the Development of Artificial Intelligence,⁹⁰⁵ which regulates the issue of education and in this regard states: 'In addition to the field of artificial intelligence and its applications, education should respond to wider changes Although it is not possible to predict what the future labour market will be like at the level of individual jobs, there are some trends that can be guided by:

- Increasing multidisciplinary concerning classical divisions of occupations and competencies, especially linking knowledge and skills from the social-humanistic and artistic field with comprehension and expertise from the natural-mathematical and technical-technological field, data openness, shared data, possibilities of exploitation of

⁹⁰⁴ The Law on the Fundamentals of the Education System (*Official Gazette of the Republic of Serbia*, No.88/2017, 27/2018 - other laws, 10/2019, 27/2018 - other law and 6/2020);

⁹⁰⁵ Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025 (*Official Gazette of the Republic of Serbia*, No. 96/2019) ;

value from data, cooperation based on the use of data and data as a fuel for artificial intelligence;

- Methods and tools used in modern professional practice are an indicator of the direction of development that is happening under the influence of artificial intelligence and other technologies so that even when the impact on future occupations cannot be predicted clearly enough, the gap between what is learned in school and what are the methods and means of modern practice in the relevant field can be reduced.

As a separate human right in the Republic of Serbia, there is a right to the protection of personal data, which is regulated in Article 42 of the Constitution⁹⁰⁶ of the Republic of Serbia. Also, the Strategy encloses a plan of upcoming activities necessary to preserve the protection of personal data. It states the following: 'Artificial intelligence raises specific issues of personal data protection for both data used for machine learning and data processed through artificial intelligence. It is necessary to ensure that personal data is protected in the development phase of solutions based on artificial intelligence (data used for 'training') and data that are subsequently processed through an already trained system that uses new data. Within this measure, the key focus will be on developing an action plan and implementing the establishment of a practical diagram of the necessary steps to be taken about personal data protection in developing solutions based on artificial intelligence that will be applied equally in all sectors of society universities). Besides, certification of products and solutions based on artificial intelligence will be established to ensure the protection of personal data and compliance with international ethical standards. It is necessary to define and develop a certification program for solutions a) established by public administration bodies and b) the private sector that will provide security and ensure public confidence that the developed solutions are in accordance with the regulations governing the protection of personal data.'

The right to access the Internet can also be understood as a basic human right in modern times. In the Republic of Serbia it is regulated in the Law on Electronic Communications.⁹⁰⁷ The great potential and advantages of the Internet lie in its unique characteristics, such as speed, worldwide availability and relative anonymity of users. At the same time, these features of the Internet enable the dissemination of information in 'real-time' and the possibility of mobilising citizens, which has created a kind of fear among governments. This has led to increased restrictions on the Internet, the application of sophisticated technology to block content, monitor and identify activists and critics, criminalise legitimate expression, and adopt restrictive laws that justify such measures. This action is contrary to the obligations of states under the International Covenant on Civil

⁹⁰⁶ The Constitution of the Republic of Serbia (*Official Gazette of the Republic of Serbia*, No. 98/2006).

⁹⁰⁷ The Law on Electronic Communications, (*Official Gazette of the Republic of Serbia*, No. no. 44/2010, 60/2013 - decision of CC, 62/2014 and 95/2018 - other law) art. 4, para. 15.

and Political Rights, which guarantees the rights to freedom of expression.⁹⁰⁸ The Strategy for the Development of Electronic Communications⁹⁰⁹ of the Republic of Serbia provides guidelines for the transition from analogue to digital television broadcasting, presented through the development of a digital television signal distribution system, including the planning of the most favourable use of the digital dividend. Digitization will provide citizens with access to a variety of content, the convergence of services, new services for people with special needs, the elderly and members of national minorities.

The right to a fair trial in our law is regulated for the first time by the Charter on Human and Minority Rights and Civil Liberties,⁹¹⁰ which is an integral part of the constitutional Charter of the State Union of Serbia and Montenegro. After Serbia ratified the European Convention on 3 March 2004, the courts had the opportunity and obligation to apply Article 6 of the Convention, thus preventing possible violations of the right to a trial within a reasonable time, which was an extremely rare case. After the dissolution of the state union of Serbia and Montenegro, Serbia adopted the Constitution of the Republic of Serbia in 2006, which in Article 32, entitled 'The right to a fair trial', states: 'Everyone has the right to a public hearing before an independent and impartial tribunal within a reasonable time which will pronounce a judgment on their rights and obligations, the grounds for suspicion resulting in the proceedings instituted and the charges against them. Everyone is guaranteed the right to free assistance of an interpreter if the person does not speak or understand the language officially used in court and the right to free assistance of an interpreter if he or she is blind, deaf or mute. The press and the public may be excluded from all or part of the proceedings only in the interests of the protection of national security, public order and morals in a democratic society, the interests of minors or the protection of the privacy of parties, following the law.' Our country guarantees the right to a fair trial within a reasonable time - Article 18 of the Constitution of the Republic of Serbia stipulates: 'The Constitution guarantees, and as such, directly applies human and minority rights guaranteed by generally accepted rules of international law, ratified by international treaties and laws. The law may prescribe the manner of exercising these rights only if it is explicitly provided by the Constitution or if it is necessary for the exercise of a particular right due to its nature, whereby the law must not, in any case, affect the essence of the guaranteed right. The application of digital technology in this sphere can lead to a violation of the principle of equality, which forms the question of human discrimination.'

⁹⁰⁸ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue.

⁹⁰⁹ The Strategy for the Development of Electronic Communications (*Official Gazette of the Republic of Serbia*, No. 68/2010).

⁹¹⁰ Charter on Human and Minority Rights and Civil Liberties (*Official Gazette of SCG*, No. 6/2003-1), art. 17, para 2.

In the Republic of Serbia the prohibition of discrimination is perhaps even the most important human right, which is regulated primarily by the Constitution in Article 21, although it does not explicitly define the concept of discrimination. Also, the prohibition of discrimination is regulated in other Articles: 'It is provided that the Constitutional Court may prohibit a religious community only if its actions provoke and incite religious, national or racial intolerance',⁹¹¹ incitement and respect for differences,⁹¹² ban on inciting racial national and religious hatred⁹¹³, Article 50 refers to the freedom of the media, Articles 76 and 77 resolve the issue of national minorities in the Republic of Serbia. The prohibition of discrimination is also regulated by certain legal norms and in-laws such as: the Law on Protection of Rights and Freedoms of National Minorities,⁹¹⁴ the Law on Employment and Unemployment Insurance,⁹¹⁵ the Law on Public Information and Media,⁹¹⁶ the Law on Free Access to Information of Public Importance,⁹¹⁷ the Law on Higher Education,⁹¹⁸ the Law on Prevention of Violence and Misconduct at Sports Events,⁹¹⁹ the Labour Law,⁹²⁰ the Law on Health Care,⁹²¹ the Law on Execution of Criminal Sanctions,⁹²² the Family Law,⁹²³ the Law on Juvenile Delinquents and Criminal Protection of Juveniles,⁹²⁴ the Law on Churches and religious communities,⁹²⁵ and the Law on Prevention of Discrimination against Persons with Disabilities.⁹²⁶ The Law on Prohibition of Discrimination⁹²⁷ in the Republic of Serbia was adopted in 2009 and at the time of its entry into force, it represents a signpost for the Republic of Serbia to reach the standard of modern society.

⁹¹¹ The Constitution of the Republic of Serbia, art. 44.

⁹¹² *ibid*, art. 48.

⁹¹³ *ibid*, art. 49.

⁹¹⁴ The Law on Protection of Rights and Freedoms of National Minorities (*Official Gazette of the FRY*, No. 11/2002, *Official Gazette of Serbia and Montenegro*, No. 1/2003 CC and *Official Gazette of the RS*, No. 72/2009 - other law, 97/2013 - CC decision and 47/2018).

⁹¹⁵ The Law on Employment and Unemployment Insurance (*Official Gazette of the Republic of Serbia*, No. 36/2009, 88/2010, 38/2015, 113/2017 and 113/2017 - other law).

⁹¹⁶ The Law on Public Information and Media (*Official Gazette of the Republic of Serbia*, No. 83/2014, 58/2015 and 12/2016 - authentic interpretation).

⁹¹⁷ The Law on Free Access to Information of Public Importance (*Official Gazette of the Republic of Serbia*, No. 120/2004, 54/2007, 104/2009 and 36/2010).

⁹¹⁸ The Law on Higher Education (*Official Gazette of the Republic of Serbia*, No. 88/2017, 73/2018, 27/2018 - other law, 67/2019 and 6/2020 - other laws).

⁹¹⁹ The Law on Prevention of Violence and Misconduct at Sports Events (*Official Gazette of the Republic of Serbia*, No. 67/2003, 101/2005 - other law, 90/2007, 72/2009 - other law, 111/2009, 104/2013 - other law and 87/2018).

⁹²⁰ The Labour Law (*Official Gazette of the Republic of Serbia*, No. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - decision of CC, 95/2018 and 113/2017 - authentic interpretation ;.

⁹²¹ The Law on Health Care (*Official Gazette of the Republic of Serbia*, No. 25/2019).

⁹²² The Law on Execution of Criminal Sanctions (*Official Gazette of the Republic of Serbia*, No.55/2014 i 35/2019).

⁹²³ The Family Law (*Official Gazette of the Republic of Serbia*, No. 8/2005, 72/2011 - other law and 6/2015).

⁹²⁴ The Law on Juvenile Delinquents and Criminal Protection of Juveniles (*Official Gazette of the Republic of Serbia*, No. 85/2005).

⁹²⁵ The Law on Churches and religious communities (*Official Gazette of the Republic of Serbia*, No. 36/2006).

⁹²⁶ The Law on Prevention of Discrimination against Persons with Disabilities (*Official Gazette of the Republic of Serbia*, No. 33/2006 i 13/2016).

⁹²⁷ The Law on Prohibition of Discrimination (*Official Gazette of the Republic of Serbia*, No. 22/2009).

The Republic of Serbia ratified the European Convention on Human Rights in 2004, which also regulates human rights issues such as the right to a fair trial and 'legal proceedings',⁹²⁸ the right to privacy and data protection,⁹²⁹ the right to freedom of expression and information,⁹³⁰ and the right to protection against discrimination in the exercise of rights and freedoms.⁹³¹ In addition to the European Convention on Human Rights, it is a signatory to the International Covenant on Civil and Political Rights, which the Republic of Serbia ratified in 1974, as well as the International Covenant on Economic and Cultural Rights, which regulates the prohibition of discrimination in Articles 2 and 10, and the right to education in Article 13.

The Republic of Serbia does not have a developed field of advanced digital technology, therefore it is not developed in its legal acts, but as a candidate for EU membership it strives to develop in that field using artificial intelligence in many ways developing economy, culture and scientific staff and the very skills needed for the jobs they will be doing in, hopefully, the near future.

2. How is personal information protected in your national legislation?

In 2018 the Republic of Serbia implemented a new Law on Personal Data Protection⁹³² as the result of introducing different European standards in the field of data protection based on the General Data Protection Regulation and Police Directive. This law aims to work on raising standards of protection in this field. Even though personal data is protected by the Constitution⁹³³ of the Republic of Serbia, Article 42 paragraph 2 refers to the fact that personal data will be defined by the rule of law. The definition of personal data given in the Law on Personal Data Protection is synchronized with the definition from GDPR. Based on Article 4 of this Law *personal data* means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'. First of all, for data to represent personal data, it must be related to a natural person, which excludes legal entities from the scope of protection.⁹³⁴ Furthermore, by the definition given, it can be stated that it is not of importance how these data are

⁹²⁸ European Convention on Human Rights, art. 6.

⁹²⁹ *ibid*, art. 8.

⁹³⁰ *ibid*, art. 10.

⁹³¹ *ibid*, art. 14.

⁹³² The Law on Personal Data Protection (*Official Gazette of the Republic of Serbia*, No. 87/2018).

⁹³³ The Constitution of the Republic of Serbia, (*Official Gazette of the Republic of Serbia*, No. 98/2006).

⁹³⁴ Stefan Andonović, Dragan Prlja, *Osnovi prava zaštite podataka o ličnosti*, (Institute of Comparative Law, Belgrade 2020), 17.

known and what kind of factors influence it, but that based on information a person can be identified by the third person.

It must be stated that this new national legislation represents the improvement of protection in this field. Based on this law, the Republic of Serbia guarantees higher protection on personal data. Namely, with the implementation of GDPR principles, this law gives ‘explicit protection to the trade of goods and services on the internet’⁹³⁵ for the first time. In addition to this, there are many other influences of GDPR in this field such as ‘regulating automated processing data and so-called algorithmic decision making’ and ‘the new conditions for consent to data processing’. Based on Article 15 of the Law on Personal Data Protection,⁹³⁶ this consent must be given for the specific personal data and blank consent is not allowed. However, maybe the most important improvement as the result of the implementation of the GDPR standard is in the field of sanctions. Even though sanctions are not high as is predicted with the GDPR they are stricter than before. This is important for the Republic of Serbia as stricter sanctions can improve data protection.

However, this regulation is not completely synchronized with the GDPR and many aspects have to be improved. ‘The Law on personal data protection has not implemented the Preamble of the GDPR, which is important for better understanding of basic principles, human rights issues and basic institutes in this field’.⁹³⁷ This is important to be further developed by the rule of law especially in a country such as Serbia, with a low level of personal data understanding. Furthermore, video surveillance is not further developed and that can represent the issue for the years to come.

In conclusion, even though this regulation represents the best protection of personal data in the Republic of Serbia so far it is important to work on synchronizing national legislation with this law as well as working on these topics that are not regulated as in GDPR. ‘This Law provides an appropriate legal framework which will require a lot of theoretical consideration and practical application to completely fulfil the role of protector of privacy’.⁹³⁸

⁹³⁵ D. Krivokapic, J. Adamovic, D. Tasic, A. Petrovski, P. Kalezic, Dr. Đ. Krivokapic, *VODIČ KROZ ZAKON O ZAŠTITI PODATAKA O LIČNOSTI I GDPR TUMAČENJE NOVOG PRAVNOG OKVIRA*, 16; <https://www.sharefoundation.info/Documents/vodic_zzpl_gdpr_share_2019.pdf> accessed 10 March 2021.

⁹³⁶ The Law on Personal Data Protection, (*Official Gazette of the Republic of Serbia*, No 87/2018).

⁹³⁷ Andonović (n 935), 150.

⁹³⁸ *ibid.*

3. To which extent is the data protection self-regulated by the private sector in your country? How do the public and private sectors cooperate in this regard?

The Law on Personal Data Protection, following the example of the GDPR, introduces new institutes of self-regulation into our legal system: the possibility of drafting a code of conduct, the possibility of certification (issuing certificates on personal data protection), as well as the application of so-called binding business rules. Given that these are completely new legal institutes, the practice of the Commissioner for the Protection of Information of Public Importance (hereinafter: the Commissioner) and other actors in this field will develop only in the future.

The Law on Personal Data Protection introduces the possibility of drafting a code of conduct⁹³⁹ so that associations and other entities representing groups of handlers or processors can apply the regulation more efficiently. The Code Institute takes into account the specifics of data processing in the relevant industry sectors and the specific needs of small and medium-sized companies. Codes should regulate in more detail the principles of fair and transparent processing, to explain in more detail the legitimate interest of the controller as a legal basis for processing in a particular case, to further regulate the collection and pseudonymisation of personal data, and how data subjects are exercised data to other countries and international organisations, the manner of resolving disputes between the controller and the person to whom the data relate peacefully, describe in more detail the mutual obligations of the controller and the processor, etc. Since the drafting of codes of conduct is only a possibility, not an obligation, The Law on Personal Data Protection determines the obligation of the Commissioner to encourage and promote the drafting of such codes.⁹⁴⁰ A potential problem may arise when determining the entities that can develop a code of conduct. According to the Law, these are associations and other entities that represent groups of handlers or processors, which suggests that the Code may be drafted by an association as a separate legal entity established by the Law on Associations. Since this part of the Law was adopted in the image of the GDPR, it is necessary to keep in mind that the English word 'associations' is used in the GDPR, which has a different meaning in our legal system.

The authors of Guide⁹⁴¹ to the Law on Personal Data Protection believe that the GDPR intends to subordinate several different entities that are united on a common basis. Therefore, it could be concluded that the intention of the domestic legislator is the same - that the code refers to the self-regulation of the behaviour of several entities that connect

⁹³⁹ The Law on Personal Data Protection, (*Official Gazette of the Republic of Serbia*, No 87/2018), art. 59.

⁹⁴⁰ *ibid*, art. 78.

⁹⁴¹ Krivokapic (n 936) 69.

certain common circumstances, and not just one association. It remains to be seen whether the associations, as independent and separate legal entities, will independently adopt such codes of conduct in practice to regulate themselves.⁹⁴² In order to draft or amend a code of conduct, a draft code or its amendments shall be submitted to the Commissioner for opinion and consent. The Commissioner is also authorized to encourage the development of such a code, and if he considers that the code is in accordance with the Law and contains sufficient guarantees for the protection of personal data, the code of conduct or its changes will be registered and published on the Commissioner's website.

Article 60 of the Law on Personal Data Protection stipulates that the control of the application of the Code is performed by 'a legal entity accredited to perform control in accordance with the law governing accreditation'. In doing so, the control of such an accredited person does not affect the possibility of control and inspection powers that the Commissioner has concerning the code of conduct (encouraging the development of a code and giving opinions and consents to the code). This Law also prescribes the conditions that a legal entity must fulfil to be accredited, but it is unclear who are the legal entities that will control the application of the code if the possibility of drafting a code comes to life in practice (since drafting a code is not an obligation). If the controller or processor violates the code of conduct, the accredited legal entity may, among other measures, temporarily or permanently exclude the controller or processor from the application of the code, and is obliged to inform the Commissioner about the measures taken.

The second institute of self-regulation that the Law on Personal Data Protection introduced in Article 61 is the possibility of establishing a procedure for issuing certificates on personal data protection, in order to prove that the controller and processor comply with the provisions of the Law, especially taking into account the needs of small and medium companies. Therefore, the purpose of issuing a certificate is easier to prove that the controller, ie processor, has implemented this Law in its business and that it adheres to it, but the issuance of the certificate does not affect the rights and obligations of operators and processors under the Law, inspection authority nor other powers of the Commissioner. Certificates are issued by either the Commissioner or the so-called certification body,⁹⁴³ based on the criteria prescribed by the Commissioner. The certificate is issued for a maximum period of three years and may be renewed under the condition that the certificate holder continues to meet the criteria for its issuance. The trustee or certification body may revoke the certificate if it is determined that the certificate holder no longer

⁹⁴² *ibid.*

⁹⁴³ The Law on Personal Data Protection (*Official Gazette of the Republic of Serbia*, No 87/2018), art. 62.

meets the required criteria. The Commissioner maintains and publishes a list of certification bodies and issued certificates on his website.

The last institute of self-regulation introduced by the Law on Personal Data Protection in Article 67 are binding business rules, which represent internal data protection rules. They are adopted and applied by the controller, i.e. processor with residence or domicile, i.e. headquarters in the territory of the Republic of Serbia, to regulate the transfer of personal data to the controller or processor in one or more countries within a multinational company or group of economic entities. Binding business rules are approved by the Commissioner if such rules comply with the following requirements:

- They are legally binding, applicable to and enforced by any member of a multinational company or group of economic operators, including their employees;
- They explicitly ensure the exercise of the rights of data subjects in connection with the processing of their data;
- They define the structure, contact details of a multinational company or group of economic entities; transfer of personal data, types of personal data, actions and purpose of processing, persons to whom the data relate and the name of the country to which they are transferred; prescribe the obligation of their application; determine the application of general principles of protection of personal data and the rights of data subjects, as well as the ways of exercising such rights; powers of persons for protection of personal data; complaint procedure; manner of cooperation with the Commissioner, etc.

If the binding business rules meet the legal requirements, the Commissioner shall approve them within 60 days from the day of submitting the request for their approval.

With the adoption of the Law on Personal Data Protection, which is an adapted text of the GDPR, a major step forward has been made in the Republic of Serbia towards regulating data protection in the private sector. However, this Law is still not clearly defined enough and leaves many legal gaps, which should fill the interpretation of court practice in the coming years, as well as the practice of the Commissioner. The fact is that this Law is a true reflection of the level of awareness of the legal regulation of this issue in our country. Unfortunately, very few private sector companies have their own privacy policies. The second institute of self-regulation is more of an incentive character since private companies have no other benefit than to improve their reputation. What is good is that the certificate is issued for 3 years, which gives economic entities a motive to continue with good practice. The third institute actively involves the Commissioner for the Protection of Equality, thus suggesting for the first time public control over the rules applied by the private sector, which should result in harmonisation of rules applied by controllers or operators of multinational companies based in Serbia to the transfer of personal data operators or controllers of their company in one or more states. Considering all the above,

it can be expected that the Republic of Serbia will adopt even more European standards in this area in the coming period, but that path will be a debt, primarily due to a lack of understanding of court practice.

4. What is the process of judicial review of cases of data protection breaches?

Regulating data privacy is one of the most important assignments in a modern legal world full of digitisation where development of science and technology creates new methods to violate human rights. The right to data privacy is defined in our legal system, not cited as data privacy, but contained in many other rights in Law on Personal Data Protection⁹⁴⁴ of the Republic of Serbia from 2018 which protects individuals when it comes to processing personal data. 'Everyone has the right to respect for his private and family life, his home and his correspondence', according to the European Convention on Human Rights.⁹⁴⁵ Primarily, The Constitution of the Republic of Serbia avouches the right to data privacy.⁹⁴⁶

Based on GDPR,⁹⁴⁷ The Law on Personal Data Protection of the Republic of Serbia guarantees a list of rights for the individuals that personal data concerns that must be respected.⁹⁴⁸ The principle of transparency requires that any information that will be used in public must be easy to understand.⁹⁴⁹ Therefore, the Law on Personal Data Protection of the Republic of Serbia prescribes all the information that must be given to the data subject before processing them. Such as identity and contact information of the controller, contact information of the Commissioner for Information of Public Importance and Personal Data Protection, the purpose of processing data, and the legal basis for it, existence of the personal interest of the controller or the interested party, and also information about the addressee of the personal data, and If controller has the intentions to deliver personal data to the other country or organisation. Additionally, the controller can provide information about the duration of possessing personal data or possibility of complaint to the Commissioner for Information of Public Importance and Personal Data Protection.⁹⁵⁰ The right to access data, the next right, first implies that the data subject has the right to ask the controller for confirmation of whether the controller processes his data or not. Every person has an unconditional right to correction of incorrect data and addition of incomplete parts of personal data.⁹⁵¹ Amongst all the other rights, individuals must have

⁹⁴⁴ The Law on Personal Data Protection (*Official Gazette of the Republic of Serbia*, No. 87/2018).

⁹⁴⁵ European Convention on Human Rights, art. 8.

⁹⁴⁶ The Constitution of the Republic of Serbia (*Official Gazette of the Republic of Serbia*, No. 98/2006), article 42.

⁹⁴⁷ General Data Protection Regulation, EU (2016/679).

⁹⁴⁸ Krivokapic (n 936) 75.

⁹⁴⁹ General Data Protection Regulation, art. 58.

⁹⁵⁰ The Law on Personal Data Protection of the Republic of Serbia (*Official Gazette of the Republic of Serbia*, No. 87/2018), art. 22.

⁹⁵¹ *ibid*, art. 29.

the right to have their personal data erased and no longer processed and the right to object. If they consider that justified because of the particular situation in which they find themselves.⁹⁵² There are situations in which the data subject has the right to restrict data processing such as when the controller no longer needs the data, but the subject needs them to accomplish some legal requirement, or when processing is illegal, but the subject opposes deletion and requires restricted data usage. And also, the situation in which the subject disputes the accuracy of the data, during the time that enables the controller accuracy check. And at last, when the data subject has filed an objection to the processing, and in progress is assessment whether the legal basis for the processing by the controller outweighs the interests of that person. If the processing is limited, this data may be further processed only with the consent of the data subject.⁹⁵³ The right to data portability is an extension of the right of access, as it requires the controller to provide personal data in a structured, machine-readable and common format when that is requested by the subject, and the subject has the right to transfer them to another controller.⁹⁵⁴

When it comes to exceptions about data subject's possibility to restrict and object, the right of access may be restricted, partly or in general, only if necessary and with respecting the fundamental rights and legitimate interests of data subject, in order to:

- 1) avoid obstruction of official or legally regulated information collecting, investigation or proceedings;
- 2) enable the prevention, investigation and detection of criminal offences, prosecution of perpetrators of criminal offences or execution of criminal sanctions;
- 3) protect public safety;
- 4) protect national security and defence;
- 5) protect the rights and freedoms of other persons.⁹⁵⁵

Our law⁹⁵⁶ says: 'Personal data breach means a breach of the security of personal data which results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed'.⁹⁵⁷

The controller is obliged to inform the Commissioner for Information of Public Importance and Personal Data Protection about the data protection breaches without undue delay, or, if possible, within 72 hours of knowing of the violation.⁹⁵⁸ But, besides informing the Commissioner, If the violation of personal data can produce a high risk to the rights and freedoms of individuals, the controller is obliged to notify the data subject

⁹⁵² *ibid*, art. 30, 37.

⁹⁵³ Krivokapic (n 936), 77.

⁹⁵⁴ *ibid*, 78.

⁹⁵⁵ The Law on Personal Data Protection of the Republic of Serbia (*Official Gazette of the Republic of Serbia*, No. 87/2018), art. 28.

⁹⁵⁶ *ibid*.

⁹⁵⁷ *ibid*, art. 4.

⁹⁵⁸ *ibid*, art. 52;

without undue delay about the violation. The controller is obliged to describe in a clear and understandable way the nature of the data breach and to share the information such as description of possible consequences of the injury, a description of the steps taken by the controller or proposed to be taken. The controller is not obliged to inform the data subject if:

- 1) He has taken appropriate technical and organisational protection measures directed to the personal data whose security has been violated, and especially, If he has prevented the comprehensibility of data to all persons who are not authorized to access specified data
- 2) He has subsequently taken measures to ensure that the breach of personal data with a high risk to the rights and freedoms of the data subject can no longer produce consequences for that person
- 3) Notifying the data subject would be a disproportionate waste of time and resources. In that case, the controller is obliged to provide information to the data subject through public notification or in another effective way. If the controller has not notified the data subject of the personal data breach, the Commissioner may order the controller to do so.⁹⁵⁹

5. Does the review constitute effective protection of data privacy?

The regulations of the Law on Personal Data Protection⁹⁶⁰ of the Republic of Serbia from 2018, prescribe three ways respond to violations of any rights guaranteed by the same: inspection by the Commissioner for Information of Public Importance and Personal Data Protection, and the procedure conducted before the court that is competent concerning the type of decision made by the Commissioner in the performance of his inspection activity: misdemeanour proceedings and civil proceedings.⁹⁶¹

The Commissioner for Information of Public Importance and Personal Data Protection represents an independent body that is competent, among other things, to perform inspection supervision over the application of the regulations of the Law on Personal Data Protection.⁹⁶² The ultimate intention is to control whether the bodies or individuals who manage the personal data of certain individuals (data controllers or processors) act legally and correctly, i.e. whether the rights of these persons are endangered or violated, as well as to take all legal steps to remedy the identified violations. Such a procedure is initiated by the person whose data is manipulated or processed, or by the Commissioner himself.

⁹⁵⁹ *ibid*, art. 53.

⁹⁶⁰ The Law on Personal Data Protection (*Official Gazette of the Republic of Serbia*, No. 87/2018).

⁹⁶¹ Saša Gajin 'Zaštita podataka o ličnosti u sektoru bezbednosti. Vodič kroz zakonsku regulativu' (Organization for Security and Co-operation in Europe, 11 June 2019), 24 <[422618.pdf \(osce.org\)](#)> accessed 9 February 2019.

⁹⁶² *ibid*.

Inspection supervision is properly carried out with the regulations of the Law on Inspection Supervision,⁹⁶³ and the Law of General Administrative Procedure of the Republic of Serbia,⁹⁶⁴ and other laws.⁹⁶⁵ According to Article 8 of the Law on Personal Data Protection, the person whose data is processed, i.e. the person to whom the data relate, the controller, processor, or any other person to whom the decision of the Commissioner refers, has the right to promptly initiate a lawsuit before the Administrative Court within 30 days from the date of receipt of the decision. If the Commissioner does not act on the complaint within 60 days from the day of filing the complaint or does not inform the complainant about the course of the procedure or the result of the procedure, the data subject possesses the right to initiate an administrative dispute. It is significant to notice that the Commissioner, from the very beginning of his existence, has established a habitude in the sphere of data protection by publishing opinions, warnings, decisions in the procedure of inspection supervision. Furthermore, the Commissioner filed criminal charges, as well as requests to initiate misdemeanour proceedings in cases where there was a suspicion there was a violation of privacy rights or certain provisions of legal norms in the area of data protection. During his work, the Commissioner managed to formulate a critical way of making decisions, which influences not only the parties participating in the procedure but also the change of legal regulations.⁹⁶⁶ Thus, the Commissioner for Personal Data Protection on the occasion of a petition filed by an organisation in the Republic of Serbia, called CRTA, stating that the Regulatory Body for Electronic Media (REM) published e-mail addresses of applicants regarding the program content of media service providers, conducted a surveillance procedure and warned REM of violations of the Law on Personal Data Protection. In the supervision procedure, it was proven that REM, by its lawful powers, informed the applicants about the ultimate result of the procedure, but in such a manner that it submitted the answer to the formed mailing list, made up of email addresses of a tremendous number of applicants. In this path, each applicant came into ownership of an enormous number of e-mail addresses of other applicants.⁹⁶⁷

The Commissioner for Information of Public Importance and Personal Data Protection is also authorized to submit a request for initiating misdemeanour proceedings, per the valid

⁹⁶³ The Law on Inspection Supervision (*Official Gazette of the Republic of Serbia*, No. 36/2015, 44/2018 — other law and 95/2018).

⁹⁶⁴ The Law of General Administrative Procedure (*Official Gazette of the Republic of Serbia*, No. 18/2016 and 95/2018 — authentic interpretation).

⁹⁶⁵ The Law on Personal Data Protection (*Official Gazette of the Republic of Serbia*, No. 87/2018), art. 78.

⁹⁶⁶ Andonović, Prlja (n 31) 126.

⁹⁶⁷ Warning of the Commissioner for Information of Public Importance and Personal Data Protection no: 072-04-566/2019-07 < [Повереник је упозорио Регулаторно тело за електронске медије на незакониту обраду података о личности - Повереник за информације од јавног значаја и заштити података о личности \(poverenik.rs\)](#)> accessed 11 February 2021.

Law on Misdemeanours,⁹⁶⁸ if he finds that the provisions of the Law on Personal Data Protection have been violated. According to Article 84 of the Law on Personal Data Protection,⁹⁶⁹ the person to whom the processed data relates possesses the right to initiate action before the civil court by filing a lawsuit against the data controller or the processor if he considers that his right guaranteed by this Law has been violated by the processing.

Filing a lawsuit in court does not affect the right of this person to initiate other administrative or judicial protection proceedings. The procedure is initiated before a higher court in the location where the defendant or the plaintiff has a permanent or temporary residence (if it is a legal entity) unless the controller or processor is a public authority. The same article of this Law,⁹⁷⁰ prescribes in more detail the content of the lawsuits, so the plaintiff may request the court to oblige the defendant to provide information from Art. 22 to 27, Art. 33 to 35 and Article 37 of this Law; correction, i.e. deletion of data on the prosecutor from Art. 29, 30, and 32 of this Law; restriction of processing from art. 31 and 32 of this Law; providing data in a structured, commonly used and electronically readable form; transfer of data to another controller referred to in Article 36 of this Law; interruption of data processing referred to in Article 37 of this Law. Revision of ultimate decisions on the mentioned lawsuits is always allowed.

According to Article 86 of the Law on Personal Data Protection,⁹⁷¹ a person who has suffered material or non-material damage due to violation of the provisions of this Law, is entitled to monetary compensation from the data controller, i.e. the processor who caused the damage. The controller shall be liable for causing this damage, and the processor shall be liable only if he does not act under the obligations prescribed by this Law directly related to him, or when he acted outside the instructions or contrary to the instructions of the data controller. The data controller, i.e. the processor will be released from liability for damage if he proves that he is not responsible for the damage in any way. If the processing is performed by several controllers, i.e. the controller or the controller and the controller together, and if they are responsible for the damage, each controller is responsible for the sheer amount of damage. The relationship between several persons covered by one lawsuit is based on the principle of a joint and several liabilities. The data subject, in connection with the protection of personal data, asserts the right to authorize the representative of the association that deals with the protection of the rights and freedoms of the data subject to represent him in this procedure. The provisions of Article 87 of the Law on Personal Data Protection⁹⁷² prescribe the conditions for imposing fines for violating legal provisions.

⁹⁶⁸ The Law on Misdemeanours (*Official Gazette of Republic of Serbia*, No. 65/2013, 13/2016, 98/2016 — decision of the Constitutional Court, 91/2019 and 91/2019 - other law).

⁹⁶⁹ The Law on Personal Data Protection (*Official Gazette of the Republic of Serbia*, No. 87/2018).

⁹⁷⁰ *ibid.*

⁹⁷¹ *ibid.*

⁹⁷² *ibid.*

They are pronounced and applied in an effective, proportionate, and preventive manner. Their range is harmonized with the provisions of the Law on Misdemeanours,⁹⁷³ which regulates the misdemeanour responsibility.⁹⁷⁴

According to Article 87 of the Law on Personal Data Protection,⁹⁷⁵ when deciding on the imposition of fines and their amount, in each specific case must be taken care of: nature, severity and duration of the violation of the law, taking into account the type, scope and purpose of processing, as well as the number of data subjects and the level of damage which they suffered; the existence of specific intent or negligence of the offender; any action of the data controller and processor aimed at eliminating or mitigating the damage suffered by the data subjects; previous cases of violation of the provisions of this Law by the data controller and processor that are relevant for the imposition of the sentence; the degree of cooperation of the controller and processor with the Commissioner in order to eliminate the consequences of the violation of the law and to eliminate or mitigate the harmful consequences of the violation; the types of personal data to which the injuries relate; the manner in which the Commissioner learned of the violation, etc.

The authority to fine belongs to the Commissioner and the misdemeanour court. The Commissioner is empowered to impose a fine based on a misdemeanour order if during the inspection it determines that a misdemeanour has occurred for which the Law prescribes a fine in a determined amount. If the person to whom the Commissioner imposed a fine refuses to compensate it, following the provisions of the law governing misdemeanour liability, as well as if it is a misdemeanour for which the Law does not prescribe a specified fine, the procedure of determining misdemeanour liability and imposing a fine is in authority of competent misdemeanour court. Penalties for breach of the Law on Personal Data Protection are in a lower quantity than those prescribed by the General Regulation on Data Protection. The highest amount of the fine is 2,000,000 RSD, while the minimum fine is 50,000 RSD. If the data controller committed several injuries at the same time, in that case, the fine can amount to up to 4,000,000 RSD. Also, a fine of 100,000 RSD can be imposed on the data controller through a misdemeanour warrant. The amount of the penalty is specified according to the unique circumstances of the case.⁹⁷⁶ Criminal Code of the Republic of Serbia,⁹⁷⁷ prescribes a fine or imprisonment of up to one

⁹⁷³ The Law on Misdemeanours (*Official Gazette of the Republic of Serbia*, No. 65/2013, 13/2016, 98/2016 — a decision of the Constitutional Court of the Republic of Serbia, 91/2019 and 91/2019 — other law).

⁹⁷⁴ Gajin (n 962) 26.

⁹⁷⁵ The Law on Personal Data Protection (*Official Gazette of the Republic of Serbia*, No. 87/2018).

⁹⁷⁶ Jelena Adamović, Milica Jovanović, Petar Kalezić, Nevena Krivokapić, Bojan Perković, Andrej Petrovski 'Vodič za medije: Zaštita ličnih podataka i novinarski izuzetak', (Share foundation, Novi Sad, 2018), 55-57 <[guide-personal-data-protection-journalist-exemption-serbian.pdf \(irex.org\)](#)> accessed 15 February 2021.

⁹⁷⁷ Criminal Code of the Republic of Serbia (*Official Gazette of the Republic of Serbia*, No. 85/2005, 88/2005 - amended, 107/2005 - amended, 72/2009, 111/2009, 121/2012, 104/2013, 108 / 2014, 94/2016 and 35/2019).

year if someone unauthorisedly appropriates or uses personal data for a purpose other than the one for which they were obtained, i.e. when such data are collected and used against the law.⁹⁷⁸ Considering the effectiveness of the labour of these bodies, it can be announced that in 2019, the Commissioner filed three criminal complaints about the criminal offence under Article 146 of the Criminal Code of the Republic of Serbia (an unauthorized collection of personal data).⁹⁷⁹ Criminal complaints were filed against two officials in the Ministry of Internal Affairs of the Republic of Serbia and one against an in-charge person in one primary school. The Commissioner was informed that during 2019, one criminal report was rejected. This extended the tradition of predominantly rejecting the Commissioner's criminal charges due to the statute of limitations for prosecution. During 2019, the Commissioner submitted 23 requests for initiating misdemeanour proceedings due to breaching of the regulations of the Law on Public Procurement. Regarding all misdemeanour requests that he has submitted so far, the Commissioner during 2019 received 19 decisions of misdemeanour courts (16 first instance and 3 decisions of the second instance court). The penal policy of the misdemeanour courts during 2019 has noticeably tightened compared to 2018. During 2019, 10 lawsuits were filed with the Administrative Court against the Commissioner's decisions (8 lawsuits were filed against the decision rejecting the applicant's appeal as unfounded in whole or in part, 1 lawsuit was filed against the decision rejecting the appeal as unfounded and 1 lawsuit was filed by controller to whom the measure of temporary prohibition of data processing and elimination of irregularities has been imposed). In 2019, the Administrative Court resolved 5 lawsuits, rejecting 2 lawsuits, accepting 2 lawsuits and returning the case to the Commissioner for the retrial, and rejecting 1 lawsuit.⁹⁸⁰

Personal data protection in Serbia emphasizes the need for a systematic approach of all competent entities, which implies the formulation of a modern Strategy for personal data protection, as an official document and Action Plan for its implementation. Therefore, it is not just one regulation that is in the competence of only one or individual bodies, but it is about the application of all regulations that refer to the processing of personal data in almost all spheres of life.

⁹⁷⁸ Adamović, Jovanović, Kalezić, Krivokapić, Perković, Petrovski (n 977).

⁹⁷⁹ Criminal Code of the Republic of Serbia (*Official Gazette of the Republic of Serbia*, No. 85/2005, 88/2005 - amended, 107/2005 - amended, 72/2009, 111/2009, 121/2012, 104/2013, 108 / 2014, 94/2016 and 35/2019).

⁹⁸⁰ Report of the Commissioner for Information of Public Importance and Personal Data Protection on the Implementation of the Law on Free Access to Information of Public Importance and the Law on Personal Data Protection for the year 2019, Belgrade (march 2020)

<<https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2019/ENIzvestaj2019.pdf>> accessed 20 February 2021.

6. What is the process of judicial review of anti-discrimination cases?

The Law on Prohibition of Discrimination⁹⁸¹ of the Republic of Serbia stipulates that everyone who considers that she/he has been injured by discriminatory conduct has the right to file a lawsuit in a court of general local jurisdiction or in the court in whose territory the prosecutor's seat or residence is located. The provisions of the Law on Civil Procedure apply accordingly to this procedure. The procedure is urgent and revision is always allowed.

Many cases of discrimination, as well as non-implementation of affirmative measures established by law, are prescribed as misdemeanours and misdemeanour penalties are established by many legal regulations.⁹⁸² The misdemeanour procedure is initiated and conducted by the Misdemeanour Court, based on the request for initiating the misdemeanour procedure. This request is submitted by the authorized bodies or the injured party. The Commissioner for the Protection of Equality may also file a misdemeanour report.⁹⁸³ The Law on Prohibition of Discrimination also stipulates that protection against discrimination can be achieved by submitting a complaint to the Commissioner or the Protection of Equality, whose existence and jurisdiction are also determined by this law. The Commissioner for the Protection of Equality is elected by the National Assembly on the proposal of its Committee on Constitutional Affairs. He is elected for 5 years and must have at least 10 years of work experience in legal affairs in the field of human rights protection as well as undoubted moral and professional values. Responsibilities are to receive and consider complaints of violations of discriminatory laws, to inform the applicant of his right to sue, to file lawsuits with the consent of the person, to file misdemeanour charges, to warn the public of typical human rights violations, to submit an annual report to the National Assembly, to monitor the implementation of the law, to recommend measures to achieve equality.⁹⁸⁴

The procedure before the Commissioner for the Protection of Equality begins with the submission of a complaint by a person whose right has been violated. The complaint is submitted in writing with evidence of discrimination. The Commissioner initiates the procedure upon the application if no procedure has been initiated before the court on the same application. He will not act on the report if it is obvious that the violation does not exist, that the principle of *ne bis in idem* has been violated or that there is simply not enough evidence. The Commissioner may make a statement to establish the facts from any person

⁹⁸¹ The Law on Prohibition of Discrimination (*Official Gazette of the Republic of Serbia*, No. 22/2009).

⁹⁸² Dr. Nevena Petrušić, Kosana Beker, *Praktikum za zaštitu od diskriminacije*, Beograd, 2012, 56, <<http://www.ravnopravnost.gov.rs/wp-content/download/Praktikum.pdf>> accessed 12 March 2021.

⁹⁸³ The Law on Misdemeanours (*Official Gazette of the Republic of Serbia*, No. 65/2013, 13/2016, 98/2016 - CC decision, 91/2019 and 91/2019 - other law).

⁹⁸⁴ The Law on Prohibition of Discrimination (*Official Gazette of the Republic of Serbia*, No. 22/2009).

involved in the case. It is very important to note that the institution of mediation is incorporated into the system of protection against discrimination, so the Commissioner initiates the conciliation procedure. If the conciliation fails, the commissioner gives his opinion within 90 days on whether there has been a violation of rights and discrimination. If there have been violations, the Commissioner gives the person who committed discrimination 30 days to eliminate the violation of rights and inform him about it. However, the institution of the Commissioner is without the power to finally eliminate the violation of rights. In case the violator of the right does not act according to the order, the commissioner can only inform the public about it and issue a warning to him.⁹⁸⁵

7. Does your country have any specific regulations on Advanced Digital Technologies, such as big data, artificial intelligence (AI), Internet of Things (IoT) and/or encryption?

At the end of 2019, the Government of the Republic of Serbia adopted the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025⁹⁸⁶ (hereinafter: Strategy), which aims to use artificial intelligence (AI) in the function of economic growth, improvement of public services, the advancement of scientific staff, and development of skills for the jobs of the future. Also, the implementation of the Strategy measures should ensure that artificial intelligence in the Republic of Serbia is developed and implemented safely and by internationally recognised ethical principles, to exploit the potential of this technology to improve the quality of life of each individual and the society as a whole, as well as to achieve Sustainable Development Goals.⁹⁸⁷

The Strategy is in line with the European Artificial Intelligence Initiative,⁹⁸⁸ which sets out the European Commission's artificial intelligence policy. In this context, the Republic of Serbia, as a candidate for EU membership, but also as a participant in the European Union Framework Program for Research and Innovation, seeks to provide the necessary extent of compliance with the European Union, which will enable full integration into the European Research Area and closer cooperation.⁹⁸⁹

⁹⁸⁵ *ibid.*

⁹⁸⁶ Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025 (*Official Gazette of the Republic of Serbia*, No. 96/2019), 3.

⁹⁸⁷ In 2015, the countries adopted the 2030 Agenda for Sustainable Development and 17 global goals (Sustainable Development Goals).

⁹⁸⁸ "Artificial Intelligence for Europe", COM(2018) 237 final,

<<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>> accessed 13 March 2021.

⁹⁸⁹ Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025 (*Official Gazette of The Republic of Serbia*, No. 96/2019), 3.

This Strategy has five special objectives:⁹⁹⁰

- Development of education geared to the needs of modern society and economy conditioned by the advancement of artificial intelligence.
- Development of science and innovation in the field of artificial intelligence and its implementation
- Development of the economy based on artificial intelligence (where this is a key competence and where it is used in different industrial branches)
- Improvement of assumptions for the development of artificial intelligence and public sector services through the implementation of artificial intelligence
- Ethical and safe application of artificial intelligence

The Ministry of Education, Science and Technological Development will report semi-annually to the Artificial Intelligence Council on the implementation of goals and strategic measures envisaged by this strategy, and the Artificial Intelligence Council will report annually to the Government of the Republic of Serbia on the implementation status and potential opportunities or risks of implementation. Three-year action plans for implementation and reports on the implementation of this strategy will be prepared by the Ministry of Education, Science and Technological Development in cooperation with the Council for Artificial Intelligence, competent ministries, competent bodies and organisations, economy and faculties.⁹⁹¹ The first Action Plan⁹⁹² was adopted on 5 June 2020, and it represents a public policy document adopted for operationalisation and achievement of general and specific objectives of the aforementioned Strategy.

According to The Law on Personal Data Protection⁹⁹³ encryption is one of the measures that can be taken to protect personal data.

Encryption is becoming a general standard in protecting the security of information systems, i.e. data that are processed in the system. Local disk encryption refers to physical devices on which important data is stored as an additional method of protection, i.e. a new level of controlled access. In case of theft of computers or disks, encryption is a solid barrier to unauthorized access to data.⁹⁹⁴

As Big Data and IoT issues are not yet developed in the Republic of Serbia, no special legal acts regulating them have been adopted. However, if such an issue occurs, the above-mentioned Law will be applied.

⁹⁹⁰ *ibid*, 28.

⁹⁹¹ *ibid*, 60.

⁹⁹² Action Plan for the period 2020–2022 for the implementation of the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020–2025 (*Official Gazette of The Republic of Serbia*, No. 81/2020).

⁹⁹³ The Law on Personal Data Protection, (*Official Gazette of the Republic of Serbia*, No 87/2018).

⁹⁹⁴ Krivokapic (n 936), 56.

It can be stated that the Republic of Serbia is on a good path of adopting appropriate legal acts in the field of technology, and we hope that in the next few years it will reach a higher standard in this field.

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?

We live in a time that is very unpredictable and which with the development of technology has provided many favourable opportunities for an easier life, but it has also opened the door to the spread of crime to new spheres and the emergence of new crimes in all legislation in the world.

The process by which the source text is transformed into ciphertext is called encryption, and it is used to ensure that no user other than the user to whom the message is intended, cannot find out the content of the message. Source text encryption is performed using a specific encryption rule or cryptographic algorithm. Any cryptographic algorithm has the source text and key as input data and gives encrypted text as output. The procedure that allows the original source text to be obtained from the encrypted text is called decryption. Decryption is the inverse of encryption. An encrypted text for which no key is known is called a cryptogram.⁹⁹⁵ With the development of technology and together with the great spread of the Internet, privacy is urgently needed during the correspondence of two people, and there is a need for some of the data to remain hidden. However, over time, face data is becoming more accessible and entering the realm of privacy, revealing the exact location of faces, recording in a database photo sent via the Internet, as well as the content of messages exchanged between two users. Given that a large number of activities undertaken by an individual in the real world have 'moved' to the virtual, the concept of privacy in the form of a justified expectation of non-interference from unjustified monitoring of these activities should also be moved from reality to the cyber world. This is necessary, especially since personal data based on which users of electronic communications services can be identified (regardless of whether it is data that is consciously made available to the public or created independently of his will) is possible using modern techniques and methods. to use in unimaginable ways - to create a virtual identity of individuals - avatars whose existence the person is not even aware of.⁹⁹⁶ Guaranteeing the right to privacy by law protects individuals from excessive interference by society and the control of other individuals about the development and expression of their personality, but at the same time enables free participation in social life. In this sense, the online private sphere is not simply the 'infosphere' that surrounds each person but

⁹⁹⁵ Dragan Spasić, *Kriptozaštita podataka u računarskim mrežama primenom simetričnih i asimetričnih kriptosistema*, Direkcija za poštanski saobraćaj.

⁹⁹⁶ Milana Pisarić, *Zaštita prava na privatnost u vezi sa krivičnim postupkom*, Zbornik Matice srpske za društvene nauke 2016, Issue 154, 60.

encompasses ‘social and contextual complexities that mix and occur in technical systems’ and therefore activity data must not be collected in a way that jeopardizes its right to free development of personality.⁹⁹⁷

When standardizing the authorisations required for the detection and proving of criminal offences, it is necessary to take into account the protection of the rights of persons according to whom measures and actions have been taken. Although the restriction of certain human rights is justified by the needs of criminal procedure, it is completely legitimate, given that measures and actions taken to detect and prove modern forms of crime carry with them the risk of unprecedented invasion of privacy, it is considered to guarantee information privacy a very important question. If collective security cannot be achieved in any other way than by unjustified supervision and monitoring of all activities of users of electronic services and collection and processing of data on them, the freedom of individuals can no longer be discussed, because ‘full transparency (actions of state bodies) paralyses planning and action, and complete secrecy threatens both freedom and security.’ Given the ability of modern computing to collect, process, and store large amounts of data and their crossover and analysis, the question of controlling this process, the dimensions and scope of which were unthinkable before the development of computers, arose as a necessity. This is contributed not only by the amount of data collected but also by the fact that individuals do not know which state bodies it is and what is the reason for economic and other entities to collect data on them.⁹⁹⁸

The Law on Information Security⁹⁹⁹ in Articles 20 and 21 prescribes which authorities are competent when it comes to cryptography, as well as all the approvals required to decipher certain material. The Ministry of Defence is in charge of information security affairs related to the approval of cryptographic products, distribution of cryptographic materials and protection against compromising electromagnetic radiation, and affairs and tasks under the law and regulations adopted based on the Law. Measures of protection against compromising electromagnetic radiation (KEMZ) for handling secret data in ICT (Information and Communication System) systems are applied per the regulations governing the protection of classified data. Protection measures against KEMZ can be applied to their initiative by ICT system operators for whom it is not a legal obligation. For all technical components of the system (devices, communication channels, and premises) where there is a risk of KEMZ, which could lead to information security breaches, a check of protection against KEMZ, and assessment of the risk of unauthorized access to classified information through KEMZ is performed by the Ministry of Defence.¹⁰⁰⁰ Also,

⁹⁹⁷ *ibid*, 61.

⁹⁹⁸ *ibid*, 62.

⁹⁹⁹ The Law on Information Security (*Official Gazette of the Republic of Serbia*, No. 6/2016, 94/2017 i 77/2019).

¹⁰⁰⁰ *ibid*, Article 23.

the Law itself in Article 25 prescribes cryptographic protection measures, as well as when they are applied :

- Cryptosecurity measures for handling classified information in ICT systems are applied per the regulations governing the protection of classified information.
- Cryptographic protection measures may also be applied during the transfer and storage of data that are not marked as secret under the law governing data confidentiality when based on law or other legal acts it is necessary to apply technical measures restricting access to data and to protect data integrity, authenticity and indisputability.
- The Government, at the proposal of the Ministry of Defence, regulates technical conditions for cryptographic algorithms, parameters, protocols, and information goods in the field of cryptosecurity used in cryptographic products in the Republic of Serbia to protect secrecy, integrity, authenticity, and non-disclosure of data.
- Cryptographic products used to protect the transmission and storage of data designated as confidential, by the law, must be verified and approved for use. For their use, it is necessary to obtain an approval issued by the Ministry of Defence, while the Government, at the proposal of the Ministry, only specifies the conditions that need to be met when submitting the request for approval.
- Approval for a cryptographic product is issued by the Ministry of Defence, at the request of the ICT system operator, the manufacturer of the cryptographic product, or another interested person.
- Authorisation for a cryptographic product may relate to a single copy of the cryptographic product or to a specific model of the cryptographic product that is being mass-produced.
- Cryptographic product approval may have a validity period.

The Ministry of Defence decides on the request for issuance of approval for a cryptographic product within 45 days from the day of submitting a proper request, which can be extended in case of special complexity of verification for another 60 days. No appeal is allowed against the decision, but an administrative dispute may be initiated. The Ministry of Defence keeps a register of issued approvals for a cryptographic product. The register of personal data contains data on responsible persons, namely: name, surname, function, and contact data such as an address, telephone number, and e-mail address. The Ministry of Defence publishes a public list of approved cryptographic product models for all cryptographic product models for which it is stated in the application for approval that the cryptographic product model should be on the public list and if the request was submitted by the manufacturer or a person authorized by the cryptographic manufacturer. product. The Ministry of Defence may withdraw or change the conditions for the previously issued approval for a cryptographic product due to new knowledge related to technical solutions applied in the product, which affect the assessment of the degree of

protection provided by the product. The Government, upon the proposal of the Ministry of Defence, shall regulate in detail the content of the request for issuance of approval for a cryptographic product, conditions for issuance of approval for the cryptographic product, manner of issuance of approval, and content of the register of issued approvals for the cryptographic product. The register of persons performing cryptographic protection from personal data contains the following data on persons performing cryptographic protection: surname, father's name and first name, date, and place of birth, personal identification number, telephone, e-mail address, education, data on completed professional training for crypto security jobs, job title, start and end date of crypto security jobs. The Register of Cryptographic Materials for Handling Foreign Classified Information is maintained by the Office of the Council for National Security and Protection of Classified Information, under ratified international agreements. The government, at the proposal of the Ministry of Defence affairs, regulates the keeping of registers in more detail.

The balance between the interests of combating crime and the protection of the right to privacy is unstable. Changes in technological development facilitate the commission of serious crimes, which in turn requires a more prepared response from the state. The legitimacy of the processing of personal data for criminal proceedings is assessed with the principle of proportionality: to what extent the risk to general security can and to what extent justify the invasion of privacy rights. The question may be asked whether there is evidence to support the thesis that the use of such intrusive measures by the competent state authorities contributes to the detection and proof of serious crimes, which was used as the main goal and justification for introducing possibilities for the application of surveillance measures. in the form of the principle of proportionality. The answer is clear - it does not exist. It is unrealistic to expect that the state will give up the possibility of applying these measures and continue to justify their existence by the need to preserve security and prevent and suppress criminal acts. Judicial control of every measure is necessary, and for such control to be effective, judges need to understand the technical possibilities that are realized within each of the measures and the implications that these measures have for personal data and privacy.¹⁰⁰¹

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?

In order to modernize policymaking and socio-economic processes, the Government of the Republic of Serbia has adopted an ambitious Strategy¹⁰⁰² for Serbia until 2023.

¹⁰⁰¹ Milana Pisarić, *Zaštita prava na privatnost u vezi sa krivičnim postupkom*, Zbornik Matice srpske za društvene nauke 2016, Issue 154, 63.

¹⁰⁰² Strategy for Development of Networks of New Generations until 2023 (*Official Gazette of the Republic of Serbia*, No. 33/2018).

According to the given plan, the Ministry of Trade, Tourism and Communications is working on the digitalisation of primarily administrative services as well as overcoming the digital gap. According to the Secretary of State, Serbia has the goal of modernisation through several international projects supported primarily by the Chinese government and companies such as Huawei¹⁰⁰³, through which, according to the Strategy for Development of Networks of New Generations until 2023, Serbia will realize all the benefits of digitalisation. The strategy of digital development in Serbia, in addition to the general benefit that the population will have due to the digitalisation of services, also has the function of unifying the market and creating the so-called single market. Although we can agree that the digitalisation of services and innovation in the world of telecommunications make the life of modern man much easier, as the crisis caused by covid-19 has successfully proven, today it is more important than ever to be aware of all the risks posed by an online business and other activities in the digital space. Threats such as cybercrime, identity theft and many others have introduced a new obligation for governments: the establishment of specialized agencies and the introduction of new legislative processes aimed at protecting human rights on the Internet.

Aware of the importance of human rights protection in the digital world, the Republic of Serbia has passed several laws aimed at protecting both individuals and legal entities from cyber attacks. According to a survey¹⁰⁰⁴ conducted by the OSCE Mission to Serbia in 2015, it is estimated that Serbia, as a country where over 50% of the population uses the Internet, is not immune to technological attacks and cybercrime, which affects institutions, state administration and individuals alike.

To provide an opportunity for digital literacy, the OSCE Mission's Office, in cooperation with the civil sector, is organizing a series of educational forums aimed at helping people learn more about the protection of rights on the Internet and how to effectively protect them. The change in human rights legislation on the Internet primarily concerns the protection of children as the most vulnerable group. The Government of the Republic of Serbia passed the Decree on the safety and protection of children on the Internet¹⁰⁰⁵ on June 30, 2016. By adopting this act, the state has recognised the need to respond institutionally and take appropriate steps in the form of a concrete legislative process to protect the rights of children. A significant step in the protection of children was taken by

¹⁰⁰³ <<https://en.bfpe.org/in-focus/region-in-focus-focus/how-did-serbia-and-huawei-cooperate-a-chronology/>> accessed 31 May 2021.

¹⁰⁰⁴ <https://www.unicef.org/serbia/media/12526/file/Internet_and_Digital_Technology_Use_among_Children_and_Youth.pdf?fbclid=IwAR24LRXWIGHUQZ5vzIwhV9u75ZvIVKMUGCvh4qqHwZs27O-E6tzmBZLW5b8> accessed 31 May 2021.

¹⁰⁰⁵ Decree on the safety and protection of children on the Internet (*Official Gazette of the Republic of Serbia*, No. 61/2016).

the UNICEF office in Serbia, which by launching a volunteer service¹⁰⁰⁶ in 2020 provided free legal aid to parents whose children were exposed to cyber violence, as well as educational and assistance programs.

In 2019 UNICEF office in Serbia produced a digital guide¹⁰⁰⁷ on children safety online. According to joint research¹⁰⁰⁸ conducted by UNICEF and Telenor children in Serbia start using the internet very young, at the age of four or during early primary school years. Given the proven fact that children become Internet users at a very young age, a logical question arises as to their safety, which has become increasingly endangered in recent years. Advances in technology and the slow progress of legislative processes that regulate Internet security in Serbia are creating a breeding ground for cyber attacks, the victims of which are mostly minors.

The impunity of online attacks on children is made more obvious by the fact that parents often feel helpless in such situations. Namely, according to a survey¹⁰⁰⁹ by the UNICEF office, every fourth parent believes that they are not educated enough about the Internet and online security.

The Law on Personal Data Protection¹⁰¹⁰ is another legal act that protects the rights of individuals, and it aims to provide protection to every person in the territory of the Republic of Serbia in the field of personal data protection. This law strictly prohibits any kind of misuse of another person's identity for the purpose of performing a job or obtaining any benefit.

The conclusion is that a balance between the protection of human rights and digital progress exists in Serbia. Of course, as in any other legal branch, there are certain weaknesses and omissions, although Serbian legislation is going well on its way to achieving a sustainable balance between technological progress and comprehensive protection of human rights.

¹⁰⁰⁶ <<https://www.unicef.org/serbia/grupno-online-volontiranje>> accessed 5 March 2021.

¹⁰⁰⁷ <<https://digitalni-vodic.ucpd.rs/>> accessed 5 March 2021.

¹⁰⁰⁸ <<https://www.unicef.org/serbia/en/press-releases/childrens-safety-internet-focus-joint-project-telenor-and-unicef>> accessed 5 March 2021.

¹⁰⁰⁹ <<https://www.unicef.org/serbia/en/internet-and-digital-technology-use-among-children-and-youth-serbia>> accessed 5 March 2021.

¹⁰¹⁰ The Law on Personal Data Protection (*Official Gazette of the Republic of Serbia*, No. 87/2018).

10. Based on your analysis, how do you believe that legislation regarding the area of protecting human rights online will develop in the upcoming five years?

According to our analysis, and to the representation of protecting human rights online in our national legislation, there is only one possible direction- moving forward and developing noticeably more. Technology is improving every day and that is our reality, and also our future, which means that we will be facing some new, unexpected ways to violate human rights. The following period is crucial when it comes to observing which personal data is repeatedly breached and in which way, and also what are the recent methods and aims for data breach.

The first step in legislating this domain could be *numerus clausus*, prescribing and being aware of every possible way in which human rights can be violated. Also, including the list of the human rights that are and can be damaged. A legal framework that identifies human rights issues caused by the advanced digital technologies must be our priority. Predicting every possible way of data breach and protecting each and every right is a very profound, but highly important step in legislation, and, naturally, can not be expected to be done fast. We can expect serious legislative work on this topic, this problem of the modern world.

A great matter to do in the future period is also raising awareness amongst people about this problem, about the ways to protect oneself, about delicate situations in which their personal data is in danger to be exposed, and, above all, to whom they can turn to in case of personal data breach. Dealing with this serious problem requires being well informed about the current events, the ways, and the extent of personal data breach, primarily by the legislator, because of the function he has in solving this growing problem.

The best way, in general, to protect data subjects from further violations is enacting convenient law by the legislator and equal application of it.

Conclusion

The fact is that in this uncertain period of global digitalisation, which is woven into all pores of our society, in third world countries, and specifically in the Republic of Serbia, there are numerous indicators of ignorance of the population in the field of human rights and personal data. Affected by major global economic crises and the devastation of war in the last thirty years, it has affected the awareness and trust of citizens to such an extent that changes in the digital environment, which is present in everyday life, are not viewed favourably. violation of personal data and human rights in the internet environment. On the other hand, the implementation of the GDPR has had a positive impact on the formation of a new legislative framework in the field of human data protection in the

digital sphere. Namely, numerous laws have been passed - the Law on Digital Property, the Law on Data Secrecy, the Law on Personal Data Protection, the Law on Electronic Communications, etc. which show the readiness of the legislature, and even the state itself, to harmonize its regulations with world and European standards.

Table of legislation

Provision in Serbian language	Corresponding translation in English
Ustav Republike Srbije	The Constitution of The Republic of Serbia
Zakon o osnovama sistema obrazovanja i vaspitanja	The Law on the Fundamentals of the Education System
Zakon o Elektronskim komunikacijama	The Law on Electronic Communications
Zakon o zaštiti prava i sloboda nacionalnih manjina	The Law on Protection of Rights and Freedoms of National Minorities
Zakon o zapošljavanju i osiguranju u slučaju nezaposlenosti	The Law on Employment and Unemployment Insurance
Zakon o javnom informisanju i medijima	The Law on Public Information and Media
Zakon o slobodnom pristupu informacijama od javnog značaja	The Law on Free Access to Information of Public Importance
Zakon o visokom obrazovanju	The Law on Higher Education
Zakon o sprečavanju nasilja i nedoličnog ponašanja na sportskim događajima	The Law on Prevention of Violence and Misconduct at Sports Events
Zakon o radu	The Labour Law
Zakon o zdravstvenoj zaštiti	The Law on Health Care
Zakon o izvršenju krivičnih sankcija	The Law on Execution of Criminal Sanctions
Porodični zakon	The Family Law
Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica	The Law on Juvenile Delinquents and Criminal Protection of Juveniles
Zakon o Crkvama i verskim zajednicama	The Law on Churches and religious communities
Zakon o zaštiti podataka o ličnosti	Law on Personal Data Protection

Zakon o sprečavanju diskriminacije nad osobama sa invaliditetom	The Law on Prevention of Discrimination against Persons with Disabilities
Zakon o prekršajima	The Law on Misdemeanours
Zakon o inspekcijskom nadzoru	The Law on Inspection Supervision
Zakon o opštem upravnom postupku	The Law of General Administrative Procedure
Krivični Zakonik Republike Srbije	Criminal Code of the Republic of Serbia
Zakon o Zabrani diskriminacije	The Law on Prohibition of Discrimination
Zakon o informacionoj bezbednosti	The Law on Information Security
Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija	Decree on the safety and protection of children on the Internet
Strategija o razvoju elektronskih komunikacija u Republici Srbiji 2010-2020	The Strategy for the Development of Electronic Communications in the Republic of Serbia for the period 2010-2020
Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. godine	Artificial development strategy intelligence in the Republic of Serbia for the period 2020-2025

Bibliography

English titles

Legislation

European Convention on Human Rights

General Data Protection Regulation, EU (2016/679)

The International Covenant on Civil and Political Rights

The International Covenant on Economic and Cultural Rights

Reports

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue.

Digital resources

Artificial Intelligence for Europe, COM(2018) 237 final,
<<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>>

Serbian titles

Legislation

Ustav Republike Srbije (*Sl. glasnik RS*, br. 98/2006) / The Constitution of the Republic of Serbia, (*Official Gazette of the Republic of Serbia*, No. 98/2006).

Zakon o osnovama sistema obrazovanja i vaspitanja (*Sl. glasnik RS*, br. 88/2017, 27/2018 - dr. zakon, 10/2019, 27/2018 - dr. zakon i 6/2020) / The Law on the Fundamentals of the Education System (*Official Gazette of the Republic of Serbia*, No. 88/2017, 27/2018 - other law, 10/2019, 27/2018 - other law and 6/2020).

Zakon o zaštiti prava i sloboda nacionalnih manjina (*Sl. glasnik SRJ*, br. 11/2002, *Sl. list SCG*, br. 1/2003 - Ustavna povelja i *Sl. glasnik RS*, br. 72/2009 - dr. zakon, 97/2013 - odluka US i 47/2018) / The Law on Protection of Rights and Freedoms of National Minorities (*Official Gazette of the FRY*, No. 11/2002, *Official Gazette of Serbia and Montenegro*, No. 1/2003 - Constitutional Charter and *Official Gazette of the RS*, No. 72/2009 - other law, 97/2013 - CC decision and 47/2018).

Zakon o zapošljavanju i osiguranju u slučaju nezaposlenosti (*Sl. glasnik RS*, br. 36/2009, 88/2010, 38/2015, 113/2017 i 113/2017 - dr. zakon) / The Law on Employment and Unemployment Insurance (*Official Gazette of the Republic of Serbia*, No. 36/2009, 88/2010, 38/2015, 113/2017 i 113/2017 - other law).

Zakon o javnom informisanju i medijima (*Sl. glasnik RS*, br. 3/2014, 58/2015 i 12/2016 - autentična interpretacija) / The Law on Public Information and Media (*Official Gazette of the Republic of Serbia*, No. 83/2014, 58/2015 i 12/2016 - authentic interpretation).

Zakon o osnovama sistema obrazovanja i vaspitanja (*Sl. glasnik RS*, br. 88/2017, 27/2018 - dr. zakon, 10/2019, 27/2018 - dr. zakon and 6/2020) / The Law on the Fundamentals of the Education System (*Official Gazette of the Republic of Serbia*, No. 88/2017, 27/2018 - other law, 10/2019, 27/2018 - other law and 6/2020).

Zakon o slobodnom pristupu informacijama od javnog značaja (*Sl. glasnik RS*, br. 120/2004, 54/2007, 104/2009 i 36/2010) / The Law on Free Access to Information of Public Importance (*Official Gazette of the Republic of Serbia*, No. 120/2004, 54/2007, 104/2009 and 36/2010).

Zakon o visokom obrazovanju (*Sl. glasnik RS*, br. 88/2017, 73/2018, 27/2018 - dr. zakon, 67/2019 i 6/2020 - dr. zakoni); / The Law on Higher Education (*Official Gazette of the Republic of Serbia*, No. 88/2017, 73/2018, 27/2018 - other law, 67/2019 i 6/2020 - other laws).

Zakon o sprečavanju nasilja i nedoličnog ponašanja na sportskim događajima (*Sl. glasnik RS*, br. 67/2003, 101/2005 - dr. zakon, 90/2007, 72/2009 - dr. zakon, 111/2009, 104/2013 - dr. zakon i 87/2018) / The Law on Prevention of Violence and Misconduct at Sports Events (*Official Gazette of the Republic of Serbia*, No. 67/2003, 101/2005 - other law, 90/2007, 72/2009 - other law, 111/2009, 104/2013 - other law and 87/2018).

Zakon o radu (*Sl. glasnik RS*, br. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - odluka US, 113/2017 i 95/2018 - autentično tumačenje) / The Labour Law (*Official Gazette of the Republic of Serbia*, No. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - decision of CC, 95/2018 and 113/2017 - authentic interpretation).

Zakon o zdravstvenoj zaštiti (*Sl. glasnik RS*, br. 25/2019) / The Law on Health Care (*Official Gazette of the Republic of Serbia*, No. 25/2019).

Zakon o izvršenju krivičnih sankcija (*Sl. glasnik RS*, br. No. 55/2014 i 35/2019) / The Law on Execution of Criminal Sanctions (*Official Gazette of the Republic of Serbia*, No.55/2014 and 35/2019).

Porodični zakon (*Sl. glasnik RS*, br. 8/2005, 72/2011 - dr. zakon i 6/2015) / The Family Law (*Official Gazette of the Republic of Serbia*, No. 8/2005, 72/2011 - other law and 6/2015).

Zakon o maloletnim učinocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica (*Sl. glasnik RS*, br. 85/2005) / The Law on Juvenile Delinquents and Criminal Protection of Juveniles (*Official Gazette of the Republic of Serbia*, No. 85/2005).

Zakon o Crkvama i verskim zajednicama(*Sl. glasnik RS*, br. 36/2006)/ The Law on Churches and religious communities (*Official Gazette of the Republic of Serbia*, No. 36/2006).

Zakon o sprečavanju diskriminacije nad osobama sa invaliditetom (*Sl. glasnik RS*, br. 33/2006 i 13/2016) / The Law on Prevention of Discrimination against Persons with Disabilities (*Official Gazette of the Republic of Serbia*, No. 33/2006 and 13/2016).

Zakon o zaštiti podataka o ličnosti (*Sl. glasnik RS*, br. 87/2018) / The Law on Personal Data Protection, (*Official Gazette of the Republic of Serbia*, No 87/2018).

Zakon o inspeksijskom nadzoru (*Sl. glasnik RS*, br. 36/2015, 44/2018 — dr. zakon and 95/2018) / The Law on Inspection Supervision (*Official Gazette of the Republic of Serbia*, No. 36/2015, 44/2018 — other law and 95/2018).

Zakon o opštem upravnom postupku (*Sl. glasnik RS*, br. No. 18/2016 and 95/2018 — autentična interpretacija) / The Law of General Administrative Procedure (*Official Gazette of the Republic of Serbia* , No. 18/2016 and 95/2018 — authentic interpretation).

Zakon o informacionoj sigurnosti (*Sl. glasnik RS*, br. 6/2016, 94/2017 i 77/2019) / The Law on Information Security (*Official Gazette of the Republic of Serbia* , No. 6/2016, 94/2017 and 77/2019).

Krivični Zakonik Republike Srbije (*Sl. glasnik RS*, br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019) / Criminal Code of the Republic of Serbia (*Official Gazette of the Republic of Serbia*, No. 85/2005, 88/2005 - amended, 107/2005 - amended, 72/2009, 111/2009, 121/2012, 104/2013, 108 / 2014, 94/2016 and 35/2019).

Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija (*Sl. glasnik RS*, br. 61/2016) / Decree on the safety and protection of children on the Internet (*Official Gazette of the Republic of Serbia*, No. 61/2016).

Zakon o zabrani diskriminacije (*Sl. glasnik RS*, br. 22/2009) / The Law on Prohibition of Discrimination (*Official Gazette of the Republic of Serbia*, No. 22/2009).

Zakon o Elektronskim komunikacijama (*Sl. glasnik RS*, br. 61/2016), br. 44/2010, 60/2013 - odluka US, 62/2014 i 95/2018 - dr. zakon) / The Law on Electronic Communications, (Official Gazette of the Republic of Serbia, No. 44/2010, 60/2013 - decision of CC, 62/2014 and 95/2018 - other law).

Reports

Report of the Commissioner for Information of Public Importance and Personal Data Protection on the Implementation of the Law on Free Access to Information of Public Importance and the Law on Personal Data Protection for the year 2019, Belgrade (march 2020)

<<https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2019/ENIzvestaj2019.pdf>>

Milana Pisarić, *Zaštita prava na privatnost u vezi sa krivičnim postupkom*, Zbornik Matice srpske za društvene nauke 2016, Issue 154.

Books

Milan Paunović, Boris Krivokapić, Ivana Krstić, *Međunarodna ljudska prava*, Belgrade 2018.

Dragan Spasić, *Kriptozaštita podataka u računarskim mrežama primenom simetričnih i asimetričnih kriptosistema*, Direkcija za poštanski saobraćaj.

Milan Milosavljević, Saša Adamović, *Kriptologija 2*, University of Singidunum, Belgrade, 2014.

Andonović Stefan, Prlja Dragan, *Osnovi prava zaštite podataka o ličnosti*, (Institute of Comparative Law, Belgrade 2020).

Periodicals

Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. godine (*Sl. glasnik RS*, br. 96/2019); / Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025 (*Official Gazette of the Republic of Serbia*, No. 96/2019).

Akциони plan za period 2020–2022 za sprovođenje Strategije razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025 (*Sl. glasnik RS*, br. 81/2020); / Action Plan for the period 2020–2022 for the implementation of the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020–2025 (*Official Gazette of The Republic of Serbia*, No. 81/2020).

Strategija razvoja mreža novih generacija do 2023. godine (*Sl. glasnik RS*, br. 33/2018) / Strategy for Development of Networks of New Generations until 2023 (*Official Gazette of the Republic of Serbia*, No. 33/2018).

Strategija o razvoju elektronskih komunikacija u Republici Srbiji 2010-2020 (*Sl. glasnik RS* br. 68/2010) / The Strategy for the Development of Electronic Communications in the Republic of Serbia for the period 2010-2020 (*Official Gazette of the Republic of Serbia*, No. 68/2010).

Digital resources

D. Krivokapic, J. Adamovic, D. Tasic, A. Petrovski, P. Kalezic, Dr. Đ. Krivokapic, VODIČ KROZ ZAKON O ZAŠTITI PODATAKA O LIČNOSTI I GDPR TUMAČENJE NOVOG PRAVNOG OKVIRA,

<https://www.sharefoundation.info/Documents/vodic_zzpl_gdpr_share_2019.pdf>.

Gajin Saša 'Zaštita podataka o ličnosti u sektoru bezbednosti. Vodič kroz zakonsku regulativu' (Organization for Security and Co-operation in Europe, 11 June 2019)

<[422618.pdf \(osce.org\)](https://www.osce.org/data-protection)>

Warning of the Commissioner for Information of Public Importance and Personal Data Protection no: 072-04-566/2019-07 < [Повереник је упозорио Регулаторно тело за електронске медије на незакониту обраду података о личности - Повереник за информације од јавног значаја и заштиту података о личности \(poverenik.rs\)](https://poverenik.rs/izjave/2019/07/24/Poverenik-je-upozorio-Regulatorno-telo-za-elektronске-mediје-na-nezakonitu-obradu-podataka-o-lichnosti-Poverenik-za-informacije-od-javnog-znacza-a-i-zastitu-podataka-o-lichnosti)>

Adamović Jelena, Jovanović Milica, Kalezić Petar, Krivokapić Nevena, Perković Bojan, Petrovski Andrej 'Vodič za medije: Zaštita ličnih podataka i novinarski izuzetak', (Share foundation, Novi Sad, 2018)

<[guide-personal-data-protection-journalist-exemption-serbian.pdf \(irex.org\)](https://www.sharefoundation.org/wp-content/uploads/2018/06/guide-personal-data-protection-journalist-exemption-serbian.pdf)>

Dr. Nevena Petrušić, Kosana Beker, *Praktikum za zaštitu od diskriminacije*, Beograd, 2012

<<http://www.ravnopravnost.gov.rs/wp-content/download/Praktikum.pdf>>



The European Law Students' Association