



INTERNATIONAL LEGAL RESEARCH GROUP ON HUMAN RIGHTS & TECHNOLOGY VOL II

elsa

The European Law Students' Association
BULGARIA

elsa

The European Law Students' Association
FINLAND

elsa

The European Law Students' Association
GEORGIA

elsa

The European Law Students' Association
GREECE

elsa

The European Law Students' Association
THE NETHERLANDS

elsa

The European Law Students' Association
NORTH MACEDONIA

International Legal Research Group on Human Rights and Technology

Vol. II

Reporting Countries:

ELSA Bulgaria

ELSA Finland

ELSA Greece

ELSA Georgia

ELSA The Netherlands

ELSA North Macedonia

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

Bojana Rusevska
Elene Ghudushauri
Evangelos Avdoulas
Hanna Järvinen
Remina Aleksieva
Uejanaua Tjijumino

National Academic Supervisors

Atanas Kirov
Daniela Ilieva
Fani Dimoska
Jenni Hakkarainen
Maria Jose Recalde-Vela
Otar Chakhunashvili
Petya Peteva
Spiros Tassis

Linguistic Editors

Andrea Rodrigues	Nata Berianidze
Emma Bowar	Parthabi Kanungo
Ilia Danai Tsigkri	Polina Vladimirova
Iva Ivanova	Remina Aleksieva
Lara Siminovski	Simranjit Kaur
Laura Vuorinen	

Technical Editors

Blagovest Ilchevski
Elke van der Heijden
Evangelos Avdoulas
Pawel Tarnowski
Stefana Feciuc

Researchers and Authors

Anastasia Nefeli Vidaki	Annika Antikainen
Anas A. Qazi	Brianna Muir

Chrysi Chatzivasileiou	Maria Oikonomou
Dimitra Vasileiadou	Makrygianni
Elena Petkovska	Maria Roussi
Gergana Urumova	Maria Vasileia
Georgia Lynch	Karampatsoli
Hanna Järvinen	Max Schaetzel
Heidimaria Manninen	Mikael Hitruhin
(Hanh Ha) Nguyen	Mitko Tatarov
Nguyen	Natália Racková
Ilmari Eskola	Pinja Oksanen
Iva Ivanova	Polina Vladimirova
Ivona Stojcevska	Remina Aleksieva
Jagoda Frost	Rusudan Tsagarel
Jari van den Berg	Sofia Aalto-Setälä
Jovica Dimitroski	Susan Saarinen
Ketevan Makharashvili	Tatiana Kyttaroudi
Konstantinos Apostolos	Tom Hartmann
Maia Mamaladze	Vasiliki Tsiompanidou
Maja Veljanova	Youmna Osama Mohamed
	Ahmed Hassanein

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	12
ELSA BULGARIA	14
Introduction	15
1. Which human rights issues do Advanced Digital Technologies pose in your country?	15
2. How is personal information protected in your national legislation?	17
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?	19
4. What is the process of judicial review of cases data protection breaches?	21
5. Does the review constitute effective protection of data privacy?	24
6. What is the process of judicial review of anti-discrimination cases?	27
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?	29
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	31
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	33
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?	35
Conclusion	36
Table of legislation	37
Bibliography	51
ELSA FINLAND	53
Introduction	54
1. Which human rights issues do Advanced Digital Technologies pose in your country?	55
2. How is personal information protected in your national legislation?	56
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?	58
4. What is the process of judicial review of cases data protection breaches?	61
5. Does the review constitute effective protection of data privacy?	63
6. What is the process of judicial review of anti-discrimination cases?	66
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?	68
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	71
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	74
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?	77
Conclusion	78
Table of legislation	81
Bibliography	83
ELSA GEORGIA	92

Introduction	93
1. Which human rights issues do Advanced Digital Technologies pose in your country?	93
2. How is personal information protected in your national legislation?	94
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?	97
4. What is the process of judicial review of cases of data protection breaches?	98
5. Does the review constitute effective protection of data privacy?	102
6. What is the process of judicial review of anti-discrimination cases?	103
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?	107
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	108
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	112
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?	114
Conclusion	114
Table of legislation	116
Bibliography	117
ELSA GREECE	120
1. Which human rights issues does Advanced Digital Technologies pose in your country?	121
2. How is personal information protected in your national legislation?	122
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?	136
4. What is the process of judicial review of cases data protection breaches?	143
5. Does the review constitute effective protection of data privacy?	146
6. What is the process of judicial review of anti-discrimination cases?	153
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?	165
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	185
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	192
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?	207
Table of legislation	209
Bibliography	224
ELSA THE NETHERLANDS	232
1. Which human rights issues do Advanced Digital Technologies pose in your country?	233
2. How is personal information protected in your national legislation?	238
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?	242
4. What is the process of judicial review of cases of data protection breaches?	247
5. Does the review constitute effective protection of data privacy?	253

6. What is the process of judicial review of anti-discrimination cases?	259
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?	265
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	270
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	275
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?	279
Conclusion	283
Table of legislation	286
Bibliography	321
ELSA NORTH MACEDONIA	330
1. Which human rights issues do Advanced Digital Technologies pose in your country?	330
2. How is personal information protected in your national legislation?	332
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?	334
4. What is the process of judicial review of cases data protection breaches?	336
5. Does the review constitute effective protection of data privacy?	338
6. What is the process of judicial review of anti-discrimination cases?	339
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?	341
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations?	343
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online?	344
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?	348
Conclusion	349
Table of legislation	350
Bibliography	367

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 BULGARIA

Contributors

National Coordinator

Remina Aleksieva

National Academic Supervisors

Associate Professor Dr. Daniela Ilieva

Petya Peteva

Atanas Kirov

National Researchers

Gergana Urumova

Iva Ivanova

Polina Vladimirova

Remina Aleksieva

National Technical Editor

Blagovest Ilchevski

National Linguistic Editor

Polina Vladimirova

Remina Aleksieva

Iva Ivanova

Introduction

Advanced digital technologies are prevalent in the modern world. They are a necessity and solve many issues that we encounter in our daily lives. They have proven to be extremely beneficial for us and for this reason their continuous development will further grow. Nonetheless, the implementation of advanced digital technologies gives rise to new issues which the modern world has not faced yet. The legislative framework on a national and international level is still ill-equipped to answer to all the threats posed by advanced digital technologies and to afford the required level of protection to human rights. This is partly due to the rapid pace of development of advanced digital technologies which impedes the legislative efforts from catching up. Although there are fields which still need to be regulated, the world community has come up to some extent with answers relating to the threats posed by advanced digital technologies.

The purpose of the current analysis enunciates the applicable national legal framework of the Republic of Bulgaria towards advanced digital technologies and to examine to what extent human rights are protected in this context. Firstly, the human rights threats and issues posed by such technologies will be reviewed. The focus will then be shifted towards personal data and the protection victims of violations thereto can seek. A summary of the judicial review of the proceedings in relation to anti-discrimination cases will be provided, followed by an in-depth look into big data, artificial intelligence, internet of things and encryption. Lastly, an evaluation of the balance reached between allowing digital advancements and protecting human rights as well as the overall condition of the legal framework will be presented with a prediction of the future legislative changes.

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

The protection of human rights is the cornerstone of modern constitutions. The first task of modern democracies is to secure fundamental rights to individuals at times of riveting technological development. Digital technologies constantly evolve and penetrate into all spheres of life and require adequate and timely measures for widespread implementation. The accelerated digital transformation is a prerequisite for governments to rethink the approach to exploiting the potential of cyber telecommunications, increase demand, supply, and efficiency of public services, and successfully overcome the main social challenges. Modern democracies face numerous challenges and threats arising in the advanced digital age and address as a key priority the protection of human rights.

The most common human rights issues are related to freedom of speech, including online (freedom of expression), breach of the right to privacy, discrimination, and dissemination of hate speech violating the right to human dignity. Freedom of speech is secured under Article 39 of the Constitution of the Republic of Bulgaria.¹ It is an absolute right as it cannot be exercised to violate the rights and good name of other people, to incite towards

¹ Constitution of the Republic of Bulgaria, Article 39 (1).

a violent change of the constitutional foundation, to incite towards the commission of crimes and to exert abuse over a person.² Moreover, the freedom of speech is safeguarded under the European Convention on Human Rights which is ratified by and in force for the Republic of Bulgaria.³

In the context of advanced digital technologies, freedom of speech is threatened by the intelligent algorithms employed by certain social media and websites which track and examine the content disseminated online. These algorithms happen to takedown or block content not conforming to the policy of the website or social media. Although users are required to consent to the terms and conditions upon using those platforms, there are cases in which the infringement of freedom of speech is disproportionate.

In a recent decision - № 8 from 15. November 2019, the Bulgarian Constitutional Court declared the assessment criteria set forth by Article 25h (2) from the Personal Data Protection Act to be unconstitutional. In particular, the criteria were found to be unclear and therefore creating unpredictability and legal uncertainty, restricting the freedom of expression. The Court extended that when measures cause restrictions over any fundamental right, it is incompatible with the EU Charter of Human Rights. In conclusion, in an area which the national legislation is not heavily covered, censorship could violate the above-mentioned rights if applied. Hence, it is banned on a constitutional level under Article 40, Paragraph 1.⁴

Processing of personal data can also cause human rights issues in the context of advanced digital technologies. Generally, individuals in the Republic of Bulgaria enjoy a high standard of protection with respect to their personal data as there is legislation on both national and European level. On the national level, the Personal Data Protection Act is guaranteeing the safety of personal data and on European level – Regulation (EU) 679/2016. Nonetheless, issues in relation to the right to protection of personal data and the right to private life in a broader context can arise. Profiling is a prohibited practice which is in direct violation of processing personal data. The threats in connection to advanced digital technologies arise when profiling is conducted by an algorithm with sufficiently big data access. This risk must not be overseen as it is contrary to the standards set out by the relevant national and European legislature.

Lastly, advanced digital technologies pose a threat in respect to the prohibition of discrimination and dissemination of hate speech. This can be seen in numerous examples. Most notably, social media platforms use intelligent algorithms in order to curate the newsfeed of each and every user to their individual preferences. Over a long period of time, this practice can incite users to disseminate hate speech or exercise discrimination. Therefore, websites and social media platforms using such algorithms must employ means for protecting the end users.

² *ibid* art. 39 (2).

³ European Convention on Human Rights, Article 10.

⁴ Constitution of the Republic of Bulgaria, Article 40 (1).

The examined issues endangering human rights are the most prevalent with respect to advanced digital technologies and more effort is needed on behalf of the Republic of Bulgaria in order for the country to effectively combat these challenges.

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

The protection of personal data is a fundamental right originally enshrined in the Treaty on the Functioning of the European Union (TFEU)⁵ and the Charter of Fundamental Rights of the European Union. The protection of individuals in respect of processing of their personal data is provided in Article 8 of the Charter of Fundamental Rights, which states that ‘everyone has the right to the protection of his personal data’.⁶ According to Article 16, paragraph 1 of the Treaty on the Functioning of the European Union ‘everyone has the right to protection of his personal data’.⁷ Article 1, paragraph 1 of Directive 95/46, which has already been repealed, stipulated that ‘member states shall protect the fundamental rights and freedoms of individuals, and in particular their right to privacy with regard to the processing of personal data’.⁸

On 27 April 2016, a significant reform of the data protection rules in the European Union took place, updating Directive 95/46/EU by amending the Regulation (EU) 2016/679 (General Data Protection Regulation). The new legal framework retains several fundamental principles and concepts from the existing legislation, but at the same time introduces higher standards of protection and expands the scope of the rights of individuals and the obligations of personal data controllers. The provision of Article 4 of the GDPR defines the meaning of the term ‘personal data’ as ‘information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is an identifiable person, directly or indirectly, in particular by means of an identifier such as name, identification number, location data, online identifier or one or more features specific to the natural person, the physiological, genetic, mental, intellectual, economic, cultural or social identity of that individual’.⁹

The GDPR applies to any natural or legal person, any public authority or another body, to which personal data are disclosed, according to Article 4, paragraph 9. Since the GDPR provides protection in all EU countries, Bulgaria included, the location of the processing of collected personal data is irrelevant. That being said, any of the above-mentioned who offers goods and/or services to citizens of the European Union and processes their personal data but is established outside the EU, is still obliged to comply with the provisions enshrined in the GDPR.

On the 25th of May 2018, a common personal data protection legislation was introduced at EU level. The GDPR is a significant step towards effectively safeguarding the rights of the individuals in the digital age. This single piece of legislation at supranational level

⁵ Treaty on the Functioning of the European Union, Article 16 (1).

⁶ Charter of the Fundamental Rights of the European Union, Article 8.

⁷ Treaty on the Functioning of the European Union, Article 16 (1).

⁸ Directive 95/46/EC, Article 1 (1).

⁹ Regulation (EU) 2016/679, Article 4 (1).

reconciled the various national provisions addressing personal data and enforces a uniform legal order in this field. In fact, the Republic of Bulgaria adopted its Personal Data Protection Act (PDPA) in early 2002, which safeguards personal data at national level in compliance with GDPR. This was even before Bulgaria was a member State of the Council of Europe and signed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (The Convention No 108).

Due to Bulgaria's implementation of the GDPR into the Personal Data Protection Act, there are many requirements related to data processing such as for employment purposes. They include employers' prohibition to either make or keep on files of employee's personal identification documents unless explicitly required by law. If they do otherwise and the processed data is not related to the employment relationship, they must justify their legitimate interest or seek the employee's consent.¹⁰ Employers must also adopt internal policies regulating whistleblowing systems, acceptable and restricted use of internal resources such as IT systems, devices, etc.¹¹ Another requirement is that data controllers are not allowed to copy ID cards, driving licenses, or residence permits, except if otherwise provided for by law.¹² The personal identification number also cannot be publicly accessible unless otherwise provided by law.¹³ Owing to the PDPA a minimum age of 14 for valid consent is set and in case it is under this span parental consent is required.¹⁴ There is an exception in regard to processing personal data, included in the Measures Against Money Laundering Act. Article 83, paragraph 1 of the above-mentioned act explicitly orders that in relation to the processing of personal data for the purposes of the prevention of money laundering and terrorist financing GDPR and PDPA are applicable.

When data processing is performed without legal grounds, the recipient must return the personal data to the data subject or destroy the data within one month of learning of the illegal processing.¹⁵ If a data subject's rights are violated under the GDPR or the Act, the data subject is entitled to file an appeal with the PDPC, Inspectorate or the court, within six months of becoming aware of the violation, but no later than two years from the date of the violation.¹⁶

The PDPA provides for the constitution of the Commission for Personal Data Protection (the Commission) in Article 6.¹⁷ The Commission protects data subjects with respect to the processing of their personal data. The Commission oversees the compliance with the GDPR and the PDPA. It is also empowered to implement state policy in the field of personal data protection.

The Commission developed the 'Horizon 2022' strategy, which aims to reduce and even prevent illegal personal data processing. The strategy envisages effective mechanisms for

¹⁰ Personal Data Protection Act, Article 25a.

¹¹ *ibid* art. 25i.

¹² *ibid* art. 25d.

¹³ *ibid* art. 25b.

¹⁴ *ibid* art. 25c.

¹⁵ *ibid* art. 25a.

¹⁶ *ibid* art. 38, para. 1.

¹⁷ *ibid* art. 6.

supervision, training in the field of personal data protection, and stimulating international cooperation. Another adapted instrument is the “National CyberSecurity Strategy“ Cyber Resilient Bulgaria” 2020 aiming to establish network and information security, improving the protection infrastructures by system modernization, developing better cooperation with NGOs and international partnership with EU, NATO, OSCE, UN etc. It also targets legal and regulatory framework standardization and boosting the awareness and cyber education.

In order to ensure compliance of the Bulgarian legal framework with the EU’s personal data protection legislation, an Amendment and Supplement Act to the Personal Data Protection Act was drafted and presented by The Ministry of Interior for public consultations. The endeavor was successful, and the project was introduced to the Parliament by the Council of Ministers on the 18th of July 2018.

The Amendment and Supplement Act transposes Directive (EU) 2016/680 of the European Parliament and of the Council introducing the latest requirements towards personal data protection in the national legislative framework. Thus, the Republic of Bulgaria is in compliance with its obligations stemming from its membership in the EU and affords citizens and legal persons alike the highest standard of protection of their personal data.

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?

In today’s technologically advanced society, data protection is considered part of the general protection of privacy according to the European Convention on Human Rights (ECHR).¹⁸ Furthermore, according to Article 12 of the Universal Declaration of Human Rights, the right to privacy is a fundamental human right.¹⁹ While there is no denying that the digital advancements are beneficial to our society, they are progressively challenging the regulation of data and human autonomy.

Historically, the regulation of data protection in the public sector has been stricter than in the private sector. The reason for this may be that initially the focus of the protection of human rights was to protect the individual from the state, not from private actors. Any lack of regulation, however, may enable a private enterprise to endanger the privacy of the individual’s data. Therefore, it is necessary to enact a legislative framework through which human rights are safeguarded from every type and form of violation.²⁰

In Bulgaria, the legal apparatus is faced with different challenges regarding regulating the protection of privacy. Our country’s old legislation has been updated to comply with the requirements of GDPR, and repealing Directive 95/46/EC. Bulgaria’s relevant legislation includes the PDPA, which was significantly amended on the 29th of February 2019 with the

¹⁸ Peter Blume, ‘Data Protection in the Private Sector’ [2015] 298.

¹⁹ Universal Declaration of Human Rights, Article 12.

²⁰ Blume (n 18) 298.

Amendment and Supplement to the Personal Data Protection Act, the Electronic Communications Act in force as of the 25th of May 2007, Rules of Procedure of the Commission for Personal Data Protection and its Administration in force as of the 10th of February 2009 and Instruction № 1 of the 21st of December 2016 on the Circumstances in which the Enterprise, Provision of Public Electronic Communications Services, Notification of Users for Breaches of Personal Data Security, Format and Manner of Notification in force as of the 6th of January 2017. The relevant pre-GDPR legislation has been revised.²¹

Regarding the private sector, national legislation concerning data privacy is again bound by the rules that are applicable also for the public sector in accordance with the European legislation.

In the context of employment in a private enterprise, for example, the legal ground for activities such as conducting background checks is dependent on consent given by the data subject. Consent is defined by Article 4 (11) of GDPR as ‘any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’. Article 7 of the same act sets out additional obligations for the controller of personal information (natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data), according to the definition in Article 4 (7) of the Regulation.

What is more, Bulgaria’s PDPA explicitly provides that the period an employer keeps relevant documentation provided by job applicants cannot be longer than six months unless they consent to a longer retention period. The act also forbids the production of copies of identity documents, like driving licenses, unless it is imposed by the law, for example in activities related to anti-money laundering. The general idea of these rules is to stop such practices by employers when there is no actual obligation for the employee to provide this kind of personal information.²²

Furthermore, regarding specific rules followed by the private sector in Bulgaria, the country's local requirements on cookie consent are implemented in the Electronic Commerce Act in compliance with the so-called “Cookie-Directive”²³. According to Article 4a in the act, the provider of information services may store information or access the information in the terminal device of the service recipient, provided that the user is given clear and exhaustive information in accordance with Article 13 of the GDPR, and the user is given the option to refuse the storage or access to the information. The

²¹‘GDPR Guide to National Implementation:Bulgaria’, (*White and Case LLP International Law Firm Practice*, 1 November 2019), 25 February 2011

<www.whitecase.com/publications/article/gdpr-guide-national-implementation-bulgaria>

²²<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/>> accessed 12 March 2021.

²³ Directive 2002/58/EC.

aforementioned article introduces an opt-in regime for the use of cookies, which means that for the use of cookies to be lawful, the user's prior consent is required.²⁴

In conclusion, both the public and the private sector are highly regulated by and are in accordance with EU legislation, although certain specific rules and acts may be established on a local level as given in the example above.

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

The national legislature of the Republic of Bulgaria affords safeguards to the protection of personal data, although there is no explicit right thereto. This notion is to be derived from Article 32 of the Constitution of the Republic of Bulgaria which stipulates the right to private life.²⁵ The right to private life encompasses the right to protection of personal data, as is recognized by the European Court of Human Rights (ECHR).²⁶ Moreover, the previously mentioned PDPA has been adopted to provide the requisite care towards private data.

The PDPA sets the required standard of protection of private data and affords certain rights to data subjects, among which is the right to rectification stipulated in Art. 56 (1) of the PDPA. Data subjects shall have the right to require that the administrator rectifies inaccurate data concerning the former. This right is subject to restrictions as evident from Article 56 (6) of the PDPA. For the purposes of prosecution in criminal proceedings and protecting public order and security, national security and/or human rights and freedoms, the administrator of data may decline the rectification of data with a formal notice in writing. Data subjects, however, may object to the processing of their data,²⁷ including when there is a breach. As the right to protection of personal data is a fundamental one, it presupposes the existence of adequate means and procedures to remedy breaches. This report aims to explain the process of judicial review of cases concerning data protection violations.

1. Review of cases concerning data protection breaches.

The review of cases dealing with violations of data protection has two stages:

- Pre-judicial stage; and
- Judicial stage.

Both phases will be examined thoroughly in their procedurally logical order.

1.1. Pre-judicial stage.

Data subjects have the right to lodge a formal application before the Commission for Personal Data Protection, an administrative body overseeing the protection of data subjects

²⁴ The Legal 500 & The In-House Lawyer "Bulgaria: Data Protection & Cyber Security" www.dpc.bg/p/doc/dpc-bulgarian-chapter-data-protection-862.pdf accessed 12 March 2021.

²⁵ The Constitution of the Republic of Bulgaria, Article 32 (1).

²⁶ *Leander v. Sweden* (26 March 1987), § 48.

²⁷ Regulation (EC) 2016/679, Article 21 (1).

by data processing,²⁸ within 6 months but no more than 2 years after gaining knowledge about a violation of their rights under the PDPA and GDPR.²⁹ The data subjects must be notified by the administrator when there is a possibility that the violation of the security of personal data may lead to substantial risk for the rights and freedoms of the data subjects.³⁰ A notification is not sent when the administrator has taken appropriate technical and organizational measures towards the data in question so as to make it not understandable for every non-authorised person through, e.g. encryption.³¹ The data subjects will also not be notified when the administrator has taken measures which guarantee that the substantial risk for their rights and freedoms will not materialise.³² The last instance in which the data subjects will not be notified is when the notification would lead to disproportionate effort on behalf of the administration – in this case a public message shall be issued or another appropriate measure shall be adopted in order for the data subjects to be effectively informed.³³ The pre-judicial stage of the review of cases concerning data protection breaches is initiated by the introduction of an application.

Firstly, the application is delegated for a review of admissibility.³⁴ The Commission then issues a decision on the admissibility of the application behind closed doors. If and when needed, the Commission may engage third parties for the elucidation of facts and circumstances in connection to the application.³⁵

Secondly, the Commission examines the application on the merits in a public session upon duly notifying the applicant and all stakeholders. The Commission may issue a decision not to review the application if it is manifestly ill-founded or excessive. The rules regarding the gathering of evidence, the appointment of experts, representation, summoning and other procedural actions are to be conducted in compliance with the Administrative Procedure Code.³⁶ The applicant shall be duly notified of the progress of the procedure within three months from lodging the application.³⁷

Lastly, the Commission issues a final decision on the merits of the application.³⁸ A written copy of the final decision on the merits is served to the applicant and the stakeholders.³⁹ The final decision on the merits is subject to judicial review under the Administrative Procedure Code within 14 days after the applicant has received a written copy of it.

1. Judicial stage.

²⁸ Personal Data Protection Act, Article 6(1).

²⁹ *ibid* art. 38(1).

³⁰ *ibid* art. 68(1).

³¹ *ibid* art. 68(3)(1).

³² *ibid* art. 68 (3)(2).

³³ *ibid* art. 68 (3)(3).

³⁴ Rules of procedure of the Commission for Personal Data Protection and its administration, Article 37(1).

³⁵ *ibid* art. 38(2).

³⁶ *ibid* art. 41.

³⁷ Personal Data Protection Act, Article 38 (2); Rules of procedure of the Commission for Personal Data Protection and its administration, Article 43.

³⁸ Rules of procedure of the Commission for Personal Data Protection and its administration, Article 38(2).

³⁹ *ibid* art. 38(3).

A judicial review may only be initiated with the introduction of an application by a stakeholder upon compliance with the aforementioned requirements set out in Article 38 (7) of the PDPA.⁴⁰ The Administrative Procedure Code stipulates the applicable rules with regard to the judicial review of cases concerning the data protection violations. The process consists of two-instances, which will be examined forthwith.

2.1. First instance.

After the formal application has been submitted, the first-instance court constitutes the parties, namely the data subject, the Commission on Personal Data Protection and all stakeholders.⁴¹ The proceedings are initiated not more than 2 months after the submission of the application.⁴² Firstly, the application is reviewed on its admissibility. If the application is inadmissible, the decision thereto may be overturned on appeal upon lodging a private application.⁴³ If the application is admissible, the judge-rapporteur orders for transcripts to be sent to the parties. Within 14 days of receiving the transcript each side may present a rejoinder attached with written evidence.⁴⁴ The court then proceeds to examine the documents submitted before it. The court is not limited to reviewing only the grounds presented by the applicant; it is rather obliged to check the legality of the disputed act in light of the presented evidence.⁴⁵ The court issues a judgement on the merits within a month after the session in which the review of the case has ended. Thus, the proceedings before the first-instance court cease.

2.2. Second instance.

The parties for which the judgement of the case is not favourable may appeal it on cassation, if it is void, inadmissible or incorrect due to a violation of the material law.⁴⁶ The application thereto must be sent within 14 days after the notification of the first-instance judgement has been published. The application is reviewed on admissibility and if it is admissible, the parties receive transcripts of it. They have 14 days to submit a rejoinder with written evidence attached. The case is sent to the cassation court after the rejoinder has been submitted or upon the expiration of the deadline. The case is reviewed by three members of the Supreme Administrative Court. The Supreme Court examines only the defects of the previous judgement specified in the application.⁴⁷ The first session is scheduled within four months after the origination of the case. The Supreme Administrative Court issues a judgement within a month after the session on which it has ended the review of the case. The Court concurs with the first-instance court and the judgement remains in force or annuls it in its disputed part, if it is incorrect. When the judgement is inadmissible, the Court invalidates it in its disputed part, returns it for another

⁴⁰ Administrative Procedure Code, Article 126.

⁴¹ *ibid* art. 153, 154.

⁴² *ibid* art. 157(1).

⁴³ *ibid* art. 160(1).

⁴⁴ *ibid* art. 163(2).

⁴⁵ *ibid* art. 168(1).

⁴⁶ *ibid* art. 209, 210(1).

⁴⁷ *ibid* art. 218(1).

review or forwards it to the competent court.⁴⁸ When the judgement is void, the Court proclaims its voidness in whole, and if the case is not subject to termination, it returns it to the first-instance court for ruling again with a new judgement.

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

The PDPA serves as the current legislative framework at national level, which regulates the protection of individuals in the processing of their personal data and in accessing such data. It exercises supervision over the compliance with the GDPR, in particular – compliance with the requirements on the remedies, liability, and penalties, enshrined in Chapter VIII of the latter. In case of violation of data subjects' rights under the PDPA and the GDPR, every natural person in Bulgaria has the right to protection. There are two types of legal proceedings, which an individual can initiate in cases of data protection breaches – administrative proceedings and judicial proceedings. When initiating administrative proceedings, the natural person can refer to the Commission for Personal Data Protection, functioning as an independent state body, which monitors compliance with the PDPA and the GDPR. As an alternative, the data subject has the right to appeal actions and acts of the data controller judicially before the relevant Administrative Court or the Supreme Administrative Court under the general rules of the Administrative Procedure Code.

Being initially established in 2002, the Commission serves as the supervisory authority at a national level, responsible for the protection of personal data. It shall protect all individuals in all matters regarding the processing of their personal data and the access to this data, as well as exercise supervision on the compliance with the GDPR and the PDPA. The Commission exercises the powers laid down in Article 58 of the GDPR. It functions as a permanent budget-supported legal entity, based in the capital city of Sofia, and has no other territorial directories within the territory of the state. It shall assist the government in the implementation of the state policy in the field of personal data protection.⁴⁹

The Commission is responsible for considering complaints from individuals against personal data controllers for alleged violations of rights under the PDPA and under the GDPR when administrative proceedings are brought. The first paragraph of Article 38 of the PDPA stipulates the period within which data subjects are entitled to refer the matter to the Commission. They have the right to turn to the Commission exclusively within the first six months of becoming aware of the violation. The limitation period has a preclusive effect – any complaint lodged after the expiry of the six-month period will not be upheld and will be dismissed. At the same time, the Commission should be notified no later than two years after the alleged infringement was committed. Both requirements are to be met cumulatively, for the provision of Art. 38, para. 1 of the PDPA to have legal effect. Up until the previously discussed last amendment of the PDPA in 2019, in cases of violation of data subjects' privacy rights, every natural person had the right to refer the matter to the

⁴⁸ *ibid* art. 221(3).

⁴⁹ Personal Data Protection Act, Article 6 (2).

Commission within one year of becoming aware of the violation, but not later than five years after its commission.

Accordingly, in order to speed up the procedure, the legislator has decided to shorten the time period for lodging the data subjects' applications. As per the last amendment of the PDPA, the Commission has the obligation to inform the applicant of the progress of the examination of the application or of the outcome thereof within three months of the referral.⁵⁰ The proceedings before the Commission could be initiated not only by written, but by an oral request as well.⁵¹ Any natural or legal person may submit an application, or the Commission can initiate proceedings of its own accord. When the request is manifestly ill-founded or excessive, it may be left without consideration and be dismissed by a decision of the Commission.⁵² The decision on whether the complaint is manifestly ill-founded or excessive is issued in a closed session according to the Rules of Procedure of the Commission for Personal Data Protection and its administration.

Other prerequisites for dismissing a written complaint would be anonymity, the lack of signature by the complainant or by a legal or authorised representative. Furthermore, for the Commission to take an action, the request shall include some obligatory requisites, which are exhaustively listed in the Rules of Procedure of the Commission for Personal Data Protection and its administration. Every submitted request to the Commission shall, firstly, contain some personal information of the requesting party, namely their names, their mailing address and permanent address, their contact telephone number, and their email address, if available. Moreover, the application should include the nature of the request, the date on which the applicant became aware of the alleged infringement, an identification of the targeted person by the request, other information, or documents, when this is provided for under the law, as well as date and signature. In cases, in which a written request contains any irregularities, the requesting party is notified to remedy the irregularities within three days of lodging the complaint.⁵³ If the irregularities are not remedied within three days, the proceedings are terminated.

Section II of Chapter Four of the Rules of Procedure of the Commission for Personal Data Protection and its Administration stipulates the procedure of handling applications and alerts under Article 38 of the PDPA, including those under the cooperation mechanism with other supervisory authorities. Under the recently promulgated Rules on the Activity of the Commission for Personal Data Protection and its Administration, there are two types of requests, that the requesting party can refer to the Commission – an application, as well as an alert. As per para. 1 of Article 35 of the Rules, the application seeks protection of rights of the requesting party for any alleged infringement under GDPR and under the PDPA. On the other hand, an alert is defined as a request, whereby any infringements of GDPR and of the PDPA are reported, without any rights of the

⁵⁰ *ibid* art. 38 (2).

⁵¹ Rules of Procedure of the Commission on Personal Data Protection and its administration, Article 27.

⁵² Personal Data Protection Act, Art. 38 (4).

⁵³ Rules of Procedure of the Commission on Personal Data Protection and its administration, Art. 28(2).

requesting party to have been allegedly violated. As mentioned above, the Commission issues a decision whether the application is admissible in a session held behind closed doors. In cases, in which further clarifying of the facts and circumstances under an application is needed, the Commission may assign an inspection, gather evidence, or request opinions from third parties under the terms established by the Administrative Procedure Code and in conformity with its powers afforded to it under Article 58 (1) of GDPR. There are certain complaints, which require more specific examination and combined expertise. If an application needs to be examined in cooperation with another supervisory authority, requisite cooperation arrangements are made. In the process of examination of the application, the Commission reviews it on the merits at a public session. The Commission is obliged to notify all parties and the relevant stakeholders.

Finally, the Commission adopts a decision on the merits of the application. It may thereby apply the measures referred to in points (a) to (h) and (j) of para. 2 of Article 58 of the GDPR or in Items 3, 4 and 5 of para. 1 of Article 80 of the PDPA. In addition to, or instead of, the aforementioned measures, the Commission may also impose an administrative fine in accordance with Article 83 of GDPR, as well as under Chapter Nine of the PDPA. After the adoption of the decision, a transcript of the decision is sent to the parties and the stakeholders.

Judicial control over the individual administrative acts of the Commission is exercised by the competent administrative court, as envisaged in Art. 132 of the Administrative Procedure Code. Furthermore, as per Art. 39, para. 1 of the PDPA upon any infringement of the rights pursuant to either GDPR or the PDPA itself, the data subject may appeal against any actions or acts of the data controller and processor before the court pursuant to the Administrative Procedure Code. The administrative proceedings are two-instance, with the Supreme Administrative Court being the cassation instance. The Supreme Administrative Court exercises supreme judicial supervision over the accurate and uniform application of laws in administrative justice. A notice of appeal may be filed within 14 days of receiving the decision of the first instance court. The Supreme Administrative Court may issue a judgement confirming or revoking that decision. The court judgement is final and binding. It affects both the data subject and the personal data controller. However, the data subject may not bring to the attention of the court an alleged violation if proceedings on the same infringement are pending before the Commission or a decision of the Commission regarding the same infringement has been appealed and there is no enforceable judgment of the court to the moment present.⁵⁴ At the request of the data subject, the Commission shall certify the lack of proceedings pending before it on said dispute.

In respect of the provision for remedies to the data protection breaches, the current legislative framework stipulates the possibility for the data subject to claim compensation for the damage suffered as a result of an unlawful processing of personal data.⁵⁵ Article 85

⁵⁴ Personal Data Protection Act, Article 39 (4).

⁵⁵ *ibid* art. 39 (2).

of the PDPA stipulates the different grounds for violations on behalf of the data controller or processor of personal data, where the data controller or the processor of personal data shall be imposed a fine or pecuniary sanction as per Art. 83 of the GDPR. Moreover, according to Art. 86, para. 1, a data controller or data processor shall be liable to a fine or a pecuniary sanction of up to BGN 5,000 for other violations under this Act. In cases of a repeated violation under para. 1, a fine or a pecuniary sanction in double of the initially imposed amount shall be imposed, as set down in the second paragraph.

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

Judicial review is a process by which a person being affected by a particular action or failure to act of a public authority may take legal actions, which could provide a remedy if the authority has not been following the law correctly. It is often a time-consuming procedure but, in many cases, it is the last resort for people to defend their legal rights.⁵⁶

Discrimination is the act of unjust or prejudicial treatment of individuals or a group of people on the grounds of their race, age, sex, sexual orientation, or a disability. Discrimination cases in Bulgaria are far from uncommon. According to the European network of legal experts in gender equality and non-discrimination's report on Bulgaria for the year of 2020⁵⁷, our country is found liable for cases associated with discrimination and hatred, including hate speech and hate crimes.

The Constitution of the Republic of Bulgaria includes a general clause of universal application, Article 6, dealing with non-discrimination, covering race, national origin, ethnicity, sex, origin, religion, education, beliefs, political affiliation, personal and social status, and property status.⁵⁸

Bulgaria's main legislation on the matter is the Protection Against Discrimination Act⁵⁹, which entered into force in January 2004. It has been enacted to transpose and comply with EU directives among which Directive 2000/43/EC and Directive 2000/78/EC against Discrimination on Grounds of Race and Ethnic Origin and against Discrimination at Work on Grounds of Religion or Belief, Disability, Age or Sexual Orientation. The act prohibits direct and indirect discrimination, including discrimination by association and by presumption. It defines the former as 'treating a person on protected grounds less favourably than another person is treated, has been treated, or would be treated in comparable circumstances'. Furthermore, according to the latter indirect discrimination is described as 'placing a person or persons who have a protected characteristic, or, who without having such a characteristic, together with the former suffer less favourable treatment, or are placed at a particular disadvantage deriving from an apparently neutral provision, criterion, or practice, unless the provision, criterion, or practice are objectively justified with a view to a legitimate aim and the means to achieving that aim are

⁵⁶ <www.leighday.co.uk/our-services/human-rights/judicial-review> accessed 10 February 2021;

<www.equalityhumanrights.com/en/advice-and-guidance/judicial-review> accessed 10 February 2021.

⁵⁷ European Commission, Country report Non-discrimination 2020 paras 1.0-2.3.

⁵⁸ Constitution of the Republic of Bulgaria, Article 6.

⁵⁹ Protection against Discrimination Act.

appropriate and necessary'.⁶⁰ Another discrimination law is the People with Disabilities Act, in force as of the 1st of January 2019. It was adopted to secure rights under the Convention on the Rights of Persons with Disabilities.

The process of judicial review of anti-discrimination cases according to the Protection Against Discrimination Act (PADA) presents two alternatives for the victims to take legal action - judicial proceedings before the general courts and specialised quasi-judicial proceedings before the Commission for Protection Against Discrimination.

The Commission was established in 2005 by the PADA as an independent collegiate semi-judicial authority with adjudicating powers. It consists of nine members, four of which are appointed by the President of the Republic of Bulgaria. The National Assembly appoints five members, including the Chair and Deputy Chair of the Commission, while respecting the principles of balanced participation of women and men and of participation of people belonging to ethnic minorities. Their mandate is five years. The Commission investigates complaints by victims by carrying out independent research, imposes financial sanctions and issues instructions and decisions that are legally binding. Its decisions are subject to appeal to two instances of courts, including the Supreme Administrative Court.⁶¹

According to Article 50 of the Protection Against Discrimination Act, the proceedings before the Commission shall be instituted on either a complaint of the people affected, an initiative from the Commission or a signal from an individual, legal entity or public authorities.⁶² The complaint or the signal shall be submitted in writing. When foreign language is used it shall be accompanied by a translation in Bulgarian. The mandatory content of the complaint to the Commission for Protection of Discrimination is in accordance with the second paragraph of Article 51 of the aforementioned act.⁶³

Furthermore, in accordance with Article 71, para. 1 of the Protection Against Discrimination Act, any person whose rights of equality of treatment have been violated shall file a claim before the general courts if the Commission has not been approached.⁶⁴ The courts can declare the case to be indeed of discrimination and award compensation, as well as order the respondent to take remedial action or to abstain from or to terminate a particular action or inaction.

The judicial review of anti-discrimination cases according to the European Commission's Bulgaria country report on non-discrimination for 2020, found that the vulnerable groups of people in Bulgaria include the Roma, refugees, people with disabilities, especially of intellectual nature, people of non-traditional faiths, LGBT people, Muslims, Jews, Turks and Macedonians⁶⁵.

⁶⁰ *ibid* art. 4 (3).

⁶¹ www.equineteurope.org/author/bulgaria_cpdl accessed 10 February, 2021.

⁶² *ibid* art. 50.

⁶³ *ibid* art. 51.

⁶⁴ *ibid* art. 71 (1).

⁶⁵ European Commission, Country report Non-discrimination 2020.

According to the Report, a common trend in Roma litigation are the forced evictions of Roma families for unlawful housing in terms of planning and building requirements and hate speech and crimes. The statistics show that although the Commission for Protection Against Discrimination generally takes an effective stance against hate crimes, courts' case-law varies. In addition, the Supreme Administrative Court and the Supreme Court of Cassation initiated a line of precedents to restrain the use of harassment bans for the purpose of anti-Roma hate speech protection and in some cases associated with negative stereotyping, they have ruled that for a claim of harassment to stand, the person must have been personally targeted rather than in an abstract way as a part of the community.

However, as shown in a case brought before the Supreme Administrative Court (case No. 11803/2017, 15 May 2019), *Media Group 24 OOD v. V. Yordanova and Protection Against*

Discrimination Commission, the Supreme Court confirmed the lower court's decision which in turn had confirmed a decision by the Commission. The case was initiated by the alleged victim of anti-Roma hate comments posted on their media. The company appealed the Commission's decision which gave them instructions to introduce a non-stop comment moderation to their site before the Plovdiv Administrative Court. This resulted in confirmation of the company's liability because it had made anonymous posting possible on its site. The Supreme Administrative Court agreed that the comments instilled ethnic hatred and did not discuss the fact that the comments targeted the Roma community as a whole and not a specific individual as pointed above.

In conclusion, as a multi-ethnic and religiously diverse country, Bulgaria's legal framework provides different means and options for the potential victims of discrimination, whether that would be proceedings before the general courts or before the Commission for Protection against Discrimination.

However, a lot more action is required for the country to ensure uniform rights for all Bulgarian citizens and that is the reason for the enhanced supervision by the Committee of Ministers of the Council of Europe.

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 Republic of Bulgaria has enacted several legislative provisions regulating digital technologies among which the Personal Data Protection Act, the Electronic Commerce Act, the Electronic Communications Act, the Electronic Governance Act, the Electronic Communication Networks and Physical Infrastructure Act and the Electronic Identification Act. Moreover, the European Union law finds application in the Republic of Bulgaria, as the country is a member state of the European Union. Therefore, the legislature on European level shall also be considered when examining the framework regulating advanced digital technologies.

Although there are many legislative provisions addressing and regulating digital technologies in the Republic of Bulgaria, there are scarce resources on matters such as the Internet of Things (IoT), big data, and Artificial Intelligence (AI). They fall within and are governed by the general regime for the use of technologies and data. A notable exception is encryption that enjoys some degree of regulation both on national and European level. Encryption denotes the process of converting data to an unrecognizable form. Its legal definition could be derived from § 1 (29) of the Additional Provisions of the Electronic Communications Act where it is stipulated that encryption stands for converting data from an understandable to a ciphered form.⁶⁶ Encryption is widely used to cover sensitive information and to keep digital correspondence private.

The GDPR recognizes encryption as an appropriate measure by processing personal data in order for security to be guaranteed to a sufficient degree.⁶⁷ This legislative decision is aimed towards securing the right to protection of personal data. This is also reflected in the PDPA in which the controller of personal data shall not inform the data subject about a violation when the former has applied the appropriate technical and organisational measures to the data in question, including *inter alia* encryption.⁶⁸ The Electronic Communications Act also reproduces the provision of Article 32 (1) of the GDPR.

Although encryption proves to be a helpful tool in guaranteeing the right to protection of personal data, in some cases it poses significant challenges to the authorities in the context of uncovering potential crimes in criminal proceedings. Encrypted data containers may be obtained by the relevant authorities by virtue of Article 163 of the Criminal Procedure Code.⁶⁹ According to Article 159 (1) of the Criminal Procedure Code all institutions, legal entities, officials and citizens are obliged to preserve and hand over objects, papers, computer information data and other data that may be relevant to the case.⁷⁰ This can lead to prolonged judicial procedures, particularly with respect to encrypted sensitive information that is difficult to obtain. Thus, the regulatory framework under which encryption is used in the judicial system requires revision, so that it reflects the development of digital technologies and does not interfere with those enterprises or persons in possession of the information, and the specialised authorities that process this information for investigation purposes.

In conclusion, the legislative framework in the Republic of Bulgaria is yet to be improved to account for the dynamic advancement of digital Technologies, namely big data, artificial intelligence (AI), Internet of Things (IoT) and encryption. The application of the European legislation in Bulgaria by itself predisposes national legislation to transform and adapt to the absorption of these technologies. With respect to the protection of human rights, further legislative and control measures are needed to preserve the appropriate use of these digital technologies.

⁶⁶ Electronic Communications Act, § 1 (29) of the Additional Provisions.

⁶⁷ Regulation (EU) 679/2016, Article 32 (1) (a).

⁶⁸ Personal Data Protection Act, Article 68 (3) (1).

⁶⁹ Penal Procedure Code, Article 163 (6).

⁷⁰ *ibid* art 159 (1).

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

The use of encryption technologies is strongly related to the inviolability of life and right to personal information and its protection. Encryption is a tool developed to strengthen the cybersecurity and the protection of personal data. The GDPR considers encryption as a measure that allows ensuring an adequate level of security in the processing of personal data.

In the meantime, however, this impregnability may prevent the competent authorities from detecting crimes, as they affect their ability to obtain evidence that could seriously assist the purposes of prosecution and in particular – the prosecution of perpetrators.

With reference to the Bulgarian legislation, the nature of encryption and encrypted data are regulated in the Criminal Procedure Code.

The question emerges: Must the person concerned be obliged to provide a password for the decryption of the data? Of course, such a problem does not exist when the person is a victim of the crime and as such will probably provide the key voluntarily.

The situation is different when it comes to the accused, as well as when the person concerned is a witness, because according to Article 115, paragraph 4 Criminal Procedure Code, the accused has the right to refuse to give explanations⁷¹ and according to Article 121, paragraph 1, the witness shall not be obligated to testify on questions, the answers to which would accuse him or her, his or her children, parents, grandparents, brothers, sisters, husband or wife or a person with whom is in actual cohabitation of committing a crime.⁷² This practically means that the accused is released from obligation to give any information in connection with the ongoing investigation, and the witnesses may only refuse to testify in certain cases.

To illustrate this, let's examine the case of Saunders vs. the United Kingdom (application no. 19187/91) which was brought before the European Court of Human rights on 17. December 1996. The case is also known as the "Guinness affairs" and it constitutes the theft, false accounting, and overall manipulation of the London stock market by Mr. Saunders to inflate the prices of Guinness' shares. His prosecution followed an investigation by the DTI and the investigators constituted an infringement of the accused's right not to incriminate himself. This was accordingly a breach of article 6 of the European Convention on Human Rights, which guarantees the right to a fair trial.

In this case, the prosecution had used Mr. Saunders' statements in an incriminating manner, to establish his involvement in the unlawful operation. That being said, part of the transcript of his answers to the inspectors had been read out to the jury.

The Court declined to make an award for Mr. Saunders' pecuniary loss pursuant to article 50 of the Convention, noting that it could not speculate on the question of whether the

⁷¹ Criminal Procedure Code, Article 115 (4).

⁷² *ibid* art. 121 (1).

outcome of the trial would have been any different had used not been made of the DTI material by the prosecution, and its finding of a breach of article 6 was not to be taken to suggest this. But the Court awarded him 75,000 pounds to cover his expenses in the Strasbourg proceedings.

In addition, the provision of Article 159 of the Criminal Procedure Code provides that at the request of the court or the bodies of the pre-trial proceedings all institutions, legal entities, officials, and citizens are obligated to preserve and transmit the digital information that may be relevant to the case.⁷³

When retrieving digital data during an investigation, the preliminary search and seizure order should include the type of device as well as its relevance to the procedure. If possible, even the specific data that is needed. The reason for this is to be found in Article 163, paragraph 7 of the Criminal Procedure Code, which implies that it is far more appropriate to seize certain data than the whole hardware⁷⁴ according to Article 163, paragraph 6 of the Criminal Procedure Code⁷⁵, as the latter may contain huge arrays of information that are not relevant to the purposes of the criminal proceedings.

In cases when there is access to huge content that is not related at all with the proceedings, or the authorities violate the privacy of unidentified people not related to the proceedings they would be acting beyond their powers. Nevertheless, decryption is approached by the competent authorities as a last resort when all other options would fail to produce a positive result.

They use any available vulnerabilities within the computer information system, but the detection of existing weaknesses by the investigating authorities would mean that the identified deficiencies would be reported, which would increase the overall level of cybersecurity but prevent further decryption attempts.

It is strongly believed that the use of backdoors such as restricting or weakening of the encryption mechanisms is not a solution because it could have irreparable consequences for cybersecurity.⁷⁶ Therefore, it should be actively sought to improve cooperation with service providers.

There is currently no international or European instrument governing the use of decryption technologies in the context of criminal justice. The issue of encryption was first addressed by the justice ministers of the Member States of the European Union during the Slovak Presidency of the Council of the European Union, and in December 2016 the ministers instructed the European Commission to examine the problem of the role of encryption in criminal proceedings and to work on possible solutions at European level. In 2017, the Commission started expert discussions on the matter. In the future, there will certainly be a legislative framework regulating encryption in the context of criminal proceedings.

⁷³ *ibid* art. 159.

⁷⁴ *ibid* art. 163 (7).

⁷⁵ *ibid* art. 163 (6).

⁷⁶ Europol and ENISA Joint Statement, (20 May 2016).

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

The development of digital technologies in Bulgaria has been on the rise, allowing for their gradual penetration into the private and public sectors. Considerable efforts have been made to protect human rights in the digital realm in the past decade, albeit progress on their appropriate implementation has been a challenge.

The EU emphasises on the importance of digital advancements and is committed to ensure digital integration through various programs. The Digital Economy and Society Index (DESI) is one of the tools used to assess member states' digital performance and development, and their contribution to the digital economy. Bulgaria is placed in 28th position out of the 28th member states in last years' edition of the report, due to its lack of progress on indicators of human capital, use of internet services and integration of digital technology, among others.⁷⁷ One of the most significant deficiencies highlighted by the report is the low level of digital skills among citizens – basic digital skills account for 29% of the total adult population compared to a substantial 58% on average.⁷⁸ This suggests that, in addition to insufficient digital skills, Bulgaria's adult citizens may not be adequately prepared to protect their privacy online. With respect to the integration of digital technology in the private sector, only 7% of small-to-medium enterprises take advantage of online commerce, with limited sales across borders.⁷⁹ The evidence outlined by the report alludes to the limited penetration of digital technologies in the private sector overall, with exceptions of the IT sector and foreign investments.

The Bulgarian government has initiated several programs concerning digital transformation of the private and public sector, including 'Digital Bulgaria 2025'⁸⁰, aimed at improving e-government services and digitalisation of the industrial sector and 'Digital Transformation of Bulgaria for 2020-2030'⁸¹ covering the potential opportunities for digital transformation growth concerning artificial intelligence (AI), the Internet of Things (IoT) and smart living. Two possible indicators as to whether Bulgaria has reached an adequate balance between allowing for digital advancements and protecting human rights are the decisions of the European Court of Human Rights and the European Commission's Rule of Law Reports.

⁷⁷ Digital Economy and Society Index (DESI). 2020. Bulgaria.

<<https://ec.europa.eu/digital-single-market/en/scoreboard/bulgaria>> accessed 12 March 2021.

⁷⁸ *ibid.*

⁷⁹ *ibid.*

⁸⁰ Ministry of Transport, Information Technology and Communications. 2020. Draft National Program 'Digital Bulgaria 2025'.

<<https://www.mtmc.government.bg/en/category/85/draft-national-program-digital-bulgaria-2025>> accessed 12 March 2021.

⁸¹ Ministry of Transport, Information Technology and Communications. 2020. Digital transformation of Bulgaria for the period 2020-2030.

<https://www.mtmc.government.bg/sites/default/files/digital_transformation_of_bulgaria_for_the_period_2020-2030_f.pdf> accessed 12 March 2021.

The practice of the European Court of Human Rights related to the use of technology⁸² stipulates that Article 10 of the Convention not only applies to the right and substance of information, but its various forms in which it is transmitted and received, particularly using the Internet as an important information tool. The recent case of *Pendov v. Bulgaria* (app. no. 44229/11)⁸³ depicts a violation of access to information related to a server owned by the applicant, which was seized and retained by prosecution authorities. In response to this, the court declared the complaints under article 10 in addition to Article 1 of Protocol No. 1 admissible. The retention of the server led to limited functionality of a website run by the applicant which was hosted on that server and to constraints of the applicants' professional activity related to the website. This case illustrates potential inadequacies of the judicial authorities of Bulgaria with respect to seizures of devices and the difficulties regarding the analysis and the return of a server containing valuable information.

The 2020 European Commission's Rule of Law Report⁸⁴ alludes to challenges regarding the public trust of institutions, particularly of the justice system. Despite continuous efforts for reform, the Prosecutor General exerts considerable influence over the governance of judges and review of cases and decisions by all Bulgarian courts. In addition to the limited accountability and lack of possibility of an effective criminal investigation, these issues have been a source of concern for the Council of Europe and the European Court of Human Rights. Although amendments of the Judicial System Act have been introduced to prevent the long period necessary to acquire life tenure and automatic promotion to higher ranking positions, the report highlights the possibilities for the State to exert political influence and potentially violate the European Convention of Human Rights using administrative tools of the judicial system, particularly amidst the pandemic.

With respect to media pluralism, the report states lack of transparency of media ownership and political interference in the media, as well as failure of the Bulgarian Parliament to incorporate the work of journalists into the newly passed amendments to the PDPA. This exception was observed as a potential threat to the visibility of political investigations by Bulgarian journalists and ties with the frequently reported threats, harassment cases and assaults on journalists. The report comments on the possibility of the government threatening media independence and exerting indirect social media censorship using political, administrative, and judicial pressure. While the judicial system has seen improvements in recent years, the state of the rule of law in Bulgaria outlined by the Commission raises concerns over human rights violations in many aspects, which can easily translate to the increasing use of technology. Although the government and judicial system's reforms do not fully capture the magnitude of the digital advancement, the limited

⁸² European Court of Human Rights (ECHR). 2015. Internet: case-law of the European Court of Human Rights. <https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf> accessed 15 March 2021.

⁸³ *Pendov v. Bulgaria* [2020].

⁸⁴ European Commission. 2020. 2020 Rule of Law Report: Country Chapter on the rule of law situation in Bulgaria. <<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1602582109481&uri=CELEX%3A52020SC0301>> accessed 17 March 2021.

availability of evidence suggests that while some efforts to reform the protection of human rights have been made, there is a potential caveat to their application regarding advanced technology.

Perhaps because of the pandemic, the government may gradually become better able to regulate the absorption of digital advancements and human rights legislation. This has been evident from the recent implementation of updated rules on the functioning of Bulgarian courts initiated by the Bulgarian Supreme Judicial Council that regulates how courts operate under the conditions of the pandemic, including access to courts' administration services and court hearings⁸⁵. The establishment of the online portal for 'e-justice' allowed for law practitioners to access case law and other administrative services remotely, by registering using an electronic signature⁸⁶. Several advancements for remote access to administrative services for citizens and enterprises have also been initiated. However, the question remains as to whether these rules are followed and implemented effectively, so that human rights are protected online.

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 legislation regarding protecting human rights online, or digital human rights per se, is set to develop rapidly in the next five years, particularly in response to the uprising development in the fields of digital technology, research, and innovation. We are observing not only a tremendous change in how we interact, digitalise our economy and gather information, but also the potential of technology and social media to undermine the exercise of human rights globally.

One proposition is that, with the help of multi-stakeholder and interdisciplinary approaches, appropriate legislation would be able to define the normative basis of digital human rights with respect to the Internet, artificial intelligence (AI) systems and other emerging technology. A recent depiction of such efforts is the development of Bulgarian university programmes in the realm of cybersecurity and the establishment of numerous NGOs working to provide expertise and advise enterprises to cyber crimes.

Secondly, Internet governance and cybersecurity could potentially benefit from establishing a multilateral model in which international understanding of human rights protection is solidified. For instance, the National Cyber Security Strategy "Cyber Resilient" Bulgaria 2020, initiated in response to the European Union Agency for Cybersecurity, has paved the way to the implementation of reports and rules with respect to cyber crime, incident response capability of public and private enterprises, encouraging research and development and training and education. This has prompted the NGO, IT and education

⁸⁵ Supreme Judicial Council Bulgaria. 2020. "Rules and measures for the work of the courts of justice in conditions of the pandemic." <<http://www.vss.justice.bg/page/view/106065>> accessed 12 March 2021.

⁸⁶ Unified portal for access to judicial services. <<https://portal.justice.bg/>> accessed 10 March 2021.

sectors to establish pathways to education on cybersecurity, both at the level of early education and professional training in the private sector.

Appropriate cohesion between the administrative capacities and enterprises would ensure not only more innovative application of digital technology but would also strengthen the productive dialogue between the government, society, and the private sector. In turn, citizens would be better informed about the opportunities and caveats of digital technology implementation. The introduction of the new EU cybersecurity strategy⁸⁷ is expected to accelerate these processes and lead to further developments in national legislation, allowing for an increase in Bulgaria's technological sovereignty in the public and private sectors.

Lastly, the government is set to investigate cyber crimes more adequately, while aiding and safeguarding digital human rights in the context of cybersecurity, using the resources and knowledge that can be developed from further research and innovation in the field.

Conclusion

Advanced digital technologies pose significant threats to human rights which are yet to be addressed by the legislative. There is visible progress with respect to personal data protection and anti-discrimination – fields in which the individuals enjoy a high standard of protection by virtue of the national and European legislation. Moreover, the remedies for violations thereto are effective and provide sufficient redress. However, the Republic of Bulgaria is yet to regulate some of the advanced digital technologies and their implications of human rights. Artificial intelligence, big data and the Internet of Things (IoT) are not explicitly addressed in the current legislation and the general regime finds application towards them. As far as encryption is in question, there are some provisions explicitly regulating this process, however there are still issues with decryption of data for the purposes of criminal justice.

The Republic of Bulgaria has made continuous efforts to regulate advanced digital technologies and to reach an adequate balance between allowing their growth and development and safeguarding human rights and has managed to achieve it to an appropriate degree. Nonetheless, there still remain fields in which the country has to adopt a legislative framework. In the upcoming years, the Republic of Bulgaria will be paving its way for technological development and cybersecurity, and thus the black fields in Bulgaria's legislation will be filled. The Bulgarian government is looking for ways to improve and strengthen its personal data protection and is dedicated to pursuing this by developing various strategies and implementing the new EU Cybersecurity Strategy. The establishment of certain specific rules and actions on a local level in accordance with EU legislation is anticipated, in order to overcome the challenges regarding regulating the protection of privacy. Alas, their lawful and appropriate application is yet to be regulated and improved.

⁸⁷ EU Cybersecurity Strategy. 2020. Available at: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0> accessed 12 March 2021.

Table of legislation

Provision in Bulgarian	Corresponding translation in English
Конституция на Република България, чл. 39 (1) Всеки има право да изразява мнение и да го разпространява чрез слово - писмено или устно, чрез звук, изображение или по друг начин.	Constitution of the Republic of Bulgaria, Article 39 (1) Everyone has the right to express an opinion and to disseminate it by word of mouth - written or oral, sound, image or otherwise.
Конституция на Република България, чл. 39, (2) Това право не може да се използва за накърняване на правата и доброто име на друго и за призоваване към насилствена промяна на конституционно установения ред, към извършване на престъпления, към разпалване на вражда или към насилие над личността.	Constitution of the Republic of Bulgaria, Article 39 (2) This right may not be used to infringe on the rights and reputation of another and to call for a forcible change of the constitutional order, to commit crimes, to incite hostility or to violence against the person.
Закон за защита на личните данни, чл. 6 Чл. 6. (1) „Комисията за защита на личните данни, наричана по-нататък "комисията", е постоянно действащ независим надзорен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Регламент (ЕС) 2016/679 и на този закон. (2) Комисията съдейства за провеждането на държавната политика в областта на защита на личните данни.“	Personal Data Protection Act, Article 6 Article 6. (1) The Commission for Personal Data Protection, hereinafter referred to as “the Commission”, shall be an independent supervisory authority which protects the individuals with regard to the processing of their personal data and the access to this data, as well as the supervision on the compliance with Regulation (EU) 2016/679 and with this Act. (2) The Commission shall provide assistance with the implementation of the state policy in the personal data protection field.
Наказателно-процесуален кодекс, чл. 162 (6): Когато претърсването и изземването са свързани с компютърни информационни системи и програмни продукти, действията	Penal Procedure Code, Article 162 (6): Where the search and seizure are related to computer information systems and software products, the actions shall be carried out in the presence of an expert – technical assistant.

се извършват в присъствието на специалист - технически помощник.	
Наказателно-процесуален кодекс, чл. 163 (6-8): (6) Иззетите предмети, книжа и компютърни информационни системи, в които се съдържат компютърни информационни данни, се предявяват на поемните лица и другите присъстващи. Когато е необходимо, те се опаковат и запечатват на мястото на изземването им. (7) Изземването на компютърни информационни данни се извършва чрез запис върху хартиен носител и друг носител. Когато носителят е хартиен, всяка страница се подписва от лицата по чл. 132, ал. 1. В останалите случаи носителят се запечатва с бележка, в която се посочват: делото, органът, извършил изземването, мястото, датата и имената на всички присъстващи съгласно чл. 132, ал. 1, които се подписват. (8) Разпечатването на носителя, изготвен по реда на ал. 7, се допуска за нуждите на разследването само с разрешение на прокурора и се извършва в присъствието на поемни лица и специалист - технически помощник.	Penal Procedure Code, Article 163 (6-8): (6) The seized objects, papers and computer information systems which contain computer information data shall be submitted to the witnesses of the procedural actions and the other persons present. Where necessary, they shall be packed and sealed at the place of seizure. (7) The seizure of computer information data shall be carried out by record on a paper carrier and another carrier. Where the carrier is a paper one, each of the pages shall be signed by the persons under Art. 132, Para. 1. In the rest of the cases the carrier shall be sealed by a note, which shall contain: the case, the body which has carried out the seizure, the place, the date and the names of all of the persons present as per Art. 132, Para. 1 and who will sign it. (8) Unsealing the carrier, made out under the order of Para. 7, shall be admitted for the necessities of the investigation only and with the permission of the prosecutor and shall be performed in the presence of witnesses of procedural actions and of an expert-technical assistant.
Наказателно-процесуален кодекс, чл. 159: (1) По искане на съда или на органите на	Penal Procedure Code, Article 159:

досъдебното производство всички учреждения, юридически лица, длъжностни лица и граждани са длъжни да запазят и предадат намиращите се у тях предмети, книжа, компютърни информационни данни и други данни, които могат да имат значение за делото.	(1) On a request of the Court or of the bodies of the pre-trial procedures, all establishments, juridical persons, officials and citizens shall be obliged to preserve and deliver the objects, papers, computer information data, the carriers of such data and data about the subscriber, which are in their possession and may be of importance for the case.
Наказателно-процесуален кодекс, чл. 115: (4) Обвиняемият има право да откаже да дава обяснения.	Penal Procedure Code, Article 115: (4) The defendant shall be entitled to refuse to give reasons.
Наказателно-процесуален кодекс, чл. 121: (1) Свидетелят не е длъжен да дава показания по въпроси, отговорите на които биха уличили в извършване на престъпление него, неговите възходящи, низходящи, братя, сестри или съпруг или лице, с което той се намира във фактическо съжителство.	Penal Procedure Code, Article 121: (1) The witness shall not be obliged to testify on questions, the answers to which would accuse him/her or his/her ascendants, descendants, brothers or sisters or spouse, or the person with whom he/she is in a factual cohabitate in the commission of an offence.
Закон за защита от дискриминацията, чл. 50: Производство пред комисията се образува по: 1. жалба на засегнатите лица; 2. инициатива на комисията; 3. сигнали на физически и юридически лица, на държавни и общински органи.	Protection against Discrimination Act, Article 50: Proceedings before the commission shall be instituted on: 1. complaint of the affected persons; 2. initiative of the commission; 3. signals of natural and legal persons, of state and municipal bodies.
Конституция на Република България, чл. 32 (1): Личният живот на гражданите е неприкосновен. Всеки има право на защита срещу незаконна намеса в личния и семейния му живот и срещу посегателство върху неговата чест, достойнство и добро име.	Constitution of the Republic of Bulgaria, Article 32 (1): The private life of citizens is inviolable. Everyone has the right to protection against unlawful interference with their private and family life, infringement against their honour, dignity and good name.

Закон за защита на личните данни, чл. 56 (1): Субектът на данните има право да поиска администраторът да коригира неточните лични данни, свързани с него. Като се има предвид целта на обработването, субектът на данните има право да поиска непълните лични данни да бъдат допълнени, включително чрез предоставяне на допълнително заявление.	Personal Data Protection Act, Article 56 (1): The data subject has the right to request the controller to correct inaccurate personal data related to him. Given the purpose of the processing, the data subject has the right to request that incomplete personal data be supplemented, including by submitting an additional application.
Закон за защита на личните данни, чл. 56. (6): Коригиране, допълване, изтриване или ограничаване на обработването на лични данни може да се откаже, като се отчитат основните права и законните интереси на засегнатото физическо лице, в случаите по чл. 54, ал. 3. В тези случаи се прилага чл. 54, ал. 4. Администраторът информира писмено субекта на данните за отказа, както и за причините за него в срока по чл. 53, ал. 3.	Personal Data Protection Act, Art. 56 (6): Rectification, supplementation, deletion or restriction of the processing of personal data may be refused, taking into account the fundamental rights and legal interests of the affected natural person, in the cases under Art. 54, para. 3. In these cases art. 54, para. 4. The administrator shall inform in writing the data subject about the refusal, as well as about the reasons for it within the term under art. 53, para. 3.
Закон за защита на личните данни, чл. 68 (1): Когато има вероятност нарушението на сигурността на личните данни по чл. 67, ал. 1 да доведе до висок риск за правата и свободите на субектите на данни, администраторът на лични данни уведомява и субекта на данните за нарушението не по-късно от 7 дни от установяването му.	Personal Data Protection Act, Article 68 (1): When there is a probability the violation of the security of the personal data under art. 67, para. 1 to lead to a high risk for the rights and freedoms of the data subjects, the personal data controller shall also notify the data subject of the violation not later than 7 days from its establishment.
Закон за защита на личните данни, чл. 68. (3) (1): Субектът на данните не се уведомява за нарушение по ал. 1, ако е изпълнено някое от следните условия: 1. администраторът е предприел подходящи технически и организационни	Personal Data Protection Act, Article 68 (3) (1): The data subject shall not be notified of a violation under para. 1, if any of the following conditions is fulfilled: 1. the controller has taken appropriate technical and organizational safeguards and

мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението, по-специално мерки, които правят личните данни неразбираеми за всяко лице, което няма право на достъп до тях, като например криптиране;	those measures have been applied to the personal data affected by the breach, in particular measures which render the personal data incomprehensible to any person who is not entitled to access them, such as encryption;
Закон за защита на личните данни, чл. 68 (3) (2): администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се реализира високият риск за правата и свободите на субектите на данни;	Personal Data Protection Act, Article 68 (3) (2): the controller has subsequently taken measures to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize;
Правилник за дейността на Комисията за защита на личните данни и нейната администрация, чл. 37 (1): Постъпило искане по чл. 35, ал. 1 се разпределя на дирекция „Правни производства и надзор“, която представя становище по редовността, допустимостта или основателността на искането, включително и анализ относно необходимостта за разглеждане на жалбата в условията на сътрудничество с друг надзорен орган, когато е приложимо.	Rules of procedure of the Commission for Personal Data Protection and its administration, Article 37 (1): Received request under Art. 35, para. 1 shall be assigned to the Legal Proceedings and Supervision Directorate, which shall present an opinion on the regularity, admissibility or validity of the request, including an analysis of the need to consider the complaint in the conditions of cooperation with another supervisory body, where applicable.
Правилник за дейността на Комисията за защита на личните данни и нейната администрация, чл. 38 (1): Комисията се произнася с решение по редовността или допустимостта на жалба по чл. 35, ал. 1, както и в случаите по чл. 38, ал. 4 от ЗЗЛД в закрито заседание.	Rules of procedure of the Commission for Personal Data Protection and its administration, Article 38 (1): The commission shall rule with a decision on the regularity or admissibility of a complaint under Art. 35, para. 1, as well as in the cases under Art. 38, para. 4 of LPPD in closed session.
Правилник за дейността на Комисията за защита на личните данни и нейната администрация, чл. 38 (2): За изясняване на фактите и обстоятелствата по постъпила жалба комисията може да възложи извършването	Rules of procedure of the Commission for Personal Data Protection and its administration, Article 38 (2): In order to clarify the facts and circumstances of the received complaint, the commission may assign the performance of an inspection,

на проверка, събирането на доказателства или искане на становища от трети лица при условията на АПК и съобразно правомощията си по чл. 58, параграф 1 от Регламент (ЕС) 2016/679.	the collection of evidence or a request for opinions from third parties under the terms of the APC and in accordance with its powers under Art. 58 (1) of Regulation (EU) 2016/679.
Правилник за дейността на Комисията за защита на личните данни и нейната администрация, чл. 40 (1): Комисията разглежда жалбата по същество в открито заседание, за което уведомява страните и заинтересованите лица.	Rules of procedure of the Commission for Personal Data Protection and its administration, Article 40 (1): The Commission shall examine the merits of the application in open court, which shall inform the parties and the persons concerned.
Закон за защита на личните данни, чл. 38 (4): Когато жалбата е очевидно неоснователна или прекомерна, с решение на комисията жалбата може да се остави без разглеждане.	Personal Data Protection Act, Article 38 (4): Where the complaint is manifestly ill-founded or excessive, the complaint may be dismissed by a decision of the commission.
Правилник за дейността на Комисията за защита на личните данни и нейната администрация, чл. 41: Събирането на доказателствата, назначаването на експерти, представителството, призоваването и други действия в производството по този раздел се извършват по реда на АПК.	Rules of procedure of the Commission for Personal Data Protection and its administration, Article 41: The collection of evidence, the appointment of experts, representation, summons and other actions in the proceedings under this section shall be carried out in accordance with the Administrative Procedure Code.
Закон за защита на личните данни, чл. 38 (3): Комисията се произнася с решение, като може да приложи мерките по чл. 58, параграф 2, букви "а" - "з" и "й" от Регламент (ЕС) 2016/679 или по чл. 80, ал. 1, т. 3, 4 и 5 и в допълнение към тези мерки или вместо тях да наложи административно наказание в съответствие с чл. 83 от Регламент (ЕС) 2016/679, както и по глава девета.	Personal Data Protection Act, Article 38 (3): The commission shall issue a decision and may apply the measures under Art. 58, paragraph 2, letters "a" - "h" and "j" of Regulation (EU) 2016/679 or under Art. 80, para. 1, items 3, 4 and 5 and in addition to these measures or instead to impose an administrative penalty in accordance with Art. 83 of Regulation (EU) 2016/679, as well as under Chapter Nine.
Закон за защита на личните данни, чл. 38 (7): Решението на комисията по ал. 3 и 4 подлежи на обжалване по реда на	Personal Data Protection Act, Article 38 (7) The decision of the commission under par. 3 and 4 shall be subject to appeal by the order

Административнопроцесуалния кодекс в 14-дневен срок от получаването му.	of the Administrative Procedure Code within 14 days from its receipt.
Административно процесуален кодекс, чл. 126: Съдебните производства започват по искане на заинтересовано лице или на прокурора в определените от този кодекс или друг закон случаи.	Administrative Procedure Code, Article 126: Judicial proceedings shall be initiated at the request of an interested person or of the prosecutor in the cases specified by this Code or another law.
Административно процесуален кодекс, чл. 153 (1): Страни по делото са оспорващият, органът, издал административния акт, както и всички заинтересовани лица. (2) Когато след издаване на административния акт органът бъде закрит, без да е посочен негов правопреемник, страна по делото е овластеният с компетентността да издава същите актове орган. (3) Когато компетентността на административния орган по въпроса бъде отнета, съдът го заличава и конституира служебно като страна по делото компетентен орган. (4) Определението по ал. 3 подлежи на обжалване с частна жалба.	Administrative Procedure Code, Articles 153 (1): Parties to the case shall be the disputant, the body, which has issued the administrative act, as well as all interested persons. (2) When after the issuance of the administrative act the body is closed, without indicating its legal successor, a party to the case shall be the body authorized with the competence to issue the same acts. (3) When the competence of the administrative body on the issue is revoked, the court shall delete it and constitute ex officio as a party to the case a competent body. (4) The definition under para. 3 is subject to appeal with a private appeal.
Административно процесуален кодекс, чл. 154 (1): Съдът конституира страните служебно. (2) Когато административният орган не е изпълнил задължението си по чл. 152, ал. 3, съдът определя срок за изпълнението му.	Administrative Procedure Code, Articles 154 (1): The court shall constitute the parties ex officio. (2) When the administrative body has not fulfilled its obligation under art. 152, para. 3, the court shall set a term for its implementation.
Административно процесуален кодекс, чл. 157 (1): Председателят на съда, негов заместник или председателят на отделението образуват административното дело, което се предава на съдия-докладчик.	Administrative Procedure Code, Article 157 (1): The President of the Court, his Deputy or the President of the Division shall open the

Съдията-докладчик, съответно председателят на отделение във Върховния административен съд, насрочва делото в срок не по-дълъг от два месеца от постъпването на жалбата в съда. Този срок не тече за периода на съдебната ваканция, освен когато в този кодекс или специален закон са предвидени по-кратки срокове.	administrative case, which shall be referred to the Judge-Rapporteur. The Judge-Rapporteur, respectively the President of a Division of the Supreme Administrative Court, shall schedule the case for a period not exceeding two months from the receipt of the appeal in court. This period shall not run for the period of judicial vacation, unless shorter periods are provided for in this Code or a special law.
Административно процесуален кодекс, чл. 159: Жалбата или протестът се оставя без разглеждане, а ако е образувано съдебно производство, то се прекратява, когато: 1. актът не подлежи на оспорване; 2. оспорваният е неправосубектен; 3. оспореният административен акт е оттеглен; 4. оспорваният няма правен интерес от оспорването; 5. оспорването е просрочено; 6. по оспорването има влязло в сила съдебно решение; 7. има образувано дело пред същия съд, между същите страни, на същото основание; 8. оспорването бъде оттеглено или бъде извършен отказ от него.	Administrative Procedure Code, Article 159: The appeal or protest shall be left without consideration, and if court proceedings have been instituted, it shall be terminated when: 1. the act is not subject to contestation; 2. the disputant is non-legal entity; 3. the disputed administrative act has been withdrawn; 4. the disputant has no legal interest in the contestation; 5. the contestation is overdue; 6. a court decision has entered into force on the contestation; 7. a case has been instituted before the same court, between the same parties, on the same grounds; 8. the contestation is withdrawn or waived.
Административно процесуален кодекс, чл. 160 (1) (1): Разпореждането, с което жалбата или протестът се оставя без разглеждане, или определението, с което делото се прекратява, подлежи на обжалване с частна жалба. Препис от нея не се представя, ако разпореждането е постановено преди връчването на препис от оспорването.	Administrative Procedure Code, Article 160 (1) (1): The order by which the appeal or the protest is left without consideration, or the ruling by which the case is terminated, shall be subject to appeal with a private appeal. A copy of it shall not be submitted if the order was issued before the service of a copy of the challenge.
Административно процесуален кодекс, чл. 163 (1):	Administrative Procedure Code, Article 163 (1):

Ако жалбата или протестът са допустими, съдията-докладчик разпорежда преписи от тях да бъдат изпратени на страните.	If the appeal or protest is admissible, the Judge-Rapporteur shall order copies of it to be sent to the parties.
Административно процесуален кодекс, чл. 163 (2): В 14-дневен срок от получаването на преписа всяка от страните може да представи писмен отговор и да посочи доказателства. Писмените доказателства, с които страната разполага, се прилагат към отговора.	Administrative Procedure Code, Article 163 (2): Within 14 days of receiving the transcript, either party may submit a written response and provide evidence. The written evidence available to the party is attached to the reply.
Административно процесуален кодекс, чл. 168 (1): Съдът не се ограничава само с обсъждане на основанията, посочени от оспорващия, а е длъжен въз основа на представените от страните доказателства да провери законосъобразността на оспорения административен акт на всички основания по чл. 146.	Administrative Procedure Code, Article 168 (1): The court is not limited only to discussing the grounds indicated by the disputant, but is obliged on the basis of the evidence presented by the parties to verify the legality of the challenged administrative act on all grounds under Art. 146.
Административно процесуален кодекс, чл. 172 (1): Съдът постановява решение в едномесечен срок от заседанието, в което е приключило разглеждането на делото. (2) Съдът може да обяви нищожността на оспорения административен акт, да го отмени изцяло или отчасти, да го измени или да отхвърли оспорването. (3) Когато бъдат отменени мълчалив отказ или мълчаливо съгласие, смятат се за отменени и изричните такива, последвали преди решението за отмяна. (4) В решението се посочват имената на страните, освен когато то има действие по отношение на всички.	Administrative Procedure Code, Article 172 (1): The court shall issue a decision within one month from the sitting in which the examination of the case has ended. (2) The court may declare the nullity of the challenged administrative act, annul it in whole or in part, amend it or reject the contestation. (3) When tacit refusal or tacit consent is revoked, the explicit ones, which followed before the decision for revocation, shall also be considered revoked. (4) The decision shall indicate the names of the parties, except when it has effect in respect of all.
Административно процесуален кодекс, чл. 209:	Administrative Procedure Code, Article 209:

Касационна жалба или касационен протест се подава, когато решението е: 1. нищожно; 2. недопустимо; 3. неправилно поради нарушение на материалния закон, съществено нарушение на съдопроизводствените правила или необоснованост.	A cassation appeal or cassation protest is filed when the decision is: 1. null and void; 2. inadmissible; 3. incorrectly due to violation of substantive law, substantial violation of the rules of court proceedings or unfoundedness.
Административно процесуален кодекс, чл. 210 (1): Право да обжалват решението имат страните по делото, за които то е неблагоприятно.	Administrative Procedure Code, Articles 210 (1): The parties to the case, for whom it is unfavorable, have the right to appeal the decision.
Административно процесуален кодекс, чл. 213а (5): След подаването на отговора или след изтичането на срока по ал. 4 делото се изпраща на касационния съд.	Administrative Procedure Code, Article 213a (5): After the submission of the answer or after the expiration of the term under par. 4 the case shall be sent to the court of cassation.
Административно процесуален кодекс, чл. 217 (1): Делото се разглежда от тричленен състав на Върховния административен съд, когато решението е постановено от административен съд, и от петчленен състав, когато решението е постановено от тричленен състав на Върховния административен съд.	Administrative Procedure Code, Article 217 (1): The case is heard by a three-member panel of the Supreme Administrative Court when the decision is rendered by an administrative court, and by a five-member panel when the decision is rendered by a three-member panel of the Supreme Administrative Court.
Административно процесуален кодекс, чл. 218 (1): Върховният административен съд обсъжда само посочените в жалбата или протеста пороци на решението.	Administrative Procedure Code, Article 218 (1): The Supreme Administrative Court discusses only the defects of the decision indicated in the appeal or protest.
Административно процесуален кодекс, чл. 217 (3): първото заседание се насрочва в срок не по-дълъг от 4 месеца от образуването му. В случай на нередовности на касационната жалба срокът тече от отстраняването им.	Administrative Procedure Code, Article 217 (3): the first meeting is scheduled for a period not longer than 4 months from its formation. In case of irregularities of the cassation appeal, the term runs from their elimination. In an

При открито заседание делото се разглежда с участието на прокурор. Върховният административен съд се произнася с решение в едномесечен срок от заседанието, в което е приключило разглеждането на делото.	open hearing, the case is heard with the participation of a prosecutor. The Supreme Administrative Court shall issue a decision within one month from the hearing in which the hearing of the case has ended.
Административно процесуален кодекс, чл. 221 (2): Върховният административен съд оставя в сила решението или го отменя в оспорваната му част, ако е неправилно. Когато Върховният административен съд остави в сила решението, той го мотивира, като може да препрати и към мотивите на първоинстанционния съд.	Administrative Procedure Code, Article 221 (2): The Supreme Administrative Court upholds the decision or annuls it in the contested part, if it is incorrect. When the Supreme Administrative Court upholds the decision, it shall motivate it and may refer it to the reasons of the court of first instance.
Административно процесуален кодекс, чл. 221 (5): Когато решението е нищожно, Върховният административен съд обявява нищожността му изцяло и ако делото не подлежи на прекратяване, го връща на първоинстанционния съд за постановяване на ново решение.	Administrative Procedure Code, Article 221 (5): When the decision is null and void, the Supreme Administrative Court declares it null and void in full and, if the case is not subject to termination, returns it to the court of first instance for a new decision.
Административно процесуален кодекс, чл. 223: Касационното решение е окончателно.	Administrative Procedure Code, Article 223: The decision of the cassation is final.
Закон за защита от дискриминацията, чл. 51 (1): Жалбата или сигналът до комисията се подават писмено. Когато са написани на чужд език, те се придружават с превод на български език. (2) Жалбата или сигналът трябва да съдържат: 1. името или наименованието на подателя; 2. адреса или седалището и адреса на управление на подателя; 3. изложение на обстоятелствата, на които се основава жалбата или сигналът;	Protection against Discrimination Act, Article 51. (1): The complaint or the signal to the commission shall be submitted in writing. When written in a foreign language, they are accompanied by a translation into Bulgarian. (2) The complaint or the signal must contain: 1. the name or the name of the sender; 2. the address or the seat and the address of management of the sender; 3. statement of the circumstances on which the complaint or the signal is based;

4. изложение на исканията към комисията; 5. дати и подпис на лицето, което подава жалбата, или на негов представител. (3) Анонимни жалби и сигнали не се разглеждат от комисията.	4. statement of the requests to the commission; 5. dates and signature of the person who submits the complaint or of his representative. (3) Anonymous complaints and signals shall not be considered by the commission.
Закон за защита от дискриминацията, чл. 71 (1): Извън случаите по раздел I, всяко лице, чиито права по този или по други закони, уреждащи равенство в третирането, са нарушени, може да предяви иск пред районния съд, с който да поиска: 1. установяване на нарушението; 2. осъждане на ответника да преустанови нарушението и да възстанови положението преди нарушението, както и да се въздържа в бъдеще от по-нататъшни нарушения; 3. обезщетение за вреди.	Protection against Discrimination Act, Article 71 (1): Except for the cases under Section I, any person, whose rights under this or other laws, regulating equality in treatment, have been violated, may file a claim before the district court, with which to request: 1. establishment of the violation; 2. ordering the defendant to terminate the violation and to restore the situation before the violation, as well as to refrain in the future from further violations; 3. compensation for damages.
Закон за електронните съобщения, § 1, т. 29 от Допълнителните разпоредби: По смисъла на този закон: "Криптографски ключ" е низ от символи, който се използва в алгоритъм за преобразуване на информация от разбираем в шифриран вид (криптиране) или обратно - от шифриран в разбираем вид (декриптиране).	Electronic Communications Act, § 1 (29) of the Additional provisions: Within the meaning of this law: A "cryptographic key" is a string of characters used in an algorithm to convert information from intelligible to encrypted (encryption) or vice versa from encrypted to intelligible (decryption).
Закон за електронните съобщения, чл. 307: В случай че предприятията, предоставящи електронни съобщителни мрежи и/или услуги, предприемат кодиране, компресиране или криптиране на прихванатите електронни съобщения, те ги предоставят на Държавна агенция "Национална сигурност" или Държавна агенция "Технически операции" в първоначалния им вид.	Electronic Communications Act, Article 307: In case the enterprises providing electronic communications networks and/or services undertake encryption, compression or encryption of the intercepted electronic messages, they shall provide them to the State Agency for National Security or the State Agency for Technical Operations in their original form.

Закон за електронните съобщения, чл. 243: (1) Предприятията, предоставящи обществени електронни съобщителни мрежи или услуги, предприемат подходящи и пропорционални технически и организационни мерки за управление на риска за сигурността на мрежите и услугите, осигуряващи ниво на сигурност, съответстващо на оценения риск. (2) Мерките по ал. 1, включително криптиране, когато е целесъобразно, са насочени към предотвратяване и свеждане до минимум на въздействието от инциденти, свързани със сигурността, върху ползвателите и върху други мрежи и услуги.	Electronic Communications Act, Article 243: (1) Undertakings providing public electronic communications networks or services shall take appropriate and proportionate technical and organizational risk management measures for the security of networks and services providing a level of security commensurate with the assessed risk. (2) The measures under par. 1, including encryption, where appropriate, shall be aimed at preventing and minimizing the impact of security incidents on users and other networks and services.
Наказателно-процесуален кодекс, чл.	Criminal Procedure Code, Article
Наказателно-процесуален кодекс, чл. 163 (6): Иззетите предмети, книжа и компютърни информационни системи, в които се съдържат компютърни информационни данни, се предявяват на поемните лица и другите присъстващи. Когато е необходимо, те се опаковат и запечатват на мястото на изземването им.	Criminal Procedure Code, Article 163 (6) The seized objects, papers and computer information systems, which contain computer information data, are presented to the witnesses and the others present. Where necessary, they shall be packed and sealed at the place of seizure.
Наказателно-процесуален кодекс, чл. 159 (1): По искане на съда или на органите на досъдебното производство всички учреждения, юридически лица, длъжностни лица и граждани са длъжни да запазят и предадат намиращите се у тях предмети, книжа, компютърни информационни данни и други данни, които могат да имат значение за делото.	Criminal Procedure Code, Article 159 (1): At the request of the court or the bodies of the pre-trial proceedings, all institutions, legal entities, officials and citizens are obliged to preserve and hand over the objects, papers, computer information data and other data that may be relevant to the case.
Наказателно-процесуален кодекс, чл. 115 (4):	Criminal Procedure Code, Article 115 (4): The accused has the right to refuse to give explanations.

Обвиняемият има право да откаже да дава обяснения.	
Наказателно-процесуален кодекс, чл. 121 (1): Свидетелят не е длъжен да дава показания по въпроси, отговорите на които биха уличили в извършване на престъпление него, неговите възходящи, низходящи, братя, сестри или съпруг или лице, с което той се намира във фактическо съжителство.	Criminal Procedure Code, Article 121 (1): The witness is not obliged to testify on questions, the answers to which would accuse him, his ascendants, descendants, brothers, sisters or husband or a person with whom he is in actual cohabitation of committing a crime.

Bibliography

English titles

Legislation

Constitution of the Republic of Bulgaria

European Convention on Human Rights

Treaty on the Functioning of the European Union

Charter of the Fundamental Rights of the European Union

Universal Declaration of Human Rights

Personal Data Protection Act

Protection against Discrimination Act

Electronic Commerce Act

Electronic Communications Act

Electronic Communication Networks and Physical Infrastructure Act

Administrative Procedure Code

Criminal Procedure Code

Regulation (EU) 679/2016

Directive 95/46 EC

Case-law

Leander v. Sweden (app. no. 9248/87)

Pendov v. Bulgaria (app. no. 44229/11)

Bulgarian titles

Legislation

Конституция на Република България

Европейска Конвенция за Правата на Човека

Договор за Функционирането на Европейския Съюз

Харта на Основните Права на Европейския Съюз

Всеобща Декларация на Човешките Права

Закон за Защита на Личните Данни

Закон за Електронната Търговия

Закон за Електронните Съобщения

Закон за Електронните Мрежи и Физическата Инфраструктура

Административно-процесуален Кодекс

Наказателно-процесуален Кодекс

Регламент (ЕС) 679/2016

Директива 95/46 ЕК

Case-law

Леандър срещу Швеция (вх. н. 9248/87)

Пендов срещу България (вх. н. 44229/11)

ELSA FINLAND

Contributors

National Coordinator

Hanna Järvinen

National Researchers

Hanna Järvinen

Pinja Oksanen

Annika Antikainen

Susan Saarinen

Sofia Aalto-Setälä

Ilmari Eskola

Mikael Hitruhin

Heidimaria Manninen

National Linguistic Editors

Laura Vuorinen

Simranjit Kaur

National Academic Supervisor

Jenni Hakkarainen

Introduction

In its Government Programme, the current Finnish Government aims to further digitalisation. The objective is to streamline legislation so as to promote digitalisation and sustainable development.⁸⁸ Advanced Digital Technologies (ADT), which include Artificial Intelligence (AI), Internet of Things (IoT), big data, and encryption, may result in substantial benefits but also pose a threat to human rights by, for example, jeopardising the right to privacy, data protection, and equality. Automation and data analytics are utilised increasingly in various administrative procedures to enhance availability, efficiency, and exempting resources.⁸⁹ For example, the Finnish Tax Administration, utilises those in the income taxation assessment and the determination of an individual's withholding rate,⁹⁰ but also the Social Insurance Institution of Finland utilizes it, for example when deciding on student benefits. Automated decision-making is, however, permitted only when based on law, provided that the rules laid down in legislation can be programmed into the data processing system, and when individual decisions do not require human consideration. However, the Deputy Ombudsman has stated that the Tax Administration's automated procedure is not based on appropriate and precise legislation and has therefore considered it as illegal. The case concerned a situation where the automated procedure had not taken into consideration a conflict regarding various types of taxes, which then led to a 20 per cent increase in taxation and a delay penalty. The Deputy Ombudsman stated that the procedure did not comply with the principles of good administration and legal protection, and was thus against the Finnish Constitution.⁹¹ The above is an example of a case where automated procedures end up proving faulty despite conforming to legislation. This gives rise to a discussion about whether the implementation of ADT in administrative procedures, as well as the technology utilised by private operators, is beneficial or even appropriate, or whether it poses a threat to the core elements of law, such as human rights.

As an EU member state, Finland is obligated to implement EU legislation; it has also implemented the European Convention on Human Rights (ECHR) and is thus obligated to secure the effective implementation of human rights. Technology is thus a common issue for both Finland and the EU, and its impacts are not delimited by state borders. As a result, there is increasing demand for regulation on technology at both EU and national level. New legislation is being considered, not only in Finland but in the EU as well. A recent example is the Artificial Intelligence Act, which has now been officially proposed to

⁸⁸ Finnish Government, 'Digitalisaatio, kokeilut ja normien purkaminen'

<<https://valtioneuvosto.fi/hallitusohjelman-toteutus/digitalisaatio>> accessed 30 May 2021.

⁸⁹ Finance Finland, 'Arviomuistio hallinnon automaattiseen päätöksentekoon liittyvistä yleislainsäädännön sääntelytarpeista'

<https://www.finanssiala.fi/wp-content/uploads/2020/09/EA_lausunto_040920_OM_Arviomuistio20yleislainsaadannon_saantelytarpeet_hallinnon_automattinen_paatoksenteke.pdf> accessed 1 June 2021.

⁹⁰ Finnish Tax Administration, 'Automaattinen päätöksenteko verotuksessa'

<www.vero.fi/tietoa-verohallinnosta/verohallinnon_esittely/tietosuoja-ja-julkisuus/tietojen_kasittely_ja_tietosuoj/automaattinen-paatoksenteke/> accessed 10 May 2021.

⁹¹ Deputy Parliamentary Ombudsman, *Verohallinnon automatisoitu päätöksentekomenettely ei täytä perustuslain vaatimuksia* (3379/2018, 20 November 2019) <www.oikeusasiamies.fi/r/fi/ratkaisut/-/eoar/3379/2018> accessed 26 April 2021.

address the possible risks arising because of AI technology, and to prohibit such actions that could violate EU values and fundamental rights.⁹² The need for legislation on automated decision procedures has been recognized in Finland as well.⁹³ This is an important and topical subject that needs to be looked into from various points of view. The world of technology is evolving fast, and the legislator, for its part, strives to respond to its developments. Which is why this report will discuss the challenges and opportunities of ADT in further detail from the Finnish perspective, with a particular emphasis on the aspects of human rights and data protection. This report also makes an effort to examine the national legal state and mirror it against the cooperation between Finland and the EU.

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

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

In 2018, the Finnish Government started a project to establish a national AI programme called Aurora. Its purpose is to develop public sector services with artificial intelligence. In this project's consultation round, concerns about privacy and equality emerged. For example, biased profiling based on distorted data obtained by AI can cause problems for job seekers.⁹⁴ Furthermore, the Non-Discrimination Ombudsman stated that there should also be a clear responsible authority that could be held responsible for potential malfunctions.⁹⁵

Another issue that has been identified at the international level as well is the threat that profiling and automated decisions pose to individuals and, above all, to equality. At worst, technologies can produce discriminatory decisions to individuals. In spring 2018, the National Non-Discrimination and Equality Tribunal of Finland knowingly gave the very first decision in Europe in a case concerning algorithmic bias, identifying a creditor's actions as discriminatory. In this case, a man applied for credit to buy building supplies but his application was denied by automated decision-making. Automatic profiling was based on the person's place of residence, gender, language, and age, among other features. On the basis of population information, the system calculated what percentage of each group had payment defaults. For example, men scored less points since statistically defaults are more common for men. Loans were granted on the basis of the scoring system. The Tribunal

⁹² See, e.g. Commission, 'Proposal for a Regulation laying down harmonised rules on artificial intelligence. Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM (2021) 206 Final. Available online at <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence> accessed 26 May 2021.

⁹³ Parliament of Finland, 'Yleislainsäädäntö automaattiselle päätöksenteolle' https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/yleislainsaadanto-automaattiselle-paatoksenteolle.aspx > accessed 20 May 2021.

⁹⁴ Ministry of Finance, *Lausuntoyhteenvedo: Kansallisen tekoälyohjelma Aurora AI:n kehittämis- ja toimeenpanosuunnitelma vuosille 2019-2023*,

https://vm.fi/documents/10623/13292513/AuroraAI_lausuntoyhteenvedo.pdf/0a2375f4-3795-81a8-a0f7-9589697756a4/AuroraAI_lausuntoyhteenvedo.pdf accessed 11 March 2021, 31.

⁹⁵ *ibid* 34.

found the creditors' actions discriminatory and imposed a significant penalty payment on the credit company.⁹⁶

1.2. Is there or what is a legal framework that provides for procedure on human rights impact assessments?

There is no existing regulation in Finland on human right related issues, or any issues, arising from the use of ADT. No legal framework that would provide for a procedure for human rights impact assessments has been enacted in Finland. The Finnish Non-Discrimination Act imposes a comprehensive obligation for public authorities and officials to promote and safeguard equality and lists supervisory officials whose task it is to supervise the compliance with the terms of this Act.⁹⁷

1.3. What are other instruments used for identifying human rights issues posed by ADT?

There are ex-post and ex-ante instruments used for identifying human rights issues in Finland. The Constitutional Law Committee of Finland supervises the compliance with the Finnish Constitution of any new laws to be enacted. The Constitution provides an obligation for public authorities to safeguard human rights (section 22).⁹⁸ Moreover, the Committee sees to it that no law violating human rights, and therefore in conflict with the Constitution, will be enacted.

As ex-post instruments there are several Ombudsmen: the Ombudsman for Children, the Data Protection Ombudsman, the Ombudsman for Equality, the Non-Discrimination Ombudsman and the two supreme overseers of legality in Finland, the Chancellor of Justice⁹⁹ and the Parliamentary Ombudsman.¹⁰⁰ They all oversee that human rights of individuals are not violated in Finland, review complaints and declare if a violation has occurred or been suspected, including those arising from the use of ADT.¹⁰¹ Due to threats and possibilities posed by ADT, the Chancellor of Justice has a new special task to monitor the legality of the administration's automatic decision-making and the general development of automated systems as well.¹⁰² No specific guidelines have yet been issued.

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

As stated in the previous section, collecting huge amounts of data of individuals necessarily involves personal information and might pose a threat to an individual's right to the protection of their personal data and privacy. Both of these rights - the right to privacy and the right to the protection of personal data - are protected as fundamental rights by

⁹⁶ National Non-Discrimination and Equality Tribunal of Finland 216/2017, <www.yvtltk.fi/material/attachments/ytltk/tapausselosteet/2SVkNzOWE/YVTltk-tapausseloste-21.3.2018-luotto-moniperusteinen_syrjinta-S_L.pdf> accessed 11 March 2021.

⁹⁷ Non-Discrimination Act (21/2004) [Yhdenvertaisuuslaki].

⁹⁸ Constitution of Finland (731/1999) [Perustuslaki].

⁹⁹ Act on the Parliamentary Ombudsman (197/2002) [Laki eduskunnan oikeusasiamiehestä].

¹⁰⁰ Act on the Chancellor of Justice (193/2000) [Laki valtioneuvoston oikeuskanslerista].

¹⁰¹ *ibid.*

¹⁰² Sanna Nikula, 'Oikeuskansleri Pöysti kiirehtii pelisääntöjä tekoälyn käyttöön: "Kenen on vastuu, jos kone tekee virheen?"' *Helsingin Sanomat* (Helsinki, 16 November 2019) <www.hs.fi/kotimaa/art-2000006311312.html> accessed 11 March 2021.

separate articles in the Charter of Fundamental Rights of the European Union (CFR).¹⁰³ Data protection is safeguarded by the EU's secondary legislation, such as the General Data Protection Regulation (GDPR). Finland has been an EU member state since 1995, so both the EU treaties and regulations are directly applicable.¹⁰⁴ The European Court of Justice (ECJ) has established the primacy of EU law over the laws of the Member States.¹⁰⁵ Because of the directly applicable nature and primacy of EU law, Finland is bound by the EU definition of the concept of personal data, and EU legislation sets a minimum standard for the protection of personal data.

GDPR art. 4(1) defines personal data as any information relating to an identified or identifiable natural person. In its case law, the ECJ has interpreted the concept of personal data rather widely, and e.g. a dynamic IP address, essay grade, and handwritten notes have fallen under the concept of personal data.¹⁰⁶ In addition to case law, the concept of personal data has also been clarified in non-binding soft law: in its opinion 4/2007, the Article 29 Working Party ('WP 29')¹⁰⁷ has given guidance for the interpretation of personal data. These guidelines are not outdated in the era of the GDPR, since the concept of personal data has not been narrowed down - quite the contrary.¹⁰⁸

Actually, a broad interpretation of personal data undoubtedly gives the GDPR a larger scope of application in a world of fast and unpredictable technological development. The European Commission itself has stated that technology evolves rapidly and the collection of vast amounts of personal data poses new challenges for data protection. It also suggests that building trust in the online environment would add balance to both data protection and economic development.¹⁰⁹ Moreover, according to *Lindroos-Hovinheimo*, the spirit of the GDPR is that the protection of personal data must be taken seriously.¹¹⁰ This might be one of the main reasons why the concept of personal data has nowadays been given such a wide interpretation.

Certain parts of the GDPR leave the member states a margin of discretion. However, no national margin of consideration is left as regards the concept of personal data, as it has

¹⁰³ Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

¹⁰⁴ 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). On EU regulations and direct applicability, see e.g. Juha Raitio, *Euroopan unionin oikeus* (Alma Talent 2020) 229 and 131-132.

¹⁰⁵ See ECJ's landmark decision, Case 6/64 *Flaminio Costa v E.N.E.L.* [1964] EU:C:1964:66.

¹⁰⁶ E.g. a dynamic IP address was interpreted as personal data in Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] EU:C:2016:779, an essay grade in Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] EU:C:2017:994, and handwritten notes in Case C-25/17 *Jehovan todistajat* (proceedings brought by Tietosuojavaltuutettu) [2018] EU:C:2018:551.

¹⁰⁷ WP 29 has since been replaced by the European Data Protection Board, which has decided to adopt all opinions of WP 29.

¹⁰⁸ Päivi Korpisaari, Olli Pitkänen, Eija Warma-Lehtinen, *Unsi Tietosuojalainsäädäntö* (Alma Talent 2018) 52-53.

¹⁰⁹ Commission, 'Proposal for a Regulation 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' COM (2012) 11 final, 1.

¹¹⁰ Susanna Lindroos-Hovinheimo, 'Henkilötietojen suoja EU-oikeudessa – yksityisyyttä yhteisön kustannuksella?' *Lakimies* 1/2018, 52, 53.

already been defined in the GDPR.¹¹¹ Recently, the Data Protection Ombudsman, who is the data protection authority ('DPA') in Finland, had a case that concerned both the concept of personal data and the legal basis for processing. The decision of the Finnish DPA reflects the broad interpretation of the concept of personal data by the national authority, in accordance with the interpretation set out in EU law. According to the decision, the data related to door openings in an apartment building's electronic lock system were to be seen as personal data since, by combining the key identification information with the information of a certain apartment, it was possible to identify the person who opened the door. The Data Protection Ombudsman stated, in line with EU law, that data do not need to be directly linked to the data subject in order for them to be categorised as personal data.¹¹²

As stated earlier, EU member states are left no margin of discretion when defining the concept of personal data, but there are national laws that complement the GDPR. Nationally, the general law (*lex generalis*) supplementing the GDPR is the Data Protection Act (in Finnish *Tietosuojalaki* 1050/2018). In addition, there are a number of special laws (*lex specialis*) that protect personal data. Much of the special legislation concerns the processing of personal data by public authorities, whereas other legislation regulating the processing of personal data relates to specific fields, such as the processing of an employee's personal data. As a matter of fact, in international comparison employees' personal data are protected at a very high level in Finland;¹¹³ this is allowed by EU law, since it only sets a minimum standard for the protection of personal data.

As a conclusion, the right to the protection of personal data is protected on a quite high level in both national and international legislation¹¹⁴ that Finland must comply with.

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?

As was explained in the previous question, there are a variety of regulatory instruments issued by national and international bodies that apply to data protection in Finland.

¹¹¹ See also Päivi Korpisaari, 'Henkilötiedot ja paikkatiedot: Miten tietosuojalainsäädäntö vaikuttaa paikkatietojen julkaisemiseen ja luovuttamiseen' Ympäristöministeriön raportteja 10/2018, 40, where it is further explained that 'personal data' does not necessarily mean sensitive information and that personal data do not necessarily relate to a person's private life. However, the nature of the information becomes relevant when considering how the information may be disclosed. Available in Finnish at https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160578/YMra_10_2018_Henkilotiedot_ja_paikkatiedot.pdf accessed 9 February 2021.

¹¹² Data Ombudsman, *Asuinrakennuksen yleisiin oviin asennettuun sähkölukkojärjestelmään liittyvä henkilötietojen käsittely* (1809/452/18, 29 July 2020) <www.finlex.fi/fi/viranomaiset/tsv/2020/20200661> accessed 8 March 2021.

¹¹³ See e.g. Kaisa Päivinen and Krista Poitsalo, 'Uudistunut työelämän tietosuojasääntely tuo yrityksille haasteita' (FIBS, 8 April 2019) <www.fibsry.fi/ajankohtaista/uudistunut-tyoelaman-tietosuojasaaentely-tuo-yrityksille-haasteita/> accessed 7 March 2021.

¹¹⁴ See also Council of Europe, the European Convention of Human Rights, Art. 8, and the Convention for the Protection of Individuals with Regard To Automatic Processing of Personal Data (SopS 35/92 and 36/92).

Despite adopting these regulations, Finland is still having issues with the challenges of the digital era.

The Constitutional Law Committee has noted that the current regulatory model is quite heavy and complex.¹¹⁵ Actors have found the Regulation to be hard to understand due to its wide interpretation¹¹⁶, but also partially impractical. This gives rise to a debate on its adequacy.

The customers' personal data is valuable for future investments, which in a way has motivated the organisations to strengthen their data policies, despite the uncertainties. Traditional law-making processes are no longer sufficient as the concepts may not be suitable for the new digital age, or the administrative bodies are too slow to deal with the emerging issues. Hence, we can argue that the regulations mentioned above only establish a baseline and need to be supplemented with 'complementary' options.

One form of complementary approach is self-regulation models, which rely on the individual actors being urged to ensure a sufficient level of protection before turning to the state regulators.¹¹⁷ Self-regulation can be defined as 'the possibility for economic operators, social partners, non-governmental organisations or associations to adopt common guidelines amongst themselves'.¹¹⁸ Those in favour of self-regulation have argued that it may not only be a cheaper option, since companies can adopt measures that benefit their individual needs, but also a more efficient way compared to the statutory regulations to keep up with the technological changes. Additionally, self-regulation can decrease the risks to consumers and impose rules to govern the behaviour of companies.¹¹⁹

On the other hand, the GDPR incorporates the principle of accountability into the Finnish national provisions, requiring companies to actively demonstrate their compliance with the Regulation.¹²⁰ Self-regulation is an accountability mechanism which encourages companies to update their contracts and internal practices, which require considerable resources.¹²¹ This being said, self-regulation can offer the private sector more leeway in how to implement the statutory regulations into the company practices.

The State Digital Programme¹²² encourages the authorities to develop the production of digital services. The private sector plays an important role in software development, and

¹¹⁵ HaVM 13/2018 vp, 5. See also PeVL 31/2017 vp and PeVL 45/2016 vp for previous statements.

¹¹⁶ Anna Pohjalainen and Laura Ylikoski, 'EU:n yleisen tietosuoja-asetuksen soveltamiskokemuksia Suomessa' Oikeusministeriön julkaisuja 2020:7, 17-18.

¹¹⁷ Hans J. Kleinsteuber, 'The Internet between Regulation and Governance' in Christian Möller and Arnaud Amouroux (eds), *The Media Freedom Internet Cookbook* (OSCE Representative on Freedom of the Media 2004).

¹¹⁸ European Commission, European Parliament & Council of Ministers (2003), 'Inter-Institutional Agreement on Better Lawmaking', OJC 321, 31.12.2003, 1.

¹¹⁹ J. J. Boddewyn, 'Advertising Self-Regulation' (1985) *Journal of Public Policy & Marketing* Vol. 4 131; Daniel Castro, *Benefits and Limitations of Industry Self-regulation for Online Behavioral Advertising*, The Information Technology and Innovation Foundation (2011) 2.

¹²⁰ Christina Tikkunen-Piri, Anna Rohunen and Jouni Makkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' (2018) 34 *Computer Law and Security Review* 134, 21.

¹²¹ The Association of Finnish Lawyers, *Lausunto yleisen tietosuoja-asetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista* (VN/5281/2019, 2019).

¹²² Ministry of Finance, *Digitalisaation edistämisen ohjelman toimintakertomus 2020* (VN/714/2020).

has the resources to provide innovations, which make the services more user-friendly. Another relevant indication of cross-sectoral cooperation is the role of the private sector in government projects. One example is the Cybersecurity Label that helps consumers choose secure digital devices and companies show their responsibility with regard to data protection issues.¹²³ The idea behind the label is that companies evaluate their cybersecurity and data protection practices. If the safeguards are appropriate, the Finnish Transport and Communications Agency Traficom awards the company a one-year certificate. The requirements of the Finnish Cybersecurity Label follow the European standards.¹²⁴ Additionally, the Cybersecurity Label helps companies demonstrate corporate responsibility and adapt their practices to European developments.

Finland is increasingly moving towards the MyData approach, which allows individuals to control their digital footprint: they not only have the right to see, monitor and know what kind of data has been collected but also have to obtain and erase it. It is based on cross-sectoral action to facilitate the coordination of public and private services.¹²⁵ MyData aims to offer a solution to the problems and abuse of personal data by introducing new ways to safeguard digital rights and data mobility. The approach is relevant especially from the Finnish health care's perspective. The health care system relies largely on private sector innovations. MyData could be a step towards digital health care, which citizens could use not only to get information on services, but also to track their own well-being. By using MyData, citizens could add their own data to the system to complement the existing health data, therefore contributing to the development of better services.

Another concrete example of multi-sectoral platforms is the *suomi.fi* web service, which is provided by the Finnish Digital and Population Data Services Agency. The suomi.fi service offers both public and private sector organisations a secure way to transfer data.¹²⁶ Many organisations have chosen to use the service as part of their own platform, for example to verify the user's identity as one needs to log into the system by using personal ID credentials. An individual can use the service to view their own data on various official registers, use digital public services or fill electronic forms. The system also includes a secure message system that allows citizens and companies to communicate with authorities. This makes the services faster and easier to access regardless of the individual's location. Furthermore, the platform is a demonstration of modern cross-border cooperation.¹²⁷

¹²³ See Cybersecurity, 'What is the Finnish Cybersecurity Label?' <<https://tietoturvamerkki.fi/en/>> accessed 14 March 2021 and Traficom, 'Finland becomes the first European country to certify safe smart devices - new Cybersecurity label helps consumers buy safer products' <www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label> accessed 14 March 2021.

¹²⁴ Cyber Security for Consumer Internet of Things: Baseline Requirements ETSI EN 303 645 V2.1.0 (4/2020).

¹²⁵ Antti Poikola, Kai Kuikkaniemi and Ossi Kuittinen, *My Data - Jobdatus ihmiskeskiseen henkilöidon hyödyntämiseen* (Liikenne- ja viestintäministeriö 2014, updated in 2018) 63.

¹²⁶ European Commission, Digital Government Factsheet 2019: Finland.

¹²⁷ See, e.g. Republic of Estonia: Information System Authority, 'PRC: Finland's and Estonia's data exchange layers connected to one another on 7 February - the rapid exchange of information between the countries is now possible' <www.ria.ee/en/news/prc-finlands-and-estonias-data-exchange-layers-connected.html> accessed 14 March 2021.

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

4.1. Right to data privacy

The right to privacy and the right to data privacy are two different rights, each with its own legal basis; however, the two rights are closely intertwined. The right to data privacy is laid down in section 10 of the Constitution of Finland.¹²⁸ The European Union's GDPR, which has been supplemented and clarified by the Finnish Data Protection Act,¹²⁹ is the most significant piece of legislation for the protection of personal data in Finland. The central obligation related to the processing of personal data comes directly from the GDPR.

Furthermore, Article 8 of the ECHR, Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union (CFR), and Article 16 of the TFEU, all guarantee the right to the protection of privacy and personal data. With all these instruments, Finland has committed to protecting data privacy and the effective compliance with these laws must therefore be enforced with effective judicial review.

4.2. The data subject's rights to restrict or object to the processing of data

In Finland, the data subject's rights to restrict and object to the processing of personal data follows the rules set by the GDPR. The underlying notion behind the restriction and objection rights is that if the processing of data is based on legal grounds, it is permitted unless the data subject expresses an objection to it.

The data subject has the right to restrict the processing of his or her own data under the circumstances defined in Article 18 of the GDPR. Under Article 21, the data subject also has the right, on specific grounds, to object to the processing of data. This may occur when public authorities process the data for public tasks or when a data controller processes data on the basis of legitimate interests. Data controllers must stop the processing unless they can demonstrate that there are compelling legitimate grounds for processing that override the data subject's rights. However, neither the GDPR nor the Finnish legislation define the concept of compelling legitimate grounds. Recital 69 and Article 21 only add that they are based on the objective assessment by the controller. It is also permitted to object to the processing of personal data without any specific grounds at all times in cases of direct marketing under Article 21(2)-(3).¹³⁰

In addition, the GDPR allows the data subject to withdraw a previously given consent for the processing at any time, when data is processed based on consent. When the processing of data is based on public or legitimate interests, the data subject can object to the processing in accordance with Article 21.

¹²⁸ Constitution of Finland (731/1999) [Perustuslaki].

¹²⁹ Data Protection Act (1050/2018) [Tietosuojalaki].

¹³⁰ Data Protection Ombudsman, 'Riittävästä toimenpiteistä huolehtiminen rekisteröidyn oikeuksien toteuttamiseksi' (9209/157/2019, 22 January 2021) <www.edilex.fi/tsv/20210724> accessed 19 February 2021. The Data Protection Ombudsman issued a reprimand to a data controller stating that it could not justify continuing direct marketing after the data subject had prohibited it with a technical error in its systems.

Furthermore, Article 89 of the GDPR allows Member States to add exemptions or derogations from the data subject's rights.¹³¹ Pursuant to section 31 and section 32 of the Finnish Data Protection Act, the rights of the data subject laid down in Article 18 and Article 21 may be derogated from when personal data is processed for scientific or historical research purposes or for archiving purposes in the public interest. Therefore, these rights are not absolute.

4.3 Communication of a data protection breach to the data subject

In Finland, a personal data breach is mostly communicated to the data subject in accordance with Article 34 of the GDPR. The breach must be communicated to the data subject when the breach is likely to result in a high risk to the rights and freedoms of the data subject. In addition, the Data Protection Ombudsman can order a data controller to communicate the breach to a data subject, when the notification does not fulfil the GDPR standards. When assessing the likelihood and severity of the risks resulting from the breach, the evaluation is based on the objective assessment by the data controller.¹³² This highlights the responsibility of the data controller, since it shifts the burden of communicating the breach to the controller. As seen in the recent case of Vastaamo, an incorrect assessment from the data controller could lead to serious physical, material or non-material damage for the data subject.

In October 2020, Vastaamo - Finland's largest private psychotherapy center - reported that confidential treatment records of thousands of patients had been hacked and partially leaked online.¹³³ Vastaamo stated that its database had first been breached in November 2018 and a second time in March 2019.¹³⁴ However, Vastaamo did not communicate the breaches to the Data Protection Ombudsman or to the data subjects. The breach became national news after Vastaamo, its patients and staff members received extortion messages demanding them to pay ransom to stop additional leaks.¹³⁵ Vastaamo's CEO knew of at least one of the two data breaches.¹³⁶ However, national authorities or data subjects were not notified before the extortion messages.

In October 2020, Vastaamo finally communicated the breach to the data subjects by publishing a communication on Vastaamo's website to fulfil its obligations under Article 34 of the GDPR. However, the Deputy Data Protection Ombudsman issued a reprimand and

¹³¹ Päivi Korpisaari, Olli Pitkänen and Eija Warma-Lehtinen, *Unsi Tietosuojalainsäädäntö* (Alma Talent 2018) 254-256.

¹³² Recitals 75 and 76 of the GDPR.

¹³³ Veli-Pekka Hämäläinen and Anu Rummukainen, "'Onko herra Ransom mokannut?'" Näin Vastaamon kiristäjä ilmestyi Tor-verkon foorumille, sai hakkerit peräänsä ja häipyi tyhjin käsin' (*Yle News*, 30 October 2020) <<https://yle.fi/uutiset/3-11616210>> accessed 20 February 2021.

¹³⁴ 'Vastaamo board fires CEO, says he kept data breach secret for year and a half' (*Yle News*, 26 October 2020) <https://yle.fi/uutiset/osasto/news/vastaamo_board_fires_ceo_says_he_kept_data_breach_secret_for_year_and_a_half/11614603> accessed 7 March 2021.

¹³⁵ *ibid.*

¹³⁶ Veli-Pekka Hämäläinen and Anu Rummukainen, "'Onko herra Ransom mokannut?'" Näin Vastaamon kiristäjä ilmestyi Tor-verkon foorumille, sai hakkerit peräänsä ja häipyi tyhjin käsin' (*Yle News*, 30 October 2020) <<https://yle.fi/uutiset/3-11616210>> accessed 20 February 2021.

ordered Vastaamo to comply with the GDPR. The Deputy Ombudsman ordered Vastaamo to personally communicate the breach to the data subjects. The Deputy Ombudsman noted that a communication on the Vastaamo website was not alone sufficient to effectively communicate the data breach concerning confidential data.¹³⁷

In addition to Article 34 of the GDPR, Section 274 of the Finnish Information Society Code¹³⁸ establishes an obligation for telecommunication operators to communicate any significant information security violations or threats to their subscribers and users. Additionally, in accordance with section 16 of the Act on Strong Electronic Identification and Electronic Signatures,¹³⁹ it is necessary to inform the identification device holders in case of a severe risk or threat to their data security.

To conclude, in Finland the main obligations related to the processing of personal data, restricting and objecting to the processing as well as communicating a breach to the data subjects come directly from the GDPR. The GDPR emphasises the responsibility of the data controller to ensure that data subjects can exercise their rights. Therefore, the data subjects need an effective remedy mechanism in cases where the controller fails to comply with the GDPR.

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

5.1. Which bodies conduct such a review?

The right to an effective judicial review and remedy are fundamental rights. These rights are protected under section 21 of the Constitution of Finland, Article 47 of the CFR and Article 13 of the ECHR. The GDPR stipulates judicial review and remedies in cases of a data breach. The following Chapter focuses on the Finnish data protection authority, the judiciary and the remedies available for data subjects.

In Finland, the Office of the Data Protection Ombudsman is the national supervisory authority.¹⁴⁰ It is an independent and autonomous authority appointed by the Government. Together with the Deputy Ombudsman, the Data Protection Ombudsman monitors the compliance with the data protection legislation in Finland and forms the Sanctions Board, which is tasked with imposing administrative fines in accordance with Article 83 of the GDPR.¹⁴¹

5.2. The process of judicial review in case of a data protection breach

¹³⁷ Office of the Data Protection Ombudsman, 'The Deputy Data Protection Ombudsman has ordered Vastaamo to notify personally its customers who have become victims of the personal data breach' [press release 23 October 2020]

<<https://tietosuoja.fi/-/apulaistietosuojavaaltuutettu-maarasi-psykoterapiakeskus-vastaamon-ilmoittamaan-tie tomurron-kohteeksi-joutuneille-asiakkailleen-henkilokohtaisesti>> accessed 18 February 2021.

¹³⁸ Information Society Code (917/2014) [Tietoyhteiskuntakaari].

¹³⁹ Act on Strong Electronic Identification and Electronic Trust Services (617/2009) [Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista].

¹⁴⁰ Data Protection Act (1050/2018) [Tietosuoja laki], Chapter 5 (Supervisory Authority).

¹⁴¹ Office of the Data Protection Ombudsman, 'The Office of the Data Protection Ombudsman safeguards your data protection rights'

<<https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman>> accessed 8 March 2021.

Under Finland's legislation, a number of remedy mechanisms are available to data subjects in case of data protection violations. The spectrum of judicial review and remedies ranges from administrative to both criminal and civil proceedings. These measures do not exclude each other.

Firstly, data subjects have the right to lodge a complaint with the Data Protection Ombudsman if their rights have been violated according to Articles 77 and 78 of the GDPR and section 21 of the Data Protection Act. After the initiation from the data subject, the Data Protection Ombudsman will decide whether to start an administrative process. The initiation of an administrative process is regulated by the Administrative Procedure Act.¹⁴² The Data Protection Ombudsman can also initiate these proceedings.

After starting the process and hearing the parties, the Data Protection Ombudsman may issue an appealable, written administrative decision in accordance with Article 58 of the GDPR. An appeal against the decision of the Data Protection Ombudsman may be filed with an Administrative Court in accordance with section 25 of the Data Protection Act and section 10 of the Administrative Judicial Procedure Act.¹⁴³ The decision of an Administrative Court can be appealed against to the Supreme Administrative Court in certain situations.

It is important to note that, with section 24(4) of the Data Protection Act, Finland added a derogation from the administrative penalties in accordance with Article 83(7) of the GDPR. Therefore, administrative fines cannot be imposed on public authorities and bodies in Finland.¹⁴⁴ This was highly debated during the preparation of the legislation. The Data Protection Ombudsman argued that the exclusion of public authorities from the administrative fine system puts the data subjects' rights in a very questionable light, since a data subject cannot typically decide if their data are processed for public purposes.¹⁴⁵

In addition to the administrative process, criminal sanctions may result from breaches of Finland's data protection laws under the Criminal Code of Finland.¹⁴⁶ For data-related criminal acts, a preliminary investigation will be conducted only if the injured party informs the pre-trial investigation authority or the prosecutor that he or she will request punishment for the offender.¹⁴⁷ Chapter 38 of the Criminal Code of Finland lays down several data processing, data privacy and data security related offences or crimes, including computer break-in and identity theft. The data protection offence, based on the GDPR,

¹⁴² Administrative Procedure Act (434/2003) [Hallintolaki].

¹⁴³ Administrative Judicial Procedure Act (808/2019) [Laki oikeudenkäynnistä hallintoasioissa].

¹⁴⁴ Public authorities are listed under section 24(4) of the Data Protection Act (1050/2018).

¹⁴⁵ Opinion of the Office of the Data Protection Ombudsman in case HE 9/2018 vp. Government's Proposal to Parliament for Legislation Supplementing the GDPR, on 15 March 2018 <www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-177690.pdf> accessed 8 March 2021.

¹⁴⁶ Criminal Code of Finland (39/1889) [Rikoslaki].

¹⁴⁷ Criminal Procedure Act (1997/689) [Laki oikeudenkäynnistä rikosasioissa].

has been introduced thereto.¹⁴⁸ Criminal liability is only an option for natural persons but not for legal persons.

Furthermore, in accordance with Article 82 of the GDPR, data controllers can also be liable for both material and non-material damage if a data subject has incurred damage as a result of the data breach. The data subject must claim compensation before the courts that are competent under Finnish law. The grounds for damages are laid down in the Finnish Tort Liability Act.¹⁴⁹ A claim for damages is heard in the national courts either alongside a criminal case or in connection with a civil action. Compensable damage includes, e.g. financial loss and intangible damage, such as mental suffering.¹⁵⁰

5.3. Does the review provide effective remedies to data protection breaches?

As seen above, Finnish legislation offers data subjects various remedy mechanisms when data subjects' rights have been breached. The assessment of what is an effective and proportioned remedy with regard to each data protection breach reflects the objective pursued by the chosen corrective measure.¹⁵¹ The aim can be to re-establish compliance with the law, to punish unlawful behaviour or even both.¹⁵²

In Finland, the Data Protection Ombudsman has imposed six administrative fines ranging from EUR 7,000 up to EUR 100,000 between May 2020 and May 2021. All six cases concerned violations of basic GDPR obligations and principles including non-compliance with general data processing principles. These decisions play an important role in the enforcement of data protection systems, since the aim is to prevent data controllers' GDPR violations in the future. However, an administrative fine imposed on the data controller to encourage them to comply with the GDPR does not rectify the damage incurred by the data subject.

The remedial system in Finland relies heavily on the active initiative taken by the data subject who wishes to exercise their rights under the GDPR.¹⁵³ As an example, all six cases above were brought to the Data Protection Ombudsman's attention by individual claims or tips from data subjects. Furthermore, in criminal and civil cases, a data subject has to actively initiate the proceedings. If damage has occurred due to a breach or violation of the GDPR, the data subject also has the burden of proof to demonstrate the link between the breach and the damage in civil cases. However, not all data subjects have the resources and knowledge to uncover non-compliance or data breaches and take further legal actions. In addition, the cost and complexity of the process can make remedy mechanisms ineffective

¹⁴⁸ DLA Piper's Data Protection Laws of the World Handbook (updated 12 January 2021) 269 <www.dlapiperdataprotection.com/index.html?t=about&c=FI> accessed March 8 2021.

¹⁴⁹ Tort Liability Act (412/1974) [Vahingonkorvauslaki].

¹⁵⁰ Päivi Korpisaari, Olli Pitkänen and Eija Warma-Lehtinen, *Uusi Tietosuojalainsäädäntö* (Alma Talent 2018) 523.

¹⁵¹ Article 29 Working Party, *Guidelines on the Application and Setting of Administrative Fines for the Purpose of the Regulation 2016/679* (3 October 2017). 6.

¹⁵² *ibid.*

¹⁵³ Charlotta Sittnikow, 'First Four Administrative Fines issued for non-compliance with the GDPR in Finland' (*Waselius & Wist Legal Updates*, 4 June 2020) <www.wf.fi/news/2020/06/first-four-administrative-fines-issued-for-non-compliance-with-the-gdpr-in-finland/#content> accessed 28 April 2021.

in practice. For all these reasons, the judicial review and remedy mechanism is not necessarily effective from the data subject's point of view.

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?

In Finland judicial reviews of anti-discrimination cases are conducted by several different authorities: the two supreme overseers of legality (the Parliamentary Ombudsman of Finland and the Chancellor of Justice) and the Special Ombudsmen. The jurisdiction of these bodies conducting the judicial review is more or less overlapping and therefore there are no strict rules on to whom a person must address their complaint. The supervision is conducted on their initiative and by investigating the complaints. They do not investigate the same cases but do transfer the cases *ex officio* to each other, if necessary.

The tasks of the two supreme overseers of legality are divided into supervising the lawfulness of the official acts of the Government and investigating complaints about the actions of public authorities or officials. The Chancellor of Justice also oversees the actions of attorneys, the president, the government, the ministries and the courts¹⁵⁴ while the Parliamentary Ombudsman oversees the Defence Forces, the Border Guard and prisons.¹⁵⁵ Unlike with the Chancellor of Justice and the Parliamentary Ombudsman, the Special Ombudsman's jurisdiction also extends to the private sector. In regards to gender-discriminatory cases, the judicial review is conducted by the Ombudsman for Equality.¹⁵⁶ Anti-discrimination cases related to data processing belong mainly to the Data Protection Ombudsman¹⁵⁷ and discrimination concerning children to the Ombudsman for Children, who oversees that rights of children are taken into account in the legislative preparation phase but does not review any complaints.¹⁵⁸ However, in matters regarding discriminatory cases, the Non-Discrimination Ombudsman¹⁵⁹ is the Special Ombudsman whose task is expressly to supervise compliance with non-discrimination provisions in the use of AI and algorithms.¹⁶⁰

When an individual has been discriminated against in the private or public sector, they may take their case to the court themselves or ask for a judicial review from these previously mentioned authorities. For example, the Non-Discrimination Ombudsman investigates, whether there has been discriminatory behaviour and then decides whether to refer the case to the Equality and Gender Equality Board or a court. Not all different treatments are

¹⁵⁴ Act on the Parliamentary Ombudsman (197/2002) [Laki eduskunnan oikeusasiamiehestä].

¹⁵⁵ Act on the Chancellor of Justice (193/2000) [Laki valtioneuvoston oikeuskanslerista].

¹⁵⁶ Act on the Ombudsman for Equality (1328/2014) [Laki tasa-arvovaltuutetusta].

¹⁵⁷ Data Protection Act (1050/2018) [Tietosuojalaki].

¹⁵⁸ Act on the Ombudsman for Children (1221/2004) [Laki lapsiasiavaltuutetusta].

¹⁵⁹ Act on the Non-Discrimination Ombudsman (1326/2014) [Laki yhdenvertaisuusvaltuutetusta].

¹⁶⁰ Non-Discrimination Ombudsman, 'Artificial Intelligence and Equality'
<<https://syrjinta.fi/en/artificial-intelligence-and-equality>> accessed 2 April 2021.

to be constituted as discrimination: according to the Non-Discrimination Act, if actions are based on a law or otherwise proportionate, they are not discriminative.¹⁶¹

6.2. Does the review constitute effective protection against discrimination?

The Finnish system is beneficial because it provides both *ex-ante* and *ex-post* control: The Constitutional Law Committee monitors that the legislative proposals are in accordance with human rights and the other multiple numbers of authorities safeguard anti-discrimination issues after the laws have been enacted. Considering that there is no legal framework for the use of AI, the importance of the Ombudsmen, more specifically the Non-Discrimination Ombudsman, increases. When there is no explicit legislation, definitions of policy or even guidelines, it is evident that there are different authorities who safeguard the human rights issues. A complaint to an Ombudsman is also an easier way to receive legal protection than a “regular” court proceeding since there is naturally a lower threshold to seek legal protection this way as lawyers would not be needed to conduct the complaint. However, the Ministry of Justice released a review in 2020, stating that discrimination is still a serious issue in Finland.¹⁶² In the Non-Discrimination Ombudsman’s annual report (2018), a concern was expressed regarding the effects of AI on human rights issues. The issue is that there is no existing guideline regarding the use of AI and therefore there is no clarity on the application of the (relevant) legislation. It is difficult to give out general guidelines that could apply in all situations since anti-discriminatory cases must generally be investigated on a case-by-case basis.¹⁶³

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

The Non-Discrimination Ombudsman has highlighted that, firstly, there may be errors and inadequacies in the teaching data of algorithms. Secondly, forecast variables and sorting criteria of the algorithms may be poorly selected and constructed and thus could be discriminative. Algorithms may also be designed to give meaning to age, language, or gender, which may create a ground for discrimination.¹⁶⁴ In its annual report from 2019, the Non-Discrimination Ombudsman has specifically stressed that the ministries’ and other authorities’ have the legally binding duty and obligation to secure equality in the use of AI by assessing the equality effects of AI already at the planning stage.¹⁶⁵

¹⁶¹ Non-Discrimination Act (21/2004) [Yhdenvertaisuuslaki].

¹⁶² Finnish Government, *Syrjintä Suomessa 2017-2019 - tietoraportti* <https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162517/OM_2020_20.pdf> accessed 12 March 2021.

¹⁶³ Non-Discrimination Ombudsman, ‘Did you know that discrimination related to the use of AI and algorithms is supervised by the Non-Discrimination Ombudsman?’ <<https://syrjinta.fi/se/-/tiesitko-etta-tekoalyn-ja-algoritmeihin-liittyvaa-syrjintaa-valvoo-yhdenvertaisuusvaltuutettu->> accessed 12 March 2021.

¹⁶⁴ Non-Discrimination Ombudsman, ‘Artificial Intelligence and Equality’ <<https://syrjinta.fi/en/artificial-intelligence-and-equality>> accessed 2 April 2021.

¹⁶⁵ Annual report of the Non-Discrimination Ombudsman of 2019, 16.

In order to prevent and detect discrimination arising from AI, the operation of AI must be regularly monitored and tested.¹⁶⁶ Another highly important tool to prevent discrimination is proactive impact assessment and that the development process is transparent and there are tools to evaluate the impact assessment. For example, for the Government's previously mentioned AI program called Aurora, a set of questions was prepared to investigate relevant issues for data protection impact assessment.¹⁶⁷ Finland should legislate guidelines at least on some level, such as the delimitation of the scope of automated decision-making.

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?

As the innovation processes are very dynamic today, the technologies that are now called advanced may seem to be underdeveloped within a few years. Thus, it is difficult to give precise definitions for various concepts of advanced digital technologies in the legislative field. This is the reason why, especially in the EU, the basic premise of regulating advanced digital technologies has been the pursuit of technology neutrality. It means that the legislation does not take a position on the methods by which the rules laid down by law are to be implemented.¹⁶⁸

Regarding big data,¹⁶⁹ the EU has aimed to open public authorities' data resources for general use by adopting several statutes related to open data and the principle of openness within the last decade. Thus, in Finland, the recent national data legislation projects have been based on the implementation of the Open Data Directive.¹⁷⁰ That is also why the Finnish Government's decision-in-principle on improving the availability of digital data in the public sector, the information policy report, and the legislative reform related to the utilisation of data in the transport services, are significant in the field of big data.¹⁷¹

¹⁶⁶ Non-Discrimination Ombudsman, 'The Non-Discrimination Ombudsman's observations on artificial intelligence's effects on equality' (09.02.2021) <<https://syrjinta.fi/-/yhdenvertaisuusvaltuutetun-huomioita-tekoalyn-yhdenvertaisuusvaikutuksista-1>> accessed 2 April 2021.

¹⁶⁷ Digital and Population Data Services Agency, *Aurora-verkon tietosuojaan vaikutustenarviointi* <https://vm.fi/documents/10623/13292513/Aurora_verkon_tietosuoja_vaikutustenarviointi.pdf/0845c1be-364c-aac7-2e9c-fb95fd19aa2a> accessed 2 April 2021, p. 4.

¹⁶⁸ For example, the GDPR, which is closely linked to the application of advanced digital technologies, is intended to apply to data privacy issues regardless of the technology used.

¹⁶⁹ For the definitions, see, for example, the Ministry of Transport and Communications, Publication 20:2014, 6-7.

¹⁷⁰ The Directive on open data and the re-use of public sector information (EU) 2019/1024 aims to harmonise and streamline the regulation and processes for the opening of public sector information resources. Utilisation of open data is also related to traffic.

¹⁷¹ Ministry of Transport and Communications, Valtioneuvoston periaatepäätös julkisen sektorin digitaalisten tietoaisteiden saatavuuden parantamisesta ja uudelleenkäytön edistämisestä 3.3.11, Ministry of Finance, Digitalisaation edistämisen ohjelma. <<https://vm.fi/digitalisaation-edistamisen-ohjelma>> accessed February 19 2021 and Statute development project LVM019/00/2017.

The Open Data Directive is implemented by amending two acts: The Information Management Act¹⁷² and the Act on the Openness of Government Activities.¹⁷³ The purpose of the Information Management Act is to ensure the consistent controlling and secure processing of the data in the public sector in order to implement the principle of openness. It aims to enable the efficient provision of administrative services, as well as to improve the interoperability of information resources.¹⁷⁴ New concepts of Dynamic data and High-value datasets are added to the Information Management Act (Sections 19 and 24(a)-(b)) and to the Act on the Openness of Government Activities (Sections 16 and 34.1). Further, to fully transpose the Directive, two new acts have been drafted: the Act on the Re-use of Data from Certain Public Enterprises and the Act on the Re-use of Publicly Funded Research Materials. The main target of these Acts is to make publicly funded research materials available free of charge in their existing formats and machine-readable form.¹⁷⁵ This legislative measure improves the availability of the data and thus contributes to the openness objectives highlighted by the EU.

Like big data, AI has many applications that are rapidly gaining ground.¹⁷⁶ This trend has been widely monitored at the EU level. On 21 April 2021, the EU Commission presented a proposal for a regulatory framework on AI to ensure that the Europeans can benefit from the newly developed technologies and to address the potentially high risks that AI poses to the safety and fundamental rights equally.¹⁷⁷ Finland's national regulatory field regarding AI will likely change in the next few years with the proposed regulation. Four years before the harmonisation proposal, Finland launched its own Artificial Intelligence Programme.¹⁷⁸ In line with the objectives of the national programme, the Finnish Ministry of Justice is currently developing general legislation to improve automatic administrative decision-making.¹⁷⁹ Particular decision-making procedures are already automated in the authority of the Finnish Tax Administration, the Finnish Immigration Service and the Social Insurance Institution (“Kela”). For example, the Kela issues 2–3 million benefit decisions annually without the benefit handler participating in the decision-making.

Currently, the national legislation reform’s purpose is to expand the automatic processes and to ensure the legality of the administration, the principles of good governance and fair trials, the principle of openness, as well as the realisation of official responsibility in

¹⁷² Act on Information Management in Public Administration (906/2019) [Laki julkisen hallinnon tiedonhallinnasta].

¹⁷³ Act on the Openness of Government Activities (621/1999) [Laki viranomaisten toiminnan julkisuudesta].

¹⁷⁴ Government proposal HE 284/2018 vp.

¹⁷⁵ *ibid.*

¹⁷⁶ For the definitions, see for example Ministry of Finance, *Eettistä tietopolitiikkaa tekoälyn aikakaudella -report*, 5-7.

¹⁷⁷ European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussel 21.4.2021, COM(2021) 206 final 2021/0106 (COD).

¹⁷⁸ Ministry of Economic Affairs and Employment, Publication 2019:23 (Final Report of the AI Programme).

¹⁷⁹ Finnish Government’s analysis, assessment and research, Publication 2019:44, pp. 21-22. Here, automatic (or algorithmic) decision making refers to a decision based on a machine learning algorithm or a rule-based system. In contrast, AI often refers to combinations of methods and systems that can perform tasks that require human intelligence, such as visual recognition, speech recognition, or logical reasoning.

automatic decision-making.¹⁸⁰ On 18 January 2021, a working group was set up to prepare regulations on the use of automation for handling administrative matters, and to consider, whether from the perspective of fundamental rights and legal protection, it would be appropriate to extend the regulation to the use of automation in actual administrative activities.¹⁸¹

Like other technology concepts, the Internet of Things (IoT) is also an indefinite construction. According to the Research Report 23/2019 of the Finnish Transport and Communications Agency (Traficom), IoT refers to objects equipped with technology and AI which operate and communicate autonomously among themselves.¹⁸² In the public sector, the concept of IoT has a reasonably strong relation to the automation of traffic systems. In the future, vehicles operating on autopilot will act as terminals in 5G networks and share great amounts of data in order to move smoothly and safely in various traffic systems.¹⁸³ Different forms of Mobility as a Service (“MaaS”) are also becoming more common. These are some of the reasons why, about a decade ago, the European Parliament and the Council adopted the Intelligent Transport System Directive (ITS).¹⁸⁴ The priority of the Directive is to accelerate the coordinated deployment and the use of intelligent transport systems in road transport across Europe.

In 2019, as in reflecting the EU’s objectives, the Finnish Ministry of Transport and Communications launched a project to prepare the national transport automation action and legislation plan covering all modes of transport in Finland.¹⁸⁵ The external legislative developments in the area of transportation are highlighted in the national plan. It is stated in the plan that the United Nations Economic Commission for Europe’s (UNECE) international regulations have a critical impact on Finnish road automation, the International Maritime Organisation’s agreements are crucial for the development of automation in water transport, and the most significant legislative project in rail automation is the EU Commission’s and European Railway Agency’s project, the 2022 revision of the CCS TSI.¹⁸⁶ Further, according to the plan, at the core of the development of unmanned aerial vehicles is the preparation of harmonised EU regulations such as the U-space system called the Single European Sky.¹⁸⁷ The plan sets out three national objectives: 1) developing transport automation with a focus on the interests of individuals and societies; 2) significantly enhancing the exchange of transport-related information, and 3) developing a comprehensive regulatory framework for transport automation. According to the plan, future legislation will allow people to break away from vehicle-related monitoring and do

¹⁸⁰ Statute drafting OM021:00/2020.

¹⁸¹ Ibid. and Ministry of Justice, Reports and opinions 2020:21.

¹⁸² Traficom, Research Reports 23/2019, 12.

¹⁸³ Ministry of Transport and Communications, Publication 10/2017, 4.

¹⁸⁴ Directive (EU) 2010/40 on the deployment of Intelligent Transport Systems (ITS) in the field of road transport and on the framework for interfaces between road transport and other modes of transport.

¹⁸⁵ Statutory development project LVM059:00/2019.

¹⁸⁶ Ibid 10.

¹⁸⁷ Ibid 11.

completely different things while staying in an autonomous vehicle.¹⁸⁸ Some of the objectives have already been implemented in the Act on Transport Services (320/2017).¹⁸⁹

Finally, in the area of encryption, the recent national developments relating to the former Finnish Government Programme's key project concerning the creation of a digital growth environment. As part of this project, the national information security strategy was drawn up.¹⁹⁰ With the legislative and developmental projects outlined in the previous sections focusing mainly on the operations of the public sector, this strategy widely impacts the private sector as well.¹⁹¹ As part of the strategy, legislative changes required by the EU Network and Information Security Directive (NIS)¹⁹² were implemented by making changes to the existing sectoral legislation. The authorities responsible for the security of network and information systems in accordance with the NIS Directive are those who are otherwise responsible for supervising the security obligations of the industry, i.e. the so-called sector-specific supervisory authorities.¹⁹³

To sum up, as a result of several harmonisation projects, Finland has followed the principle of technology neutrality when drafting national legislation in the field of advanced digital technologies. Thus, so far, there are no specific Acts in the Finnish system that explicitly would define concepts of big data, AI, IoT or encryption. These terms remain abstract and acquire their legal interpretation through complex national sectoral legislation. However, the situation may change in some respects soon as the EU's proposal for the legal framework on AI is taken forward¹⁹⁴. Because of the wide harmonisation, the measures taken by the EU in areas other than just AI regulation are relevant when the national legislative questions related to advanced digital technologies are concerned. These areas include, for example, digitalisation projects, open data systems, algorithmic decision-making processes, and smart transportation networks.

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

Section 10(2) in the Constitution of Finland protects the secrecy of confidential messages by stating that '[t]he secrecy of correspondence, telephony and other confidential communications is inviolable'. This section protects confidential communications in a technologically neutral manner.¹⁹⁵ Moreover, section 10(4) clarifies some important

¹⁸⁸ Ministry of Transport, *the national transport automation action and legislation plan*, 8-9.

¹⁸⁹ See especially Chapter 18 regarding the interoperability of information systems. For example, Section 156, which is directly related to MaaS, has raised several GDPR-related questions concerning the implementation of acting on someone else's behalf.

¹⁹⁰ Ministry of Transport and Communications, Publication 7/2016.

¹⁹¹ Ministry of Transport and Communications, Publication 2/2018.

¹⁹² Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS).

¹⁹³ Government proposal HE 192/2017 vp., Publications of the Ministry of Transport and Communications 9/2017 and Network and information security directive – Working group's final report to support national implementation.

¹⁹⁴ See Commission's Proposal for a Regulation laying down harmonised rules on artificial intelligence, COM(2021) 206.

¹⁹⁵ Government proposal HE 309/1993 vp. 53.

exceptions to the main rule and allows the possibility of decrypting personal messages in certain circumstances under Finnish law, e.g. when investigating a crime. This, however, poses a threat to the right to privacy and confidential messages and also the right to a fair trial.

Furthermore, covert coercive measures, under which personal messages may be decrypted,¹⁹⁶ have been regulated precisely in order to balance, on one hand, the effectiveness of criminal investigations and, on the other hand, the two above mentioned human rights. The Finnish laws do not define implicitly the concept of decryption. However, e.g. telecommunication interception reveals the content of a personal message. Conditions for the use of this coercive measure are further clarified in the Police Act ((PA) in Finnish “Poliisilaki” 872/2011), Coercive Measures Act ((CMA) in Finnish “Pakkokeinolaki” 806/2011).¹⁹⁷

All of the above-mentioned laws have a similar rule for assessing prerequisites for covert coercive measures that might lead to the decryption of messages. Firstly, general prerequisites must be met. The CMA provides general prerequisites for the use of covert coercive measures. These general prerequisites consist of two components: the use of covert coercive measure must 1) produce information *needed to clarify* an offence, and 2) be used only if they can be assumed to have *particularly important significance* in clarifying the offence. The use of covert coercive measures must be terminated earlier than originally supposed to if 1) the purpose for which they are used has been achieved, or 2) the prerequisites no longer exist.¹⁹⁸ Secondly, the special prerequisites clarify more thoroughly which exact criminal offences must be suspected for the specific coercive activity.¹⁹⁹ Naturally, the earlier the police are allowed to decrypt a message, the more serious the suspected crime has to be.

Key decryption decodes the encrypted message through a key or a password. This especially poses a threat to privacy since revealing the key allows access to a wide amount of data. The Finnish law allows decryption generally in case of using covert coercive measures, which means that it may be conducted even by key disclosure: in accordance with CMA Chapter 8 (section 23), passwords and other corresponding information necessary to conduct a search of data must be provided to a criminal investigation authority at its request. Even though the Finnish law does not specify different encryption

¹⁹⁶ Coercive measures in this context, that allow the police to find out the content of a confidential message, are: telecommunications interception, obtaining of information other than through telecommunications interception, traffic data monitoring, traffic data monitoring with the consent of the possessor of a network address or terminal end device, obtaining base station data.

¹⁹⁷ See also Criminal Investigations Act (CIA in Finnish “esitutkintalaki” (805/2011)). There can be three different situations under which the authorities may decrypt a personal message: for 1) civil investigation (regulated under the PA (Chapter 5a)), and in order to 2) prevent (regulated under the PA (Chapter 5)) and 3) detect a crime that has actually happened. This Report mainly concerns the last category since the question refers to criminal investigations and thus to a crime that has already happened.

¹⁹⁸ The CMA (Chapter 10, section 10(3)). This section can be compared to the corresponding section 2(3) (Chapter 5) of the PA.

¹⁹⁹ For example, the prerequisites for telecommunications interception are stated in the CMA (Chapter 10, section 3).

methods in more detail, the authorities are bound to follow principles set out in CMA Chapter 1.²⁰⁰

Even though the police request to use the coercive measures, it is generally a District Court that grants the permission to use such measures.²⁰¹ Thus, the competencies are decentralised. However, in reality, this arrangement does not always ensure the lawfulness of the procedure. For example, the Parliamentary Ombudsman issued a remark to a district judge because the judge had granted the police a warrant to conduct the telecommunications interception without a sufficient legal basis.²⁰² So, even the decisions made by the Courts might allow an illegal and unnecessary interference with the right to privacy.

The existence of legal remedies is a key way of achieving legal protection. Because the suspect is not aware of being targeted for the secret coercive measures, they must be given special protection in case secret coercive measures are used without a legal basis. This is done firstly by giving him or her the right to lodge an extraordinary appeal of the warrant issued by a court.²⁰³ Secondly, the suspected person has a right to be informed of the coercive measure by a written notice afterwards.²⁰⁴ In reality, the media has criticised, due to a few reported cases, that the police's obligation to find out and verify the identity of the persons, who have been subject to covert coercive measures, has been interpreted narrowly. This leads to the fact that the coerced person has not been informed of the use of coercive measures, and as a result, the suspect cannot question the lawfulness of the coercive measure before the court.²⁰⁵ So, although the suspect has the right to be informed under the law, it seems that this right is not being realised *de facto*, which seems alarming in the light of the suspect's right to privacy and right to a fair trial. Thirdly, it is in the suspect's favour that the information is destroyed when it is no longer needed for the purpose of investigating a crime.²⁰⁶ Finally, it is in favour of the individuals that the lawfulness of the

²⁰⁰ Such principles include proportionality (section 2) and minimum intervention (section 3).

²⁰¹ Government proposal HE 224/2010 vp. 51–53 and Government proposal HE 220/2010 vp. 136–137. The Court decides on the telecommunication interceptions and on obtaining the request of an official with the power to arrest in accordance with the CMA (Chapter 10, section 5(1)).

²⁰² The purpose of the police was to prevent a felony against life or health but, however, it did not fulfil the special prerequisites since it was not one of the crimes listed in the PA. See the Parliamentary Ombudsman's decision EOAK/7688/2020 on 13 January 2021, available in Finnish at <www.oikeusasiamies.fi/r/fi/ratkaisut/-/eoak/7688/2020> accessed 18 February 2021.

²⁰³ The CMA, (Chapter 10) section 43(5). In addition, the section provides that the extraordinary appeals shall be considered urgently.

²⁰⁴ The CMA, (Chapter 10) section 60(1) provides that the suspected person must have the right to be informed after the matter has been submitted to the prosecutor or the criminal investigation has otherwise been terminated or interrupted, at the latest within one year of the termination of the use of a coercive measure.

²⁰⁵ See Susanna Reinboth, 'Telepakkokeinoilla puututaan yksityiselämän suojaan – niiden käytön hämäristä perusteluista on ruoskittu niin poliisia kuin tuomareitakin' (14 January 2017). Translation of the headline in English would be 'Coercive measures interfere with the right to privacy – both the police and judges have been flogged for vague justifications for their use' (*Helsingin Sanomat* 14.01.2017) <www.hs.fi/kotimaa/art-2000005045743.html> accessed 16 February 2021.

²⁰⁶ However, the CMA, (Chapter 10) Section 57 provides a prolonged time up to 5 years under specific circumstances.

official acts and actions of the authorities is supervised by the Chancellor of Justice and the Parliamentary Ombudsman.

In conclusion, it seems that the relevant human rights, right to privacy and right to a fair trial, have been taken into account in the legislation, but in reality, the suspected person is not always informed about the decryption of their messages, which invades both the right to privacy and the possibility to question the legality of the decryption of personal messages before the court.

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

Finland has a history of being a frontrunner in shaping information society policies, and the position has been strengthened after Finland adopted broader regimes of European law, namely the ECHR.²⁰⁷ However, Finland does not have any specific national legislation on human rights issues that arise from the use of advanced digital technologies.

According to the digital skills survey, Finns are generally competent in using digital devices and services.²⁰⁸ Additionally, Digibarometer shows that Finland is among the top three. Finland's success can be explained by its even performance across numerous indicators and the country's capabilities to utilise digitalisation.²⁰⁹ However, the survey raises the concern that certain groups of the population and companies cannot keep up with the increasingly digitalised world. The implementation of data protection, and the possibilities of the disabled and the elderly people to use the services, are the major challenges. One of the issues is that individuals may not have the necessary skills to operate online. Another issue is the difficulty to understand the language used by the public authorities.

Finland aims to be a digitally equal country where everyone has the same opportunities to express themselves online. While the aim is well-thought, digitalisation has been previously seen as a somewhat scary concept.²¹⁰ This idea is still strongly present in the debates, which has led some individuals to become reluctant to adopt the skills needed for digital services, arguing that they will rather manage it in a traditional manner, i.e. using physical face-to-face options. On the other hand, digitalisation has been deemed to increase economic inequalities since low-income citizens are less likely to have resources, such as devices or their own internet connection to use. Fortunately, many public places in Finland, such as libraries and schools, provide access to computers and other digital services for free.

²⁰⁷ Marko Ala-Fossi, Anette Alén-Savikko, Jockum Hilden, Minna Aslama Horowitz, Johanna Jääsaari, Kari Karppinen, Katja Lehtisaari, and Hannu Nieminen, 'Operationalising communication rights: the case of a "digitalwelfare state"', *Internet Policy Review*, 8(1) (2019) 4.

²⁰⁸ Ministry of Finance & Digital and Population Data Services Agency, *Digitaitokartoitus – Digitaalinen kysely* (2020).

²⁰⁹ ETLA, 'Summary of Cybersecurity in Finland' (2020)

<<https://www.etla.fi/julkaisut/digibarometri-2020-kyberturvan-tilannekuva-suomessa/>> accessed 24 May 2021

²¹⁰ Ministry of Finance, *Digitaalinen Suomi – Yhdenvertainen kaikille: Digi Arkeen -neuvottelukunnan Toimintakertomus*, Publication 2019:23, 13.

An amendment to the current Act on the Provision of Digital Services²¹¹ has been prepared regarding the accessibility of services.²¹² The purpose is to make sure that the diversity of people and their needs are taken into account. The issues can come down especially on linguistic rights, which are guaranteed under the Finnish Language Act.²¹³ However, the current legislation does not cover the use of 'plain language' which would be beneficial especially for immigrants, people with cognitive challenges or individuals with hearing or sight impairments.²¹⁴ High-quality investments, such as disability-friendly software systems or translation applications, are needed to solve these issues.

A report on Europeans' attitudes towards Cybersecurity shows that the Finns feel fairly well-informed about the risks of cybercrimes.²¹⁵ They also seem to trust the authorities with their online data more than the other European countries, despite the recent data breach cases.²¹⁶ One example is the Vastaamo-case, which was described in section 4.3 of this report. However, Finland faces threats to the right to privacy and freedom of speech.²¹⁷ Social media platforms are mostly monitored by private companies, who decide the limits of appropriate speech. It is arguable whether those limits are sufficient, since there has been, for example, an increase in online hate speech. This affects people's willingness to participate in public debates²¹⁸, and therefore impacts actualisation of democracy.

The topic of privacy brings together the changes caused by digitalisation. While Finland has a long-standing history of guaranteeing the right to privacy, there is an underlying concern that the state's interests might coincide with the economic interests of different corporations.²¹⁹ The EU has big plans for Data Economies, which could benefit from the flexible flow of data between organisations, and hence weakening the current data protection legislation. Open data, which can be transferred easily between organisations, offers important opportunities for the national economy and future innovations. However, lack of confidence towards new digital technologies makes it difficult to utilise their use effectively. Firstly, regulation methods provided by the government do not create an environment where concrete ICT-opportunities could thrive. The Finnish government's readiness to utilise big data - the matter which consists of large amounts of data from

²¹¹ Act on the Provision of Digital Services (306/2019) [Laki digitaalisten palvelujen tarjoamisesta] and the Act on Electronic Services and Communication in the Public Sector (307/2019) [Sähköisen viestinnän palvelulaki].

²¹² Government proposal HE 60/2018 vp.

²¹³ Language Act (423/2003) [Kielilaki].

²¹⁴ Ministry of Finance, Digitaalinen Suomi – Yhdenvertainen kaikille: Digi Arkeen - neuvottelukunnan Toimintakertomus, Publication 2019:23, 27-28.

²¹⁵ The European Commission, Europeans' attitudes towards cyber security (Special Eurobarometer No. 464a), Publications Office of the European Union (2017) 58-60.

²¹⁶ See Vastaamo- case at Section 4.3 of this Report.

²¹⁷ Anna Björk, 'Finland in the International Human Rights System', Publications of the Government's Analysis and Research Activities 2019:50.

²¹⁸ Aleksi Knuutila et al, 'The Impact of Hate Speech on Public Decision-making', Publications of the Government's Analysis and Research Activities 2019:57.

²¹⁹ Marko Ala-Fossi, Anette Alén-Savikko, Jockum Hilden, Minna Aslama Horowitz, Johanna Jääsaari, Kari Karppinen, Katja Lehtisaari and Hannu Nieminen, 'Operationalising communication rights: the case of a "digitalwelfare state"' Internet Policy Review 8(1) (2019). See also Lex Nokia (repealed in 2015).

various sensors and digital services - has been low.²²⁰ Furthermore, there are shortcomings with Finnish cybersecurity and data protection legislation, although the latter is mostly due to GDPR and European regulation. A few Finnish companies received their first administrative fines under Article 89 of the GDPR in spring 2020 that were imposed on the cases concerning the failure to inform the data subjects of their data protection rights.²²¹ This shows that companies are struggling to balance legislation changes and the fast technological developments.

Ethical issues, such as the implementation of privacy protection and the transparency of algorithm decision-making, have come to the forefront of the AI debate. However, the National Artificial Intelligent Report does little to address individual rights.²²² On the other hand, the Finnish Government has high hopes that AI could be used to combat online hate speech, which has increased massively on social media platforms, affecting how people express themselves.²²³ The aim is to get insights on how the platforms could monitor and delete inappropriate messages more effectively. The criteria for hate speech is given by those handling the AI system, meaning that artificial intelligence does not decide which consists of inappropriate content.²²⁴ However, we need to be aware that individual views and opinions can impact the criteria.

Digital technologies have offered new opportunities in public participation, such as electronic participation (e-participation), where citizens can submit their initiatives to the Finnish Parliament. Despite this, the country reports indicate that there are weaknesses in Finland's participatory competencies.²²⁵ One of the issues is that the digital dimension is not open enough for diverse debates since people's opinions are being silenced by the majorities. Additionally, elderly people do find new systems more intimidating.

In conclusion, Finland's status as a "digital welfare state" falls short²²⁶ as the policies concerning the governance of the objectives discussed in these sections focus more on the economic goals than the actual promotion of these rights. Other sections of this report have shown that digital developments raise concerns with protection of privacy, fair judicial processes and, for example, cybersecurity. Experts suggest that more research is needed on the human rights issues in the digital dimension.²²⁷ Due to Finland's Chairship in the

²²⁰ Risk Analysis of the National Audit office of Finland (2015)

²²¹ Borenus, 'Lessons to be learned from the First Administrative Fines Imposed by the Data Protection Ombudsman – Documentation is the Key' June 2 2020
<www.borenus.com/2020/06/02/lessons-to-be-learned-from-the-first-administrative-fines-imposed-by-the-data-protection-ombudsman-documentation-is-key/> accessed 23 February 2021.

²²² Ministry of Economic Affairs and Employment, *Edelläkävijänä tekoälyaikaan: Tekoälyohjelman loppuraportti* 2019:23, p. 35.

²²³ Laura Kettunen, 'Utilisation of Artificial Intelligence in monitoring hate speech', Publications of the Ministry of Justice, Reports and Guidelines 2021:15.

²²⁴ Ibid, 28.

²²⁵ Ministry of Justice, the National Action Plan 2017-2019 (2017).

²²⁶ Marko Ala-Fossi, Anette Alén-Savikko, Jockum Hilden, Minna Aslama Horowitz, Johanna Jääsaari, Kari Karppinen, Katja Lehtisaari and Hannu Nieminen, 'Operationalising communication rights: the case of a "digitalwelfare state"'. Internet Policy Review 8(1)(2019) 10.

²²⁷ Assi Harkoma, 'Perus- ja Ihmisoikeustutkimuksesta Suomessa - asiantuntijoiden näkemyksiä', Ihmisoikeuskeskus (2017).

Freedom Online Coalition (FOC) this year, Finland has the opportunity to not only advocate for an open and safe internet but also show that it can be the leader to achieve an ethical digitalisation environment.²²⁸

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?

It is a well-known fact that technology develops faster than the legislation governing it. The areas that are not governed by written laws are governed by soft law instruments and self-regulation. When new laws are passed, covering new areas that were previously covered by soft law instruments, the scope of soft law diminishes and the scope of regulated laws grows. We believe that the scope of the legislation will grow and take over the issues currently covered by lesser instruments.

Future developments can be expected in two fields. Firstly, Finland is an EU member state, which means that legal developments in the EU will ultimately affect the Finnish legislation. Secondly, developments on the national level will likely occur in areas that are not covered by the EU legislation. Both areas must be inspected to understand the legal developments in the future.

10.1 The future developments in the EU

The EU has adopted a digital strategy to enhance people's rights and control over their data. As part of the European Digital Strategy, the European Commission has introduced two new proposals – the Digital Markets Act (DMA) and the Digital Services Act (DSA).²²⁹

The DMA is meant to set the rules for so-called “gatekeepers”. The gatekeepers are defined as companies that have a significant impact on the market and are present in several EU countries. Companies, such as Google, Facebook and Twitter would all qualify as gatekeepers. This would make a major difference to the Finnish legislation since currently, companies of various sizes need to abide by the same rules. The DMA would change this premise as the gatekeepers would be targeted with more restrictions and rules.²³⁰

The premise of the DMA seems to be promising. The gatekeepers strongly affect the daily life of normal people. The DMA protects human rights by restricting the undue influence of the gatekeepers. This creates fairer competition, which protects the right to work, a human right recognized under Article 23 of the Universal Declaration of Human Rights.

²²⁸ Ministry for Foreign Affairs of Finland, ‘Finland to lead the Freedom Online Coalition in 2021’ <https://um.fi/current-affairs/-/asset_publisher/gc654PySnjTX/content/suomi-internetvapausi-c3-a4riest-c3-b6n-johtoon-vuodelle-2021> accessed 1 May 2021.

²²⁹ European Commission, A Europe fit for the digital age - Empowering people with a new generation of technologies. <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en> accessed 12 March 2021.

²³⁰ European Commission, The Digital Markets Act: ensuring fair and open digital markets <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en> accessed 12 March 2021.

The most important takeaway of this Act is the way it is specifically aimed at the gatekeepers. Now that the floodgates are open, there is a possibility that the legislation would be specifically aimed at the gatekeepers in the future. The DSA also contains specific obligations for large platformers to manage certain risks and to enhance the fundamental rights of individuals online.²³¹ These plans were made before Twitter banned Donald Trump, the former president of the United States of America, from using the platform. The incident has reminded people of the power that social media platforms control over public discussion and will likely result in legislative changes in the future.²³²

10.2. National developments in the Future

As noted in Chapter 3 of this Report, Finland has one of the strictest data protection regulations within the EU member states. The Finnish approach emphasises individual freedom, so it is unlikely that the approach on preferring legislation over self-regulation will change. The recent data breach case of Vastaamo²³³ makes this even more unlikely.

The new laws will likely be enacted in the future to address the areas that are not covered by the Finnish legislation yet. However, these laws would likely be targeted on specific issues. For example, there are currently multiple drafts aiming to address specific data protection issues.²³⁴ The approach of filling gaps with specific laws is likely to prevail in Finland.

Conclusion

This Report has covered an extensive range of topics regarding the status between technologies and human rights in the legislative context of Finland and the EU. Especially questions arising from the scopes of the right to privacy, the right to data protection, the right to good governance, the right to an effective remedy and a fair trial, and the right to equality and non-discrimination have been explored.

The EU legislation and the ECHR have built the ground for ensuring human rights and data protection in Finland. The GDPR aims to ensure the rights and freedoms of data subjects when their data is being processed. It is complemented by national laws, and a few *lex specialis* address the processing operations at specific sectors and by public authorities. This report finds that the Finnish system relies heavily on the active initiative taken by the data subjects who seek to exercise their rights under the GDPR. Furthermore, it has been argued that as the Finnish DPA may not impose administrative fines on public authorities and bodies like its Scandinavian peers, for example on the unlawful use of camera

²³¹ European Commission, The Digital Services Act: ensuring a safe and accountable online environment<https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en> accessed 12 March 2021.

²³² Euractiv, Twitter's 'problematic' Trump ban troubles Europe (*Euractiv* 12 January 2021) <www.euractiv.com/section/global-europe/news/twitters-problematic-trump-ban-troubles-europe/> accessed 12 March 2021.

²³³ Description of the case is found in Chapter 4.3 of this Report.

²³⁴ Finlex, current drafts listed by ministry.<www.finlex.fi/fi/esitykset/he/vireilla/> accessed March 8 2021.

surveillance and facial recognition²³⁵, the rights and freedoms of the data subjects might be in jeopardy since typically they cannot decide if their data have been processed for the public purposes.²³⁶

In terms of the use of the ADT, no specific national legislation addresses human rights regarding this field in Finland. A legal framework providing a procedure for human rights impact assessments is yet to be enacted. Several norms and processes seek to ensure the protection of human rights. Moreover, the need to reform the legislation has been identified.

The EU strives for technology neutrality in legislation allowing new interpretations as the technology evolves, and thus also actions need to be taken when the indications of new threats to human rights arise. It follows from this approach that currently there are no specific acts explicitly defining the concepts of big data, AI, IoT or encryption in Finland. However, to address the risks arising from AI, the EU Commission adopted a proposal for a legal framework on AI on 21 April 2021.²³⁷ This very first AI Regulation proposal broadly defines the AI systems, introduces a preferred policy option with a proportionate risk-based approach on high-risk AI systems, and a voluntary code of conduct approach for other AI systems. It seeks to prohibit AI practices that would violate EU values and fundamental rights.²³⁸

The EU has adopted a digital strategy to deploy digitalisation to serve people and businesses. At the national level, the Finnish Government Programme for the Promotion of Digitalisation sets the national goal for providing digitally accessible public services by 2023 and thus seeks to ensure equality for citizens and to support the cooperation between the public and private sectors.²³⁹ The cooperation between the private and public sectors as being promoted in several governmental projects facilitates user-friendly and secure digital services and promotes the use of the best practices in order to safeguard the data protection for data subjects.²⁴⁰

²³⁵ DT 26 February 2020, DT-19/01478-6/KBK, para 5.3, 6: The Norwegian DPA fined Rælingen municipality for the use of school app Showbie in the breach of several violations when processing special categories of data; IMY 20 August 2019, DI-2019-2221: The School in Skellefteå used camera surveillance for monitoring the attendance of the students without conducting a DPIA or seeking prior consultation; IMY 10 February 2021, DI-2020-2719, A126.614/2020, p. 4-5: The Swedish DPA fined the police for the unlawful use of facial recognition; IMY 13 November 2020, DI-2019-7024, p. 2-3: The Swedish DPA fined the City of Stockholm for the lack of technical and organizational measures to protect personal data on a school platform.

²³⁶ See more in Chapter 5.2; Opinion of the Office of the Data Protection Ombudsman in the Government proposal HE 9/2018 vp. Government's proposal to Parliament for legislation supplementing the GDPR, on 15 March 2018 <www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-177690.pdf> accessed 17 May 2021.

²³⁷ European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussel 21.4.2021, COM(2021) 206 final 2021/0106 (COD).

²³⁸ *ibid.*, pp. 9, 11-12, 17, Art. 3, 5-6.

²³⁹ Ministry of Finance, Digitalisaation edistämisen ohjelman asettamispäätös 25.2.2020 <<https://vm.fi/digitalisaation-edistamisen-ohjelma>> accessed 29 May 2021, pp. 1-2.

²⁴⁰ See more about this in Chapter 3.

Finland was among the first countries to provide affordable broadband access as a legal right²⁴¹ and the think tank Center for Data Innovation, regarding Finland, was the best in the EU to make available official information to its citizens.²⁴² The Finnish digital public services and the level of digital knowledge in the country are ranked to be the best in the EU.²⁴³ Furthermore, the freedom of the press²⁴⁴ has had an important role in facilitating the public discussion when a potential violation of fundamental rights has been identified, such as following the obligations related to the use of coercive measures in criminal investigations in order to ensure the right to privacy and the right to a fair trial.²⁴⁵

The Finns are among the most frequent users of the internet in the EU and their trust towards the public authorities' ability to keep their data safe is the highest within the EU Member States.²⁴⁶ This Report indicates the challenges arising from the automated decision-making procedures by the public authorities. The need for regulatory reform has been identified in this respect, especially from the point of view of delimiting the scope of automated decision-making, ensuring good administration, and safeguarding legal certainty.²⁴⁷

In general, while comparing on the international level, data protection and the protection of fundamental rights is at a very high level in Finland.²⁴⁸ Even though this Report has also identified challenges in this respect, Finland has taken an active role in solving them and seeks to redeem the expectations arising from the trust of the Finnish citizens upon the actions of the authorities.

²⁴¹ Hannu Nieminen, 'European broadband regulation: The "broadband for all 2015" strategy in Finland' in Maria Löblich and Senta Pfaff- Rüdiger (eds.), *Communication and media policy in the era of the internet: Theories and processes* (Nomos 2013) 119-133.

²⁴² Nick Wallace and Daniel Castro, The state of data innovation in the EU, Center for Data Innovation (October 2017) 13.

²⁴³ European Commission, The Digital Economy and Society Index (DESI) <<https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi>> accessed 17 May 2021.

²⁴⁴ Reporters without Borders, 2021 World Press Freedom Index <<https://rsf.org/en/ranking>> accessed 17 May 2021.

²⁴⁵ See the example given in Chapter 8.

²⁴⁶ European Commission, 'Europeans' attitudes towards cyber security' (Special Eurobarometer No. 464a), Publications Office of the European Union (2017) 58-60.

²⁴⁷ Niklas Vainio, Kari Hämäläinen and Ella Rautiola, Arviomuistio hallinnon automaattiseen päätöksentekoon liittyvät yleislainsäädännön sääntelytarpeista, Ministry of Justice Publications 2020:21, p. 8.

²⁴⁸ World of Justice Project, Rule of Law Index <<https://worldjusticeproject.org/rule-of-law-index/>> accessed 19 May 2021. In 2020, Finland was ranked as the 3rd in the world on the Rule of Law Index.

Table of legislation

Provision in [native] language	Corresponding translation in English
Perustuslain (731/199) 10 §: Yksityiselämän suoja Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.	Section 10 in the constitution of Finland: The right to privacy Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act. The secrecy of correspondence, telephony and other confidential communications is inviolable. Measures encroaching on the sanctity of the home which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime may be laid down by an Act. Limitations of the secrecy of communications may be imposed by an Act if they are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, during deprivation of liberty, and for the purpose of obtaining information on military activities or other such activities that pose a serious threat to national security.
Poliisilain 5 luvun 2 §: Salaisten tiedonhankintakeinojen käytön edellytykset Salaisen tiedonhankintakeinon käytön yleisenä edellytyksenä on, että sillä voidaan olettaa saatavan rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi tarvittavia tietoja.	Police Act Chapter 5, Section 2: Preconditions for use of secret methods of gathering intelligence The general precondition for the use of secret methods of gathering intelligence is that this can be assumed to result in gaining information necessary for preventing, detecting or averting the threat of an offence.

Sen lisäksi, mitä salaisten tiedonhankintakeinojen käytön erityisistä edellytyksistä jäljempänä säädetään, telekuuntelua, tietojen hankkimista telekuuntelun sijasta, suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, henkilön teknistä seurantaa, teknistä laitetarkkailua, peitetoimintaa, valeostoa, tietolähteen ohjattua käyttöä ja valvottua läpilaskua saadaan käyttää vain, jos niillä voidaan olettaa olevan erittäin tärkeä merkitys rikoksen estämiselle tai paljastamiselle. Peitetoiminnan ja valeoston käyttäminen edellyttää lisäksi, että se on välttämätöntä rikoksen estämiseksi tai paljastamiseksi. Salaisen tiedonhankintakeinon käyttö on lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole.	In addition to the provisions below on the special preconditions for the use of secret intelligence gathering methods, telecommunications interception, obtaining data other than through telecommunications interception, extended surveillance, on-site interception, technical observation, technical tracking of a person, technical surveillance of a device, undercover activities, pseudo purchases, controlled use of human intelligence sources and controlled deliveries may be used only if they can be assumed to be of very great significance for the prevention or detection of an offence. Use of undercover activities or pseudo purchases also requires that this be essential for the purpose of preventing or detecting an offence. Use of a secret intelligence gathering method shall be discontinued before the end of the fixed period stated in the decision if the purpose of its use has been met or if the preconditions for it no longer exist.

Bibliography

English titles

Legislation

UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III)

Commission, 'Proposal for a Regulation 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' COM (2012) 11 final

Commission, 'Proposal for a Regulation laying down harmonised rules on artificial intelligence. Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM (2021) 206 Final

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5

Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108

Charter of Fundamental Rights of the European Union [2012] OJ C326/391

Consolidated version of the Treaty on European Union [2012] OJ C326/13

Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47

Directive (EC) 95/46 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

Directive (EU) 2010/40 of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport Text with EEA relevance.

Interinstitutional agreement on better law-making [2003] OJ C321

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information

Convention for the protection of individuals with regard to automatic processing of personal data (SopS 35/92 and 36/92)

Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussel 21.4.2021, COM(2021) 206 final 2021/0106 (COD)

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

Article 29 Working Party Opinion 4/2007 on the concept of personal data (Adopted on 20 June 2007)

Article 29 Working Party Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679 (Adopted 3 October 2017)

Commission, Digital Government Factsheet 2019: Finland

Cyber Security for Consumer Internet of Things: Baseline Requirements ETSI EN 303 645 V2.1.0 (4/2020)

European Commission, Europeans' attitudes towards cyber security (Special Eurobarometer No. 464a) Publications Office of the European Union (2017)

Wallace N and Castro D, The state of data innovation in the EU, Center for Data Innovation (October 2017)

Network and information security directive – Working group's final report to support national implementation

Books

Kleinstauber H, 'The Internet between Regulation and Governance' in Christian Möller and Arnaud Amouroux (eds), *The Media Freedom Internet Cookbook* (OSCE Representative on Freedom of the Media 2004)

Nieminen H, (Löblich M and Pfaff-Rüdiger S (eds.)) *Communication and media policy in the era of the internet: Theories and processes* (Nomos 2013)

Periodicals

Boddewyn JJ, 'Advertising Self-Regulation' (1985) *Journal of Public Policy & Marketing* Vol. 4 131

Castro D, Benefits and Limitations of Industry Self-regulation for Online Behavioral Advertising, , The Information Technology and Innovation Foundation (2011)

The European Commission, Europeans' attitudes towards cyber security (Special Eurobarometer No. 464a) (2017) Publications Office of the European Union

Tikkunen-Piri C, Rohunen A and Makkula J, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' (2018) 34 *Computer Law and Security Review* 134

Digital resources

Cybersecurity, 'What is the Finnish Cybersecurity Label?' <<https://tietoturvamerkki.fi/en/>> accessed 14 March 2021

DLA Piper's Data Protection Laws of the World Handbook (updated 12 January 2021)
Available online <<https://www.dlapiperdataprotection.com/index.html?t=about&c=FI>>
accessed 8 March 2021

European Commission, A Europe fit for the digital age - Empowering people with a new generation of technologies
<https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en>
accessed 12 March 2021

European Commission, The Digital Services Act: ensuring a safe and accountable online environment
<https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en> accessed 12 March 2021

European Commission, The Digital Economy and Society Index (DESI)
<<https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi>>
accessed 17 May 2021

Euractive, 'Twitter's 'problematic' Trump ban troubles Europe' (12 January 2021)
<<https://www.euractiv.com/section/global-europe/news/twitters-problematic-trump-ban-troubles-europe/>> accessed 12 March 2021

Office of the Finnish Data Protection Ombudsman, 'The Deputy Data Protection Ombudsman has ordered Vastaamo to notify personally its customers who have become victims of the personal data breach' [press release 23 October 2020]
<<https://tietosuoja.fi/-/apulaistietosuojavaaltuutettu-maarasi-psykoterapiakeskus-vastaamon-ilmoittamaan-tietomurron-kohteeksi-joutuneille-asiakkailleen-henkilokohtaisesti>>
accessed 18 February 2021

Office of the Finnish Data Protection Ombudsman, 'The Office of the Data Protection Ombudsman safeguards your data protection rights'
<<https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman>> accessed 8 March 2021

Reporters without Borders, 2021 World Press Freedom Index
<<https://rsf.org/en/ranking>> accessed 17 May 2021

Republic of Estonia: Information System Authority, 'PRC: Finland's and Estonia's data exchange layers connected to one another on 7 February - the rapid exchange of information between the countries is now possible'
<www.ria.ee/en/news/prc-finlands-and-estonias-data-exchange-layers-connected.html>
accessed 14 March 2021

Sittnikow C, 'First Four Administrative Fines issued for non-compliance with the GDPR in Finland' (Waselius & Wist Legal Updates, 4 June 2020)
<www.ww.fi/news/2020/06/first-four-administrative-fines-issued-for-non-compliance-with-the-gdpr-in-finland/#content> accessed 28 April 2021

Traficom, 'Finland becomes the first European country to certify safe smart devices - new Cybersecurity label helps consumers buy safer products' <www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label> accessed 14 March 2021

World of Justice Project, Rule of Law Index <<https://worldjusticeproject.org/rule-of-law-index/>> accessed 19 May 2021

Case-law

Case 6-64 *Flaminio Costa v E.N.E.L.* EU:C:1964:66.

Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:779.

Case C-434/16 *Peter Nowak v Data Protection Commissioner* EU:C:2017:994.

Case C-25/17 *Jehovan todistajat (Proceedings brought by Tietosuojavaltuutettu)* EU:C:2018:551.

DT 26 February 2020, DT-19/01478-6/KBK (Norwegian Data Protection Authority)

IMY 20 August 2019, DI-2019-2221 (Swedish Authority for Privacy Protection)

IMY 13 November 2020, DI-2019-7024 (Swedish Authority for Privacy Protection)

IMY 10 February 2021, DI-2020-2719, A126.614/2020 (Swedish Authority for Privacy Protection)

Finnish titles

Legislation

Rikoslaki 39/1889 [Criminal Code of Finland]

Vahingonkorvauslaki 412/1974 [Tort Liability Act]

Laki oikeudenkäynnistä rikosasioissa 689/1997 [Criminal Procedure Act]

Suomen perustuslaki 731/1999 [Constitution of Finland]

Laki viranomaisten toiminnan julkisuudesta 621/1999 [Act on the Openness of Government Activities]

Laki valtioneuvoston oikeuskanslerista 193/2000 [Act on the Chancellor of Justice]

Laki eduskunnan oikeusasiamiehestä 197/2002 [Act on the Parliamentary Ombudsman]

Kielilaki 423/2003 [Language Act]

Hallintolaki 434/2003 [Administrative Procedure Act]

Yhdenvertaisuuslaki 21/2004 [Non-Discrimination Act]

Laki yksityisyyden suojasta työelämässä 759/2004 [Act on Protection of Privacy in Work Life]

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009 [Act on Strong Electronic Identification and Electronic Trust Services]

Esitutkintalaki 805/2011 [Criminal Investigations Act]

Pakkokeinolaki 806/2011 [Coercive Measures Act]

Poliisilaki 872/2011 [Police Act]

Tietoyhteiskuntakaari 917/2014 [Information Society Code]

Tietosuojalaki 1050/2018 [Data Protection Act]

Laki digitaalisten palvelujen tarjoamisesta 306/2019 [Act on the Provision of Digital Services]

Sähköisen viestinnän palvelulaki 307/2019 [Act on Electronic Services and Communication in the Public Sector]

Laki oikeudenkäynnistä hallintoasioissa 808/2019 [Administrative Judicial Procedure Act]

Laki julkisen hallinnon tiedonhallinnasta 906/2019 [Act on Information Management in Public Administration]

OM021:00/2020 [Statute drafting]

LVM019:00/2017 [Statute development project]

LVM059:00/2019 [Statute development project]

HaVM 13/2018 vp [Statute development project]

HE 309/1993 vp. [Government proposal]

HE 220/2010 vp. [Government proposal]

HE 224/2010 vp. [Government proposal]

HE 192/2017 vp. [Government proposal]

HE 60/2018 vp. [Government proposal]

HE 284/2018 vp. [Government proposal]

EOAK/7688/2020 [Parliamentary Ombudsman's Decision]

Opinion of the Office of the Data Protection Ombudsman in case HE 9/2018 vp. Government's Proposal to Parliament for Legislation Supplementing the GDPR, on 15 March 2018

<www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-177690.pdf> accessed 8 March 2021

PeVL 31/2017 vp. [Statute development project]

PeVL 45/2016 vp. [Statute development project]

Reports

Association of Finnish Lawyers, Lausunto yleisen tietosuojasetuksen toimivuudesta ja sen soveltamiseen liittyvistä kokemuksista (VN/5281/2019, 2019)

Digital and Population Data Services Agency, Aurora-verkon tietosuojan vaikutustenarviointi. Available online

<https://vm.fi/documents/10623/13292513/Aurora_verkon_tietosuoja_vaikutustenarviointi.pdf/0845c1be-364c-aae7-2e9c-fb95fd19aa2a> accessed 2 April 2021

Finnish Government's analysis, assessment and research, Publication 2019:44

Finnish Government, Syrjintä Suomessa 2017-2019 -tietoraportti

Korpisaari P, Henkilötiedot ja paikkatiedot: Miten tietosuojalainsäädäntö vaikuttaa paikkatietojen julkaisemiseen ja luovuttamiseen, Ympäristöministeriön raportteja 10/2018

Ministry of Economic Affairs and Employment, Edelläkävijänä tekoälyaikaan: Tekoälyohjelman loppuraportti, Työ- ja Elinkeinoministeriön julkaisuja 2019:23

Ministry of Finance, Eettistä tietopolitiikkaa tekoälyn aikakaudella -report

Ministry of Finance, Digitalisaation edistämisen ohjelman toimintakertomus 2020 (VN/714/2020)

Ministry of Finance, Digitaalinen Suomi – Yhdenvertainen kaikille: Digi Arkeen -neuvottelukunnan Toimintakertomus, Valtiovarainministeriön julkaisuja 2019:23

Ministry of Finance & Digital and Population Data Services Agency, Digitaitokartoitus – Digitaalinen kysely (2020)

Ministry of Justice, Reports and opinions 2020:21

Ministry of Justice, the National Action Plan 2017-2019 (2017)

Ministry of Transport and Communications, Publication 20:2014

Ministry of Transport and Communications, Publication 7/2016

Ministry of Transport and Communications, Publication 9/2017

Ministry of Transport and Communications, Publication 10/2017

Ministry of Transport and Communications, Publication 2/2018

Ministry of Transport and Communications, Valtioneuvoston periaatepäätös julkisen sektorin digitaalisten tietoaisteiden saatavuuden parantamisesta ja uudelleenkäytön edistämisestä 3.3.11; Ministry of Finance: Digitalisaation edistämisen ohjelma. Available online: <<https://vm.fi/digitalisaation-edistamisen-ohjelma>> accessed 19 February 2021

Opinion of the Office of the Data Protection Ombudsman in case HE 9/2018 vp Government's proposal to Parliament for legislation supplementing the general EU GDPR, on 15 March 2018. Available in Finnish at <<https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-177690.pdf>> accessed 8 March 2021

Pohjalainen A and Ylikoski L, 'EU:n yleisen tietosuoja-asetuksen soveltamiskokemuksia Suomessa' Oikeusministeriön julkaisuja 2020:7

Poikola A, Kuikkaniemi K and Kuittinen O, My Data - Johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen (Liikenne- ja viestintäministeriö 2014, updated in 2018)

Traficom Research Reports 23/2019

Vainio N, Hämäläinen K and Rautiola E, Arviomuistio hallinnon automaattiseen päätöksentekoon liittyvät yleislainsäädännön sääntelytarpeista, Oikeusministeriön julkaisuja 2020:21

Books

Korpisaari P, Pitkänen O and Warma-Lehtinen E, *Uusi tietosuojalainsäädäntö* (Alma Talent 2018)

Raitio J, *Euroopan unionin oikeus* (Alma Talent 2020)

Periodicals

Ala-Fossi M, Alén-Savikko A, Hilden J, Horowitz A, Jääsaari J, Karppinen K, Lehtisaari K and Nieminen H, 'Operationalising communication rights: the case of a "digitalwelfare state"', *Internet Policy Review*, 8(1) (2019)

Björk A, 'Finland in the International Human Rights System', *Publications of the Government's Analysis and Research Activities* 2019:50

Harkoma A, 'Perus- ja Ihmisoikeustutkimuksesta Suomessa - asiantuntijoiden näkemyksiä', *Ihmisoikeuskeskus* (2017)

Lindroos-Hovinheimo S, 'Henkilötietojen suoja EU-oikeudessa – yksityisyyttä yhteisön kustannuksella?' *Lakimies* 1/2018

Digital resources

Borenus, 'Lessons to be learned from the First Administrative Fines Imposed by the Data Protection Ombudsman – Documentation is the Key' (June 2 2020) <www.borenus.com/2020/06/02/lessons-to-be-learned-from-the-first-administrative-fine-s-imposed-by-the-data-protection-ombudsman-documentation-is-key/> accessed 23 February 2021

Finlex, current drafts listed by ministry <www.finlex.fi/fi/esitykset/he/vireilla/> accessed 8 March 2021

Finance Finland, 'Arviomuistio hallinnon automaattiseen päätöksentekoon liittyvistä yleislainsäädännön sääntelytarpeista' <https://www.finanssiala.fi/wp-content/uploads/2020/09/FA_lausunto_040920_OM_Arviomuistio20yleislainsaadannon_saantelytarpeet_hallinnon_automattinen_paatoksenteko.pdf> accessed 1 June 2021

Finnish Data Ombudsman, Asuinrakennuksen yleisiin oviin asennettuun sähkölukkojärjestelmään liittyvä henkilötietojen käsittely (1809/452/18, 29 July 2020) <www.finlex.fi/fi/viranomaiset/tsv/2020/20200661> accessed 8 March 2021

Finnish Government, 'Digitalisaatio, kokeilut ja normien purkaminen' <<https://valtioneuvosto.fi/hallitusohjelman-toteutus/digitalisaatio>> accessed 30 May 2021

Finnish Ministry of Finance, Lausuntoyhteenveto: Kansallisen tekoälyohjelma AuroraAI:n kehittämis- ja toimeenpanosuunnitelma vuosille 2019-2023, <https://vm.fi/documents/10623/13292513/AuroraAI_lausuntoyhteenveto.pdf/0a2375f4-3795-81a8-a0f7-9589697756a4/AuroraAI_lausuntoyhteenveto.pdf> accessed 11 March 2021

Finnish Tax Administration, 'Automaattinen päätöksenteko verotuksessa' <www.vero.fi/tietoa-verohallinnosta/verohallinnon_esittely/tietosuoja-ja-julkisuus/tietojen_kasittely_ja_tietosuoj/automaattinen-paatoksenteko/> accessed 10 May 2021

Hämäläinen P and Rummukainen A, 'Onko herra Ransom mokannut?' Näin Vastaamon kiristäjä ilmestyi Tor-verkon foorumille, sai hakkerit peräänsä ja häipyi tyhjin käsin' (Yle News 30 October 2020) <<https://yle.fi/uutiset/3-11616210>> accessed 20 February 2021

Ministry for Foreign Affairs of Finland, 'Finland to lead the Freedom Online Coalition in 2021'

<https://um.fi/current-affairs/-/asset_publisher/gc654PySnjTX/content/suomi-internet-vapausj-c3-a4rjest-c3-b6n-johtoon-vuodelle-2021> accessed 1 May 2021

Ministry of Finance, 'Digitalisaation edistämisen ohjelman asettamispäätös' (25.2.2020) <<https://vm.fi/digitalisaation-edistamisen-ohjelma>>

National Non-Discrimination and Equality Tribunal of Finland 216/2017, <www.yvtltk.fi/material/attachments/ytaltk/tapausselosteet/2SVkNzOWF/YVtltk-tapausseloste_21.3.2018-luotto-moniperusteinen_syrjinta-S._L.pdf> accessed 11 March 2021

Non-Discrimination Ombudsman, 'Did you know that discrimination related to the use of artificial intelligence and algorithms is supervised by the Non-Discrimination Ombudsman?'

<<https://syrjinta.fi/se/-/tiesitko-etta-tekoalynn-ja-algoritmeihin-liittyvaa-syrjintaa-valvoo-yhdenvertaisuusvaltuutettu->> accessed 12 March 2021

Non-Discrimination Ombudsman, 'The Non-Discrimination Ombudsman's observations on artificial intelligence's effects on equality' (09.02.2021) <<https://syrjinta.fi/-/yhdenvertaisuusvaltuutetun-huomioita-tekoalynn-yhdenvertaisuusvaikutuksista-1>> accessed 2 April 2021

Non-Discrimination Ombudsman, 'Artificial Intelligence and Equality' <<https://syrjinta.fi/en/artificial-intelligence-and-equality>> accessed 2 April 2021

Office of Data Protection Ombudsman, 'The Office of the Data Protection Ombudsman safeguards your data protection rights' <<https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman>> accessed 8 March 2021

Office of the Data Protection Ombudsman, 'The Deputy Data Protection Ombudsman has ordered Vastaamo to notify personally its customers who have become victims of the personal data breach' (press release 23 October 2020). <<https://tietosuoja.fi/-/apulaistietosuojavaaltuutettu-maarasi-psykoterapiakeskus-vastaamon-ilmoittamaan-tietomurron-kohteeksi-joutuneille-asiakkailleen-henkilokohtaisesti>> accessed 18 February 2021

Parliament of Finland, 'Yleislainsäädäntö automaattiselle päätöksenteolle' <https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/yleislainsaadanto-automaattiselle-paatoksenteolle.aspx> accessed 20 May 2021

Päivinen K and Poitsalo K, 'Uudistunut työelämän tietosuojasääntely tuo yrityksille haasteita' (FIBS, 8 April 2019)

<www.fibsry.fi/ajankohtaista/uudistunut-tyoelaman-tietosuojasaantely-tuo-yrityksille-haastaita/> accessed 7 March 2021

Reinboth S, 'Telepakkokeinoilla puututaan yksityiselämän suojaan – niiden käytön hämäristä perusteluista on ruoskittu niin poliisia kuin tuomareitakin' (14 January 2017) <www.hs.fi/kotimaa/art-2000005045743.html> accessed 16 February 2021

Sanna Nikula, 'Oikeuskansleri Pöysti kiirehtii pelisääntöjä tekoälyn käyttöön: "Kenen on vastuu, jos kone tekee virheen?"' Helsingin Sanomat (Helsinki, 16 November 2019) <www.hs.fi/kotimaa/art-2000006311312.html> accessed 11 March 2021

Sittnikow C, 'First Four Administrative Fines issued for non-compliance with the GDPR in Finland' (Waselius & Wist 4 June 2020) <www.fi/news/2020/06/first-four-administrative-fines-issued-for-non-compliance-with-the-gdpr-in-finland/#content> accessed 28 April 2021

Yle News, 'Vastaamo board fires CEO, says he kept data breach secret for year and a half' 26 October 2020 <https://yle.fi/uutiset/osasto/news/vastaamo_board_fire_ceo_says_he_kept_data_breach_secret_for_year_and_a_half/11614603> accessed 7 March 2021

Case-law

Data Protection Ombudsman, 'Riittävästä toimenpiteistä huolehtiminen rekisteröidyn oikeuksien toteuttamiseksi' (9209/157/2019, 22 January 2021) <www.edilex.fi/tsv/20210724> accessed 19 February 2021

Finnish Deputy Parliamentary Ombudsman, Verohallinnon automatisoitu päätöksentekomenettely ei täytä perustuslain vaatimuksia (3379/2018, 20 November 2019) <www.oikeusasiamies.fi/r/fi/ratkaisut/-/eoar/3379/2018> accessed 26 April 2021

The Finnish Data Ombudsman's decision 1809/452/18 on 29 July 2020 <www.finlex.fi/fi/viranomaiset/tsv/2020/20200661> accessed 12 March 2021

The Finnish Data Ombudsman's decision 9209/157/2019 on 22 January 2021 <www.edilex.fi/tsv/20210724> accessed 19 February 2021

ELSA GEORGIA

Contributors

National Coordinator

Elene Ghudushauri

National Academic Coordinator

Elene Ghudushauri

National Researchers

Ketevan Makharashvili

Maia Mamaladze

Rusudan Tsagareli

National Linguistic Editor

Nata Berianidze

National Academic Supervisor

Otar Chakhunashvili

Introduction

The Internet has made the access and exchange of information easier and faster than ever. Individuals are providing their personal data online, knowingly and sometimes unknowingly for many different purposes, such as purchasing goods and services, playing, e-learning or paying taxes, accessing different websites and social media platforms. While such technological developments create new opportunities, especially during the pandemic situation, it also creates additional risks to privacy and data protection possibilities.

This document aims to analyse the overall situation in Georgia regarding personal data protection, as well as existing trends and challenges in this respect. The document reflects the issues of Human Rights violations related to data protection, such as the right to privacy, as well as the specific cases regarding the violation of the personal data protection legislation and responsive measures commenced by the government. In addition, this document aims to analyse existing legislation regulating the data protection issues, as well as the system of implementation of this legislation in question.

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

The importance of understanding the human rights dimensions of Advanced Digital Technologies is reflected in the various inquiries and reports commissioned and produced by a growing number of civil society organisations and by International and Regional Organisations such as the Council of Europe to which Georgia is a member state. As it was stated in the Report commissioned by the Parliamentary Assembly of the Council of Europe, digital technologies have a wide-ranging impact on human rights,²⁴⁹ such as the right to a fair trial and due process, privacy and data protection, freedom of expression, etc. However, in Georgia, so far little attention has been paid to this crucial topic and actions taken by the government can be deemed insufficient, especially in light of the pandemic situation due to the Covid-19. As a result, a significant violation of human rights is taking place. The main reason for this is that the issues and problems of personal data protection, especially in the context of the rapid development of information technology, are relatively new to Georgian legislation and legal practice.²⁵⁰

One of the challenges Advanced Digital Technologies pose for the Georgia government is to ensure balance between the two interests: demand for rapidly growing innovative technologies that give new opportunities to businesses and the protection of fundamental human rights, personal data and privacy. Advanced Digital Technologies such as artificial intelligence, blockchain, biometric verification technologies, etc, enables companies to process personal data in order to benefit their business.

²⁴⁹ van Est, Q. C., Joost Gerritsen, and Linda Kool. "Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality." (2017), 46.

²⁵⁰ K. Korkelia, Collection of Articles, 2011, 327.

Human error is one of the biggest challenges in data privacy and security in Georgia. Ill-informed and unaware employees can use weak passwords, mistakenly delete data, fall for phishing scams, and browse websites not under acceptable use.

Even though there is the positive tendency of raised awareness on the part of the investigators and operative staff, as well as on the part of the private companies, absence of awareness on the part of the members of public society and customers regarding the data protection threats remains a problematic issue.

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

Article 37 of the Constitution of Georgia guarantees the human rights to receive complete, objective and timely information on the state of their own work and living environment. According to Article 41 of the Constitution of Georgia, every citizen of Georgia has the right to access the information contained in state institutions, as well as the official documents there, in accordance with the law, if they do not contain state, professional or commercial secrets. This provision also establishes the obligation to protect personal data.²⁵¹ These Constitutional provisions are of high importance for protecting Human Rights related to personal data, as their violations are subject to Constitutional Court's Jurisdiction. For example, in its recent decision of June 7, 2019, the Constitutional Court of Georgia discussed the legal grounds of the processing of sensitive data by the common courts of Georgia.²⁵² In the decision, the Constitutional Court invalidated the normative content of article 6 of the Law, which banned the disclosure by the common courts of Georgia in the form of public information of the court acts issued during the open hearings.²⁵³

The domestic legislative package regarding the data protection in Georgia, which is now still in force, is a result of, at least partially, several scandals that took place after the parliamentary elections of 2012.²⁵⁴ The primary legal act regulating data processing activities in Georgia is the Law of Georgia on Personal Data Protection No. 5669,²⁵⁵ which was adopted on 28 December 2011. Before the adoption of the 2011 Statute, Personal data issues were regulated by the Administrative Code of Georgia, however, these regulations were brief and left space for wide interpretation. The purpose of the 2011 law is *“to ensure the protection of human rights and freedoms, including the right to privacy, in the course of personal data processing”*.²⁵⁶ The right to privacy restrains governmental and private actors from threatening and interfering with the privacy of individuals.²⁵⁷ Under Article 12 of the 1948 Universal Declaration of Human Rights, which has customary nature, *“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*

²⁵¹ Freedom of Expression – Guideline for State Institutions (Second Edition), 5.

²⁵² No. 1/4/693,857.

²⁵³ *ibid.*

²⁵⁴ The opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, 6.

²⁵⁵ <<https://matsne.gov.ge/en/document/view/1561437?publication=9>> accessed 12 March 2021.

²⁵⁶ Law on personal data protection, Article 1.

²⁵⁷ <<http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>> accessed 12 March 2021.

against such interference or attacks”.²⁵⁸ This right is further protected under Article 17 of ICCPR, Article 8 of ECHR and Article 7 and 8 of the EU Charter of Fundamental Rights.

Georgian law on Data Protection is further assisted by and enforced in conjunction with normative acts, namely the Law of Georgia on State Inspector Service,²⁵⁹ Resolution of the Government of Georgia on the Approval of the Regulations on the Activities of the Personal Data Protection Inspector and the Rule of Exercising the Power by Him/Her,²⁶⁰ Order of the Personal Data Protection Inspector on the Approval of the List of the Countries Having the Appropriate Guarantees,²⁶¹ and Order of the Personal Data Protection Inspector on the Approval of the Regulations of the Service.²⁶²

While assessing the legal framework of data protection in Georgia, emphasis should be placed on International treaties and Regulations as well, under which the Georgian government has taken upon several obligations and has the responsibility to harmonise its domestic legislation. Such International documents are Convention for the Protection of Individuals concerning Automatic Processing of Personal Data within the system of Council of Europe,²⁶³ to which Georgia is a signatory state and General Data Protection Regulation 2016/679 adopted by the European Union.²⁶⁴

The Scope of application of Georgian Legislation on Data Protection is quite wide as it applies to data controllers defined as a public agency, a natural or legal person who individually or in collaboration with others determines purposes and means of personal data processing and who, directly or through a data processor, processes personal data, data processors defined as any natural or legal person who processes personal data for or on behalf of the data controller, and data subjects defined as any natural person whose data is being processed.²⁶⁵ Article 3 paragraph 3 of the Law of Georgia on Personal Data Protection enumerates grounds under which the statute is not applicable, which prevents wide interpretation of the legislation in question.²⁶⁶ Other entities to which Law applies include diplomatic representations and the consular office of Georgia abroad.²⁶⁷

In addition, to protect personal information under the Law of Georgia on Personal Data Protection, it is important to define its territorial scope as well.²⁶⁸ This law applies to the processing of data on the territory of Georgia through automatic or semi-automatic means, and the processing of data through non-automatic means, which data form part of the filing system or are intended to form part of the filing system.²⁶⁹

²⁵⁸ Article 12, UDHR.

²⁵⁹ <<https://matsne.gov.ge/en/document/download/4276790/3/en/pdf>> accessed 12 March 2021.

²⁶⁰ <<https://matsne.gov.ge/ka/document/view/1972677?publication=0>> accessed 20 March 2021.

²⁶¹ <<https://matsne.gov.ge/ka/document/view/2502808?publication=0>> accessed 8 March 2021.

²⁶² <<https://www.matsne.gov.ge/ka/document/view/3212774?publication=0>> accessed 9 March 2021.

²⁶³ <<https://www.coe.int/en/web/conventions/full-list//conventions/treaty/108>> accessed 12 March 2021.

²⁶⁴ <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>> accessed 12 March 2021.

²⁶⁵ Law of Georgia on Personal Data Protection, Article 2, 3.

²⁶⁶ *ibid*, art 3 (3).

²⁶⁷ *ibid*, art 3 (2) (a).

²⁶⁸ Freedom of expression guidebook, 2 ed, p. 10.

²⁶⁹ Law of Georgia on Personal Data Protection, Article 3.

The regulator for data protection is the Office of the State Inspector, more specifically a personal data protection inspector who is a public official responsible for the supervision of the execution of personal data protection legislation.²⁷⁰ The State Inspector has three main functions:

- controlling the legality of data processing activities;
- monitoring of secret investigative actions and activities carried out in the central bank of electronic communication identification data; and
- investigation of crimes committed by the representatives of law enforcement bodies, officers or persons equal to them.²⁷¹

Chapter III of Law of Georgia on Personal Data Protection regulates Rights and Obligations of Data Controllers and Data Processors. More specifically, Data controllers may process personal data in the form and manner permitted by the Law, including to process personal and special category data; to process the data for direct marketing purposes, and to conduct the video-surveillance and more.²⁷²

The main responsibility of the data controller is to ensure that the following requirements are met:

- there is a proper legal ground (such as, for example, data subject's consent) to process the personal data;
- the personal data is being processed for specific, clearly defined and legitimate purposes;
- the personal data is processed only to the extent necessary for legitimate purposes;
- the personal data is adequate and proportionate to the purposes for which it was collected;
- the data is kept only for the period necessary to achieve the purpose of data processing;
- the data controller and data processor took necessary technical and organisational security measures to ensure the protection of personal data from accidental or illegal destruction, modification, disclosure, access and any other form of illegal use or accidental or illegal loss; and
- The security measures implemented by the data controller and data processor are adequate for the risks of personal data processing.²⁷³

The most important part of the Law of Georgia on Personal data protection to safeguard Human Rights is chapter IV of the Statute, which regulates the Rights of Data Subjects. Article 21 ensures Data subjects' constitutional and fundamental right to have access to information. When personal data is collected directly from a data subject, data controller or data processor must provide the data subject with the following information:

- which personal data are being processed;
- the purpose of data processing;

²⁷⁰ *ibid*, art 2 (s).

²⁷¹ Law of Georgia on the State Inspector Service, Article 2.

²⁷² Law of Georgia on Personal Data Protection, Article 3.

²⁷³ Implemented by the data controller, Chapter III.

- the legal grounds for data processing;
- how the data were collected;
- to whose personal data were disclosed, and the grounds and purpose of the disclosure.²⁷⁴

However, this provision is not mandatory for the data processor or data collector if the data subject already has the information or is already subject to public knowledge.²⁷⁵ The data subject must be provided with the above information immediately upon request or not later than 10 days after the request if for responding to the request it is required to:

- retrieve and process the information at another institution or structural unit or consult with either one;
- retrieve and process voluminous documents not linked to each other; and
- consult with its structural unit located in another populated place, or with another public agency.²⁷⁶

A breach of the Law of Georgia on Data Protection can result in criminal, administrative, and/or civil liability.

Criminal liability - The illegal collection, retention, use or dissemination of personal data, which caused considerable damage, can result in fine, corrective labour and/or imprisonment for three years. As for the unlawful use and/or dissemination of information on private life or of personal data through a piece of work disseminated in a certain way, through the internet, including social network, mass media or other public appearance, which has resulted in considerable damage, can be punished by fine or corrective labour for up to two years, or with imprisonment for up to four years.²⁷⁷ The legal entity can be imposed a fine, deprived of the right to run the business, or imposed liquidation and a fine.

Administrative sanctions - The State Inspector may draw up an administrative offence protocol and impose administrative liability upon a data processor and an authorised person, more specifically, order temporary or permanent termination of data processing, the blocking, destruction, or depersonalisation of personal data, the termination of transfer and issuance of administrative fines.²⁷⁸

Civil claim - Individuals may, also, bring a civil claim depending on the harm caused by the breach of the Law.

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?

Data protection should be realised according to the national legislation. However, because of the difference between the private and public sectors, there are some important issues which need to

²⁷⁴ Law of Georgia on Personal Data Protection, Article 21(1).

²⁷⁵ *ibid*, art 21(2).

²⁷⁶ *ibid*, art 21(3).

²⁷⁷ Criminal Code of Georgia, Article 157.

²⁷⁸ Law of Georgia on the State Inspector Service, Article 16.

be mentioned. First of all, the private sector can make self-regulations about disciplinary actions. Also, they can regulate how the employees have access to personal information and also accomplish regular monitoring of the process. It is important to be clear about the employees' consequences of illegal access to personal information.²⁷⁹ Statistics say that in the private sector there is indifferent attitude about the preservation of personal data.²⁸⁰ And because of that, one of the most common appeals from the state inspector is to have regulated terms of the preservation of the personal information. Thus the State inspector, as we mentioned above, allows the private sector to regulate those basic issues and have a self-regulation system according to the legislation.

Cooperation between the public and private sector is one of the most important issues. Currently, in Georgia, we don't have many cases when the private and public sectors cross each other. However, if we discuss the state inspector's appeal to the public sector, which is kind of similar to the private sector's appeal, at this point we can see the cooperation lines between them. As the state inspector said, the public sector should have internal documents which regulate the security of personal data. Also, they need to have an effective mechanism to control the individuals who process the data, as well as, have the regulations which define responsibility of these people.²⁸¹

From our point of view, the same recommendations and appeals for both sectors from the state inspector provide a good basis for their future cooperation.

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

The protection of personal data in Georgia became particularly important after the adoption of the Law of Georgia on Personal Data Protection on the 28th of December 2011. However, there was no body to supervise the implementation of the law, prevent violations and eliminate them until 2013. On the 19th of July 2013, the Government of Georgia issued Ordinance N180 "On Approval of the Regulation on the Activities of the Personal Data Dispute Inspector and the Rules of Exercise of His Powers", according to which the Chancellery of the Government of Georgia should have provided the necessary expenses for the functioning of the Inspector and his staff from the allocations assigned from the Reserve Fund of the Government of Georgia.

The definition of personal data in Georgia and the determination of its scope was carried out through the General Administrative Code of Georgia before the adoption of the special law, however, the policy of aspiration to Europe necessitated a separate legislative act to regulate this issue.

At present, the General Administrative Code of Georgia does not contain any provision concerning data protection. It is regulated by the Law Of Georgia On Personal Data Protection. Like most countries, The Law on Personal Data Protection in Georgia defines personal data as

²⁷⁹ Report on the activities of the State Inspector's Service, 2018, 82.

²⁸⁰ *ibid*, 83.

²⁸¹ Report on the activities of the State Inspector's Service, 2018, 32

any information connected to an identified or identifiable natural person. An individual shall be identifiable when he/she may be identified directly or indirectly, in particular by an identification number or by any physical, physiological, psychological, economic, cultural or social features specific to this person; paragraph 2 a) of the Law of Georgia on Personal Data Protection.

It is noteworthy that The Constitution of Georgia does not contain the concept of personal information, however, Article 18 (3) provides a list of information related to a person's health, finances or other private matters that belongs to the field of personal data and the information is protected from disclosure without the consent of the data subject.

It should also be noted that Article 18 of the Constitution provides the right to privacy of every person, and if we rely on the Constitutional Court's definition²⁸² of the right to privacy, according to which "persons are guaranteed the right to physical and moral inviolability, name and personal data." Personal data relating to a person's health, finances, or other private matters should be protected by the right to privacy. Moreover, the Constitutional Court has emphasised that, given the broad and multifaceted content of privacy, it is impossible to give an accurate and comprehensive explanation of it.

According to the Article 2 (f) of the Law of Georgia on Personal Data Protection data subject is any natural person whose data is being processed. It should be noted that this provision regulates the protection of personal data of individuals only, and the legislator does not provide such regulation for legal entities. The tendency to extend the record of the law only to natural persons was conditioned by the scope of regulation of the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.²⁸³

The law of Georgia on Personal Data Protection grants certain rights to a data subject (to request information about processing of his/her personal data, to request to have his/her personal data corrected, renewed, supplemented, blocked, deleted and destroyed; to withdraw at any point his/ her consent on processing his/her personal data; to address the State Inspector's Service or the court concerning any violation of his/her rights), and a data controller shall ensure practical application of these rights. The State Inspector's Service reviewed 21 cases throughout 2019 concerning the rights of data subjects: 10 cases against public institutions and 11 cases against private entities. As a result, 12 administrative offences have been revealed.²⁸⁴

According to the Law of Georgia on Personal Data Protection, when collecting data directly from a data subject, data controller or a data processor shall provide data subject with the following information: the identity and the registered address of the data controller and the data processor (when applicable); purpose of data processing; whether provision of data is mandatory or voluntary; if it is mandatory to provide information on legal consequences of refusal to submit them; the right of a data subject to obtain information on his/her personal data processed, request their correction, updating, addition, blocking, deletion and destruction. The analysis of cases reviewed by the State Inspector's Service demonstrates that in the course of

²⁸² "Georgian Young Lawyers Association" and Citizen of Georgia - Ekaterine Lomtadze v. Parliament of Georgia [2007] Judgment N1/3/407 of the Constitutional Court of Georgia.

²⁸³ European Convention for the Protection of Human Rights, CETS No. 108.

²⁸⁴ Report on the activities of the State Inspector's Service, 2019, 39.

administrative proceedings conducted by public bodies, they fail to provide comprehensive information to data subjects, including about the fact that their interviews are being audio-video recorded.

The State Inspector's Service examined the cases of informing data subjects by private and public entities based on the applications of data subjects. As a result, violation of established rules was revealed in a number of cases. Following types of violations have been identified: the data subject was not provided information within the 10-days term established by the law; the information provided was not complete and didn't comply with the request; the data subject's right to receive information was unlawfully restricted. Reorganisation, application of new case management systems, systematisation of archives and other similar reasons were cited as causes for not providing information within established deadlines. These reasons have been considered non-compliant with the law, as the law provides for no possibilities of extending the established deadline for informing the data subject. In contrast with requesting information on data processing, the law establishes no deadlines for handing over copies of documents containing personal data to a data subject. However, it is important to satisfy the request of a data subject in a reasonable time in order to ensure efficient implementation of the data subject's rights. Reasonability of this term should be assessed considering the volume of work that needs to be carried out, the form in which the requested document is being kept, need for requesting information/document from other structural entities or subdivisions and other factors characteristic to each individual case. In some cases that were reviewed by the Service, unreasonable delays have been established. The State Inspector's Service considered that failing to submit information in a reasonable time constituted the violation of the rule of informing the data subject and issued relevant recommendations. The cases reviewed during the reporting period also indicate that data controllers do not always substantially review individual circumstances of data subjects' requests; the data subjects often receive incomplete information issued based on certain templates that do not correspond to data subjects' requests.

According to the law of Georgia on Personal Data Protection, it is possible to restrict data subject's right to receive information only in cases when exercise of these rights endangers: the interests of national security and defence, the interests of public security, crime detection, investigation and prevention, significant financial and economic interests of the country. In some cases, the State Inspector's Service found the restriction of data subject's right unlawful. Following trend was observed in 2019 in relation to restricting data subject's right to information: persons having status of a victim in criminal proceedings requested criminal case files, referring to the provisions of the Law of Georgia on Personal Data Protection. The Criminal Procedure Code of Georgia does not entitle a victim in a criminal procedure to receive copies of a criminal case file, which may be assessed as a rule limiting a data subject's right to information. However, the State Inspector's Service issued a recommendation to respective entities (Ministry of Internal Affairs of Georgia and Prosecution Service of Georgia), requiring that they assess balance between the interests of a data subject and other lawful interests and issue information to a data subject if no legal grounds for restricting their right to information

are present. It is noteworthy to mention that in the majority of cases that were reviewed, relevant competent bodies provided copies of respective documents to data subjects.

A very important provision in the Law of Georgia on Personal Data Protection is the Right to appeal. If the rights under this Law are violated, a data subject shall have the right to apply to the State Inspector's Service or to the court under procedures determined by law, and if a data controller is a public institution, he/she may also submit an appeal to the same or senior administrative body. Also, a data subject has the right to request from a body considering the case to block data until a decision is made. And a data subject has the right to appeal the decision of a higher administrative body or the State Inspector to the court under procedures determined by law.

State Inspector's is a legal successor of the Personal Data Protection Inspector's Office, that monitored lawfulness of data processing since 2013 and conducted oversight of covert investigative actions since 2015. State Inspector's Service is an independent state authority that, as a legal successor of the Office of the Personal Data Protection Inspector, has operated in Georgia since 10 May, 2019. The key directions of its activities are: Monitoring lawfulness of personal data processing; Monitoring covert investigative actions and activities performed within the central databank of electronic communications identification data; Impartial and effective investigation of grave crimes committed by a representative of law-enforcement authorities, by an official or a person equal to an official against human rights and freedoms, investigation of malfeasance crimes committed with the use of violence or insulting personal dignity of a victim. The State Inspector is inviolable. Any type of influence on the State Inspector or illegal interference with his/her activities, shall be prohibited and is punishable by law.

One of the key functions of the State Inspector's Service is the oversight of data protection legislation and monitoring lawfulness of data processing in Georgia. For this purpose, the Inspector's Office conducts its activities in four main directions: Audit (inspection) of the lawfulness of data processing in public and private entities; Handling citizens' complaints related to data protection; Providing consultations to public and private entities on the issues related to data protection; Informing the public about the state of data protection in Georgia and events related to it.

Inspection is auditing the lawfulness of data processing in public and private organisations, that the Inspector is entitled to carry out at any time on his/her own initiative or on the basis of an interested person's complaint.

If a citizen believes that his/her personal data is processed in violation of the law, he/she enjoys the right to address the State Inspector. In the process of handling a complaint, the Inspector examines and evaluates submitted facts and circumstances. If required, the Inspector requests additional materials from relevant persons and conducts an inspection of the data controller or data processor. The term of handling a complaint is two months. On the basis of a substantiated decision this term may be extended for one month.

Mechanisms of Responding to Violations is following: If the Inspector identifies a violation in result of an inspection or handling a citizen's complaint, he/she is entitled to: Impose a relevant

administrative liability, including a fine or a warning on the data controller and data processor; Order elimination of the deficiencies in an indicated form and within an indicated period; require temporary or permanent termination of data processing; blocking, erasure, destruction or depersonalisation of data, termination of transfer to another state or international organisation; Address the court if a data controller or data processor fails to comply with the Inspector's orders; Address a competent authority if the Inspector believes that elements of crime are present; Inspector's decision is mandatory and it may be appealed at a court in accordance with the procedure established by the legislation.

The Inspector's Office provides free-of-charge consultations to citizens and organisations on data protection issues. Any interested individual or legal person can reach the Inspector's Office in a verbal or written form or via phone and receive a consultation on his/her rights, obligations, legislation and any other issues of concern.

Raising public awareness is one of the key priorities of the Inspector's Service, while establishing the culture of respect for privacy in the country is part of its mission. Accordingly, the public is regularly informed on the importance of data protection, its rights and obligations, accompanying risks and activities of the Inspector's Office. Multiple projects, events and activities are being planned and implemented via diverse and modern channels of communication, digital and interactive forms, multimedia platforms and educational activities.

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

According to the Law of Georgia on the State Inspector Service "*State Inspector Service shall be established, which is an independent body. The purpose of the State Inspector Service is to control the legality of personal data processing.*"²⁸⁵ The State Inspector has annual reports about the situation, which includes some kinds of reviews of the data protection cases. Annual reports include statistics of public and private sector, as well as, law-enforcing organs' activities. According to Article 13 (b) of the Georgia Law on the State Inspector Service, "*the state inspector service shall be reviewing applications related to personal data protection.*"

Therefore, it is an obligation for this body to review the cases of data protection breaches properly.

Process of judicial review is defined in Article 14 of the Georgia Law on the State Inspector Service. According to this Article, the State Inspector Service is obliged to review the application related to the data protection. Within 10 days the state inspector service shall decide which measures should be taken and notify the applicant. Also, state inspector service has a right to investigate circumstances about the received application. Limit of the time for reviewing is two months. It may be extended by not more than one month.

After reviewing, the state inspector service shall decide one of the measures, under Article 16 of this Law. According to this Article, During the process of judicial review, if the State Inspector's Service detects violation of this Law or other normative acts that regulate data processing, he/she may apply one or several following measures simultaneously:

²⁸⁵ Law of Georgia on the State Inspector Service, Article 2 (a).

- demand the elimination of violations and deficiencies related to the data processing in the form and within the time limit indicated by him/her;
- demand the temporary or permanent termination of data processing if measures and implemented procedures applied by a data processor or an authorised person for the protection of data security fail to comply with the requirements established by the legislation of Georgia;
- demand the termination of data processing, their blocking, deletion, destruction or depersonalisation if he/she believes that the data processing is conducted in violation of the legislation of Georgia;
- demand the termination of data transfer to other states and international organisations if the transfer of data is carried out in violation of the legislation of Georgia;
- give written advice and recommendations to a data processor and an authorised person if they insignificantly violate the data processing procedures;
- impose an administrative liability on the violator.

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

Judicial review is the process by which judges examine the decisions of public bodies and consider whether the law has been correctly followed. Judicial review can be an expensive and time-consuming process but it is often the last mechanism people have for checking the abuse of power within Government and public bodies. It is therefore crucial for upholding the rule of law. Judicial review is most effective when it forms part of a focused campaign to raise public awareness about issues of either significant local concern or wider public interest.²⁸⁶

It is important to mention that the purpose of Georgian anti-discrimination law is to eliminate all forms of discrimination and to ensure equal enjoyment of the rights established by the legislation of Georgia for any natural and legal person irrespective of their race, skin colour, language, sex, age, citizenship, origin, place of residence, property or rank, religion or belief. In addition to this, everyone should enjoy their rights established by the law, regardless of national, ethnic or social background, profession, marital or health status, disability, sexual orientation, gender identity and expression, political or other views or other marks.²⁸⁷ Discrimination especially occurs when individuals or groups are unfairly treated in a way that is worse than other people are treated, on the basis of their actual or perceived membership in certain groups or social categories. Based on Georgian legislation, In order to eliminate discrimination, any institution is obliged to: respond promptly and effectively to any fact of alleged discrimination; in case of confirmation of the fact of discrimination, in accordance with the legislation of Georgia and internal regulations, impose liability on the person violating it and ensure that the consequences of discrimination are eliminated without violating the rights and legitimate interests of a third party and, of course, its activities, as well as legal acts and internal regulations, if any, comply with this Law and other

²⁸⁶ <<https://www.leighday.co.uk/our-services/human-rights/judicial-review/>> accessed 12 March 2021.

²⁸⁷ Law of Georgia on the Elimination of All Forms of Discrimination.

anti-discrimination legislation. The first step of the process of judicial review on anti-discrimination cases is appealing to the Public Defender.²⁸⁸ The Public Defender of Georgia is the body that can supervise the elimination of discrimination and ensure equality. In order to exercise the powers granted by the legislation of Georgia, the Public Defender of Georgia records and analyses statistical data on facts of discrimination, takes measures to raise public awareness on issues of discrimination and Cooperates with international governmental and non-governmental organisations, local non-governmental organisations and representatives of civil society on discrimination issues. Also, it is important that in order to perform his functions, the Public Defender of Georgia is entitled, as an interested person, to apply to a court in accordance with the Administrative Procedure Code of Georgia and request the issuance of an administrative act or action if the administrative body has not responded to its recommendation or has not shared that recommendation and there is sufficient evidence to prove discrimination. We must mention that for the purposes of this Law, the Public Defender of Georgia has an opportunity to develop opinions on the necessary legislative changes and submit them to the Parliament of Georgia in the form of a legislative proposal. Besides, any person who considers himself a victim of discrimination has the right to file a lawsuit against the person or institution who allegedly discriminated against him/her and also to demand compensation for moral and/or material damage.²⁸⁹ It means that the second body that conducts judicial review of anti-discrimination cases is the court.

In case of discrimination, the public defender provides legal representation, consultation, and advice to clients. Public defender represents clients during criminal investigative proceedings and prepares a defence, conducts legal research, gathering facts and interviewing the client and witnesses. When the ombudsman is on his/her duties he/she may have, checking conducting to request a state authority, municipal body, public institution or official, and in connection with a case of discrimination - as well as a natural person, legal entity, other organisational entity, association of persons without creating a legal entity or entrepreneurial entity and Certificate, document and other materials and any official To request and receive a written explanation from the official, a person equal to him/her, and in connection with a case of discrimination - as well as a natural person, legal entity, other organisational entity, association of persons without creating a legal entity or entrepreneurial entity.

The elements that are taken into consideration when such review is conducted are the relevant materials and the facts that give rise to the suspicion of committing a discriminatory act After which the person committing the alleged discriminatory act bears the burden of proving that no discrimination has taken place. As we know, Any kind of discrimination such as direct discrimination that is the treatment or creation of conditions that put a person in an unfavourable position in comparison with other persons in similar conditions or put persons in substantially unequal conditions on an equal footing in the exercise of the rights established by the legislation of Georgia, or indirect discrimination that is a situation when a form, neutral and substantially discriminatory provision, criterion or practice puts a person in an unfavourable

²⁸⁸ Organic Law of Georgia on the Public Defender of Georgia.

²⁸⁹ Law of Georgia on the Elimination of All Forms of Discrimination.

position compared to other persons in similar conditions or equals persons in substantially unequal conditions, is prohibited in Georgia. Discrimination must not be a special and temporary measure designed to promote or achieve de facto equality and also, discrimination shall not be deemed to be any difference, inadmissibility or advantage concerning a specific job, activity or field based on specific requirements. If there is an irresistible interest of the state and state intervention is necessary in a democratic society in this case different treatment, creation of conditions and/or situation is permissible. According to the article “Analysis of Georgian labour legislation”²⁹⁰: It is noteworthy the decision # N2/7/219 of 2003²⁹¹ of the Constitutional Court of Georgia that defined the principle of equality: “equality before the law means recognition and protection of all rights and freedoms of individuals who are in equal conditions and have adequate perceptions towards issues identified by the law. The mentioned principle also deals with the lawmaking activities of a state to ensure that individuals who are in equal conditions are granted equal privileges and imposed equal obligations. It is obvious that different legal regulations should not be per se considered to be a violation of the principle of equality before the law. A lawmaker is entitled to prescribe differentiated conditions that should be justified, rational and reasonable. At the same time, persons in equal conditions should enjoy the same level of differentiation.” Three elements of the prohibition of discrimination mentioned in the definition should be identified: a) granting equal privileges (imposing equal responsibilities) to persons who are in equal conditions; b) admissibility of differentiated regulations; c) justification, rationality and reasonability are the basis of legitimacy of differentiated approach. Accordingly, if individuals are in unequal conditions based on social and economic factors or due to health or other conditions, lawmakers allow their unequal treatment through granting them privileges based on the principle of equity, and of course, this can’t be considered as an element of discrimination.²⁹²

Theoretically, Georgia has a variety of pieces of legislation that protects minorities from discrimination. The 2014 law on the elimination of all forms of discrimination specifically provides legal protections for discrimination on the basis of gender identity, ethnicity, among other attributes, But the main thing is if Georgian legislation, its review constitutes effective protection against discrimination.

It is noteworthy to mention that a new study, presented by Media Development Foundation²⁹³, a local watchdog, said that in 2019 homophobic hate speech statements have drastically increased in Georgia, while remarks involving xenophobia, racism and religious discrimination observed decline. The study, focusing on five forms of hate speech – homophobia, xenophobia, religious discrimination, hate speech with different motives, and racism – monitored discriminatory statements made by media, political parties, civil society organisations, clerics and representatives of society. According to the research, in 2019, a total of 1918 discriminatory statements have

²⁹⁰ Analysis of Georgian labour legislation, 2014, 7.

²⁹¹ <<https://constcourt.ge/ka/judicial-acts?legal=162>> accessed 12 March 2021.

²⁹² Analysis of Georgian Labour Legislation – Gender-Based Discrimination in the Workplace and its Legal Implications.

²⁹³ <<http://www.mdfgeorgia.ge/eng/home>> accessed 12 February 2021.

been recorded, most of them being homophobic (63.3%), while xenophobic comments came second with 28.1%. In general, compared to 2018, the number of homophobic statements has increased drastically (2019-1214; 2018 – 732), whereas xenophobic (2019 – 538; 2018 – 802), discriminatory in the religious sense (2019 – 76; 2018 – 154), and racist (2019 – 6; 2018 – 54) commentaries have declined.²⁹⁴

Violence/discrimination based on sexual orientation and gender identity is one of the most problematic issues in Georgia. According to the ombudsman, LGBT individuals often experience abuse, intolerance, and discrimination in every sphere of life. Homophobic statements by public officials feed widespread homophobia in society. In its first implementation report on the European Union–Georgia Association Agreement²⁹⁵, adopted in November 2018, the European Parliament hailed the country’s progress, but also called on authorities to address some outstanding concerns, such as labour standards, environmental protection and discrimination against vulnerable groups and women. In his July report, the United Nations (UN) independent expert on the enjoyment of all human rights by older persons noted, inter alia, the “frequent” nature of old age discrimination in the labour market, gender-based violence, lack of programmes preventing violence against older persons. She called on authorities to devise a strategy addressing discrimination and ageism.²⁹⁶

Also, despite the legislative amendment to article 53’ of the Criminal Code of Georgia, which ensures that bias-motivated by the sexual orientation or gender identity of a victim may be taken into account as an aggravating circumstance when determining sanctions, there are still no official statistics about crimes conducted on sexual orientation or gender identity grounds in the country.²⁹⁷ According to the registered cases and conducted studies, it has become clear that in Georgia the law prohibiting discrimination is not efficient.

Also, it is important to mention that focusing on human rights in the digital age is key. The grave violations of human rights leave no room for doubt. discrimination, intimidation, and cyber-bullying on the internet lead to real-world targeting, harassment, violence and murder, even to alleged genocide and ethnic cleansing. Failure to take action will result in further shrinking of civic space, decreased participation, enhanced discrimination, and a continuing risk of lethal consequences – in particular for women, minorities and migrants, for anyone seen as “other”. Georgian legislation does not regulate this issue properly.

Georgian judicial review does not constitute effective protection against discrimination. Georgia needs to constantly seek out and assess gaps in protection. This doesn’t just mean passing new laws that eliminate discrimination but also adapting the way we use institutions and processes. the anti-discrimination Strategy must be a consolidated set of public policy measures, conditions and instruments to be implemented by the Georgian bodies to prevent or reduce all forms and specific cases of discrimination, in particular against specific individuals or groups of individuals concerning their characteristics.

²⁹⁴ <<https://civil.ge/archives/366618>> accessed 12 March 2021.

²⁹⁵ <https://www.europarl.europa.eu/doceo/document/A-8-2018-0320_EN.html> accessed 12 March 2021.

²⁹⁶ EU – Georgia Association Agreement.

²⁹⁷ Criminal Code of Georgia.

Georgia needs to provide expertise, build competencies, advocate and raise awareness among policymakers, legal professionals, law enforcement agencies and civil society organisations to enable them to fully align national legislation and bylaws on anti-discrimination, hate crimes, and hate speech as well as relevant monitoring mechanisms to the Council of Europe standards; Ensure their effective implementation; Increase public appreciation for the laws' contribution towards democracy, human rights, peace and prosperity in the Georgian society.²⁹⁸

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?

Nowadays artificial intelligence influences important issues in everyday life. Georgia does not provide any specific regulations on advanced digital technologies, such as big data, artificial intelligence, Internet of Things or encryption. The term "artificial intelligence" is mentioned only three times in the normative acts of Georgia. None of them is a legislative act. Two of these regulations address the development of artificial intelligence-based services in the private financial sector, and one recognises the status of AI as a high-tech start-up. Georgian legislation does not say anything about the use of artificial intelligence systems by public institutions. However, this does not mean that public institutions are prohibited from using artificial intelligence. To determine the place of artificial intelligence in the Georgian legal space, it is important to understand what artificial intelligence is in general. There is no internationally recognised and accepted concept of the definition of artificial intelligence.

Although there is no special legislation in Georgia regulating artificial intelligence, the Constitution of Georgia, like other legislative acts, sets out a number of normative requirements that apply to the use of artificial intelligence by public institutions. According to the first and fourth paragraphs of Article 4 of the Constitution of Georgia, Georgia is a state governed by the rule of law, and state power is exercised within the limits established by the Constitution and the law. This provision of the basic law of the State reinforces the principle of the rule of law, which in turn requires that any action of the State be compatible with the requirements of the law. The main purpose of the compatibility of artificial intelligence with the principles of democracy and the rule of law - is to respect human dignity, freedom and the right to information and self-determination.

The implementation of artificial intelligence systems in the Georgian public sector is at an early stage of development, however, in the private sector, there are many successful examples of the use of this technology, remote verification systems, automatic document identification systems, communication automation programmes and many other tools. This sector has become particularly profitable in the face of pandemic conditions due to increased demand for remote services. Consequently, it is already clear what potential the large-scale use of artificial intelligence has in terms of increasing efficiency and cost-effectiveness in various processes. However, some

²⁹⁸<<https://rm.coe.int/project-summary-fight-against-discrimination-hate-crimes-and-hate-speech/1680924c31>> accessed 8 March 2021.

risks can arise as a result of system misuse, technical glitches, and mismanagement of personal data.²⁹⁹

As a result of the study, the absence of normative acts regulating artificial intelligence systems and documents defining ethical norms in the target agencies becomes apparent. In order for the public sector to get the most out of these technologies, it is vital to have access to the information about the systems used, their publicity to eliminate bias risks and gain a high degree of reasoning and trust.

First of all, the public sector should contribute to the creation of a national ecosystem for AI to build national start-ups in the country, industry, attract investors and donors, using AI applications by different sectors, and achieve socio-economic growth and prosperity through artificial intelligence. At the same time, for the development of artificial intelligence, the government should create a regulatory framework that balances and reduces the threats, risks, challenges associated with artificial intelligence systems, and provides effective mechanisms for enforcing the legal and ethical standards adopted. Moreover, Georgia thrives to be involved in external legislative developments. For instance, Georgia actively takes part in CEPEJ GT-QUAL³⁰⁰. The CEPEJ has developed important reference texts concerning the implementation of digital justice in the judicial systems of the member states of the Council of Europe: the Guidelines on how to drive change towards cyber justice as well as the European Ethical Charter for the use of artificial intelligence in judicial systems and their environment, which quickly established itself as a reference at international level and Georgia is ready to implement all the regulations in the national legislation.

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

Technological innovation creates powerful forces for change to which societies must adjust. It is noteworthy that encryption has enormous benefits for security and privacy and the use of encryption by individuals and organisations should be encouraged. It is easy to guess that the challenge comes from devices, applications and services that provide encryption that is impossible to access without the assistance of the user and the impact of this on public safety. Encryption scrambles plaintext messages. It turns data into unreadable code that can only be deciphered by those that have a secret key or password. There are two types of encryption: recoverable encryption and unrecoverable encryption. Recoverable encryption is when some encryption products and services allow a third party to provide access to decipher encrypted communications without the cooperation of the sender or recipient of the message or the owner of the device on which the encrypted data is stored. Unrecoverable encryption products and services use cryptographic techniques that prevent any third party. Unrecoverable encryption is what causes the greatest challenge for law enforcement. People who fear government surveillance worry that restrictions on encryption will put their privacy at risk. At the same time,

²⁹⁹ Use of Artificial Intelligence Systems in Georgia: Legislation and Practice, 2021, 29.

³⁰⁰ <<https://www.coe.int/en/web/cepej/georgia>> accessed 12 March 2021.

there is a growing risk to public safety as organised crime, terrorists, and child pornographers are drawn to the use of encrypted communications platforms that are technically impossible to access by law enforcement or by the companies that provide the device and applications. Societies must choose how to balance privacy, cybersecurity and public safety to decide whether increased use of unrecoverable encryption creates risks that justify regulation of its design, Sale, or use.³⁰¹

The Criminal Code of Georgia requires liability for the violation of the secrets of private communication. According to the Criminal Code of Georgia, Unauthorised recording or interception of private conversation, as well as, unauthorised extraction of computer data.

It is noteworthy that the Criminal Code of Georgia request exception: “Criminal liability for the crime provided for in paragraph 1 of this Article shall not be imposed on the person who provided the obtained/stored information provided for in paragraph 1 of this Article to the investigative bodies and thus provided information on other committed/expected criminal acts.”³⁰²

The Criminal Code of Georgia also provide liability for violation of the secrecy of personal correspondence, telephone conversations or other means of communication: “Illegal receipt, opening, disclosure, acquaintance with or storage of the content of personal correspondence or postal mail, recording of conversations by telephone or other technical means or telegraph, computer system, fax or other technical means, shall be punishable by a fine or correctional labour for a term not exceeding two years, or by imprisonment for a term not exceeding three years;³⁰³ Illegal use, dissemination or other provision of access to messages received or transmitted by personal correspondence or mail, by telephone or other technical means or by telegraph, computer system, fax or other technical means-Is punishable by imprisonment for a term of two to five years”. However, it is important that the Criminal Code of Georgia excludes liability if this action can help to the criminal investigations: “Criminal liability for the crime provided for in paragraph 1 of this Article shall not be imposed on a person who has provided the obtained/stored information provided for in paragraph 1 of this Article to the investigative bodies and has provided information on other committed/expected criminal acts in this way”.³⁰⁴

In conclusion, we can say that Georgian legislation requires encrypted personal messages to be decrypted and accessible for criminal investigations.

The Constitution of Georgia ensures the inviolability of Rights to privacy and family life, personal space and also inviolability of communication: A person's personal and family life is inviolable. Restriction of this right is permissible only in accordance with the law, in order to ensure the necessary state or public security in a democratic society or to protect the rights of others.³⁰⁵ It is noteworthy that these fundamental rights are not absolute and may be restricted by

³⁰¹The Effect of Encryption on Lawful Access to Communications and Data, James A. Lewis, Denise E. Zheng, William A. Carter, Report of the CSIS Technology Policy Programme, February 2017.

³⁰² Criminal Code of Georgia, Article 158 (2).

³⁰³ *ibid*, art 159 (1, 2).

³⁰⁴ *ibid*.

³⁰⁵ Constitution of Georgia, Article 15 (1).

the state under certain conditions. However, any decision to restrict this freedom must be substantiated and the need to restrict the secrecy of personal life must be made clear. It means that restriction of the above-mentioned fundamental freedoms by the Constitution is allowed only by a court decision, or without it, in case of urgent necessity defined by law. The need for a court decision is a guarantee that the relevant state agencies will not abuse their rights. The court is the institution where the representatives of the executive power must prove the necessity of restricting the right to privacy of a person. It is this mechanism that guarantees the protection of citizens. It is therefore important for the judiciary to be independent and to pay particular attention to any cases involving the restriction of personal life. This regulation is provided in article 15.2³⁰⁶

The first paragraph of Article 7 of the Law of Georgia on Operative-Investigative Activities states that an operative-investigative measure is the action of a state body or official authorised in accordance with the rules established by this Law, which, within its competence, ensures the fulfilment of the tasks provided for in Article 3 of this Law. The third article even points to that The tasks of the operative-investigative activity are: A) detect, prevent and prevent a crime or other unlawful act; B) the identification of a person who prepares, commits or who has committed a crime or other unlawful act; c) the person in the state body of the order, which, despite a call, to avoid investigation or court before the announcement; the defendant or the defendant's search and the relevant state authority to submit, if he is to avoid the imposed coercive measure of use or assigned punishment Happen; D) search and identification of property lost as a result of criminal or other unlawful encroachment; e) for tracing the missing person search; f) criminal law dealing with the necessary actual data mining; G) Identification of the perpetrator of a crime or other illegal act (determination of name, surname, age, citizenship); H) Information-analytical support for the management of penitentiary institutions.³⁰⁷

The list of circumstances in which such decryption may be conducted is closely related to the Principles of operative-investigative activities. This kind of decryption may be conducted if its implementation is provided for by law and is necessary for a democratic society to the legitimate objectives to achieve - national security or public safety to ensure the prevention of disorder or crime has been committed from the beginning to prevent the country's economic well-being of interest or to protect the rights and freedoms of others. An operative-investigative measure (in this case, decryption procedure) is necessary for a democratic society if its implementation is caused by an urgent public need and it is a suitable and proportionate means of achieving a legitimate goal. operative investigative measure the scope of this event is the result of obtained data of operative-searching activities legitimate purposes and objectives proportionate to be.

In some cases, (for example, when power is used illegally) decryption of encrypted personal messages and accessibility for criminal investigations can pose a threat to human life, health, honour, dignity, and property. Also, it can endanger the rights of a legal entity.

³⁰⁶ *ibid*, art 15 (2).

³⁰⁷ Law of Georgia on Operative-Investigative Activities, Article 3.

In general, illegal restriction of the rights and freedoms of a natural and legal person by a body (public servant) carrying out operative-investigative activities shall give rise to liability in accordance with the rules established by the legislation of Georgia. Also, Georgian legislation determines that It is prohibited to carry out operative-investigative activities to achieve a task the identification of a person who prepares, commits or who has committed a crime or other unlawful act; that is not provided by this law (task could be for example: detect, prevent and prevent a crime or other unlawful act, criminal law dealing with the necessary actual data mining, etc.)

Due to law 'About operative-investigative activities' a person who believes that an operative-investigative measure against him has resulted in an unlawful restriction of his rights and freedoms may appeal the lawfulness of the operative-investigative measure to the relevant higher state body, the prosecutor or a court. Illegal notification of the operative-investigative measure creates the basis for recognising the information obtained as a result of this measure as inadmissible evidence in accordance with the rules established by the Criminal Procedure Code of Georgia. The burden of proving the legality of an operative-investigative measure rests with the body conducting the operative-investigative measure.

It is also mentioned that the bodies carrying out operative-investigative activities (public servants) are prohibited from secretly participating in the activities of the legislative, executive and judicial authorities of Georgia, the highest representative bodies of the Autonomous Republics of Abkhazia and Adjara, as well as the municipal bodies. Covert participation in the activities of officially registered public and political organisations, religious organisations is prohibited, unless these activities are aimed at overthrowing or violently changing the constitutional order of Georgia, violating the country's independence, territorial integrity, or if these organisations do not engage in propaganda of war or violence, religious or social strife. In such a case, the consent of the Prosecutor General of Georgia is required. The material obtained as a result of the operative-investigative measure provided for in Article 7, Paragraph 3, Subparagraph "a" of this Law shall be destroyed immediately after 6 months from the termination of the operative-investigative measure. This material is destroyed by the prosecutor submitting a motion to the court on the conduct of the operative-investigative measure with the participation of the judge issuing the relevant verdict. A report on the destruction of the said material shall be drawn up and it shall be certified by the signatures of the relevant prosecutor and the judge. This protocol shall be submitted to the State Inspector's Office, and in the criminal case pending before the State Inspector's Office - to the Supreme Court Judge (Supervising Judge) appointed by the Chairman of the Supreme Court of Georgia and shall be reflected in the Register of Covert Investigative Actions.³⁰⁸

On the one hand, we can say that Georgian legislation requires some kind of protection for the person whose personal messages are encrypted (Article 11 contains the same content too: 1. The results of operative-investigative activities can be used to prepare and carry out investigative and procedural actions, measures to prevent, prevent and open crime. 2. Operational inspection

³⁰⁸ Law of Georgia on Operative-Investigative Activities, Article 6.

materials do not constitute a basis for restricting the rights and freedoms of a natural person and the rights of a legal entity) and liability for those authorised bodies which have the power of encryption.

But the key is if these regulations are enough and if this legislation is correctly used in a practice. The level of law on the one hand defines that an operative-investigative measure can be carried out only if it is directly provided by law, but the law does not specify, in particular or even in general terms, what category of crime prevention it is possible to use operative measures. Also, Georgian legislation does not contain any indication of time constraints (except in exceptional cases) and the circle of persons to whom this type of action may be applied, which is usually a fundamental component of key international standards of covert activity.

In Conclusion, it seems that authorised bodies have too much power/freedom that gives them the opportunity to restrict the inviolability of rights to privacy.

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

We live in a world today where digital advancements and extensive flows of information have become natural and unquestioned features of day to day life. Everything from Social Media to different online services have come to define the way of our life. When referring to balance between the human rights of privacy and freedom of expression on the one hand and allowing digital advancements on the other hand, states are obliged to take as its starting point the internationally recognised laws and standards for human rights set out in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights.³⁰⁹ Freedom of expression and right to privacy are clear-cut parts of this international legal system of human rights and facilitate the realisation of other human rights. The negative as well as the positive obligations of governments to respect, protect, promote, and fulfill human rights is the foundation of this framework. This includes the duty to ensure that domestic legislation is in conformity with international human rights laws and standards on freedom of expression and right to privacy.³¹⁰

It is the obligation of the Georgian Government to create a national legislation and practice adequate safeguards against the abuse of power or arbitrariness from the side of authorities. “Article 8 of the European Convention on Human Rights provides for the right to private life. Interception of communication is not necessarily incompatible with that right; but it must be carried out consistently with the requirements of both the ECHR and the Council of Europe Data Protection Convention.”³¹¹ The current practice before the European Court of Human Rights indicates that violation of the right to privacy by law enforcement bodies is still common and even for the purposes of the crime investigation or the state security a subject to debate.³¹²

³⁰⁹ BSR | Protecting Human Rights in the Digital Age, 5.

³¹⁰ *ibid.*

³¹¹ Report of the Council of Europe experts Joseph A. CANNATACI and Graham SUTTON, Key Points Regarding Access to Personal Data by Law Enforcement and by National Security Agencies, September 2014.

³¹² Council of Europe, Guide on Article 8 of the European Convention on Human Rights, paras. 175 – 191.

Although the right to privacy is guaranteed by the Constitution of Georgia, in recent years illegal surveillance has become a systematic practice in Georgia, where politicians, journalists and activists are secretly videotaped and then blackmailed³¹³. Adopted in 2011, The Law on Personal Data Protection was not followed with the relevant enforcement provisions and thus proved ineffective. In 2013 a special commission was set up in to monitor compliance with the law.³¹⁴ A Personal Data Protection Inspector has been appointed to review citizens' complaints and monitor data retrieval in the country and assess the legality of data processing. In addition to this, the Inspector submits annual reports to Parliament.

According to the report conducted by the Personal Data Protection Inspector, in 2015 at least 14 cases were found in which the prosecutor's office obtained the data without a court ruling. In 2015 and the pre-election period of 2016, audio and video recordings of the private lives of oppositionists were widely made public. In December 2016, the Public Defender noted numerous violations of the right to privacy and family life during that year.³¹⁵ In 2016, the Georgian Young Lawyers Association (GYLA) revealed numerous facts of search and seizure by the Prosecutor's Office on the grounds of "urgency", which were later approved by the court,³¹⁶ indicating a lack of understanding and respect for the right to privacy.

According to the report published by the Personal Data Protection Inspector in 2019, cases of disclosure of personal data have been identified not only by official authorities, but also in the private sector. Data processing organisations process data obtained through services or other activities, in some cases, without any legal basis or need. For example, one of the companies published the identity and personal information of a citizen through a financial contract, on the social network Facebook.³¹⁷

In its report the Personal Data Protection Inspector identified two cases of violation of personal data by higher education institutions. LEPL - Tbilisi Apolon Kutateladze State Academy of Art published a list of 73 students in debt on their Facebook page in order to inform them about the non-payment of fees. Since the institution could not justify why it was necessary to publish financial debt information in a form which is accessible to any person, disclosing the data was considered a violation of the law and the academy was held administratively liable.³¹⁸

LEPL - Ilia State University using Google search engine made an excel file available in which was provided the results of the examinations of 190 candidates for the Master's degree, along with their personal Numbers, Names, Surnames, Cell Phone Numbers, Course, Scores, gender, legal address, etc. Hidden in the same file was additional 243 individuals' personal data.³¹⁹ Even though, unlike the previous case, the university justified its action in the interests of a transparent examination process, in the data processing process, the university failed to follow safety rules

³¹³ <<https://agenda.ge/en/news/2016/562>> accessed 12 March 2021.

³¹⁴ Thomas Hammarberg's Report, 2013, p. 21.

³¹⁵ Report on the activities of the State Inspector's Service, 2016.

³¹⁶ #9 Report of the GYLA.

³¹⁷ Report on the activities of the State Inspector's Service, 2019, pp. 56-57.

³¹⁸ *ibid*, pp. 58.

³¹⁹ *ibid*.

and released more volumes and terms than was required to achieve legitimate goals. The University was held administratively responsible.

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?

Data protection forms a part of the general protection of privacy as for example stated in article 8 of The European Convention on Human Rights. Data protection has evolved and became a more important issue in Georgia as well, due to the technological developments and possibilities. As it was stated above, Georgian legislation still has a long way to go in order for it to provide perfect protection of human rights of individuals where data protection is concerned.

In order for the Georgian legislation and practice to be in conformity with the International legal system and standards, and ensure an adequate balance between allowing digital advancements and protecting human rights online, the presence of a local data protection officer should be mandatory in every public institution, as well as in certain private companies that deal with large amounts of personal data. At the same time, it is necessary to raise public awareness on issues such as using social media.

Regarding the process of judicial review of cases of data protection breaches, it is worth mentioning that in the last years the judicial assessment process has significantly improved in Georgia, considering that the number of cases brought before the court has also notably increased.³²⁰ It is especially noteworthy to consider how this positively will affect the improvement of the data protection situation in the following 5 years. In this respect the judicial review can play an important role. However, there are still concerns in this area, such as the unreasonable delays, which might slow down the process of development.

Considering that cases of discrimination in the context of personal data protection will be assessed not only through the Georgian Law on data protection, but also 2014 Law on the elimination of all forms of discrimination, hopefully, existing state of affairs will enhance at a better pace. This is especially promising as awareness regarding the anti-discrimination issues in Georgian society has significantly risen in the last years.

As for the regulations regarding this, this is one of the areas which need not only mechanisms for effective enforcement, but also amendments in legislation must be made in the following 5 years, as the absence of normative acts regulating artificial intelligence systems and documents defining ethical norms in the target agencies is apparent.

Conclusion

While the definition, qualifying criteria and general minimum standards of protection for data protection in Georgia seem to replicate the provisions of the 1981 Council of Europe Personal Data Protection Convention, the overall situation is still far from perfect. It is also worth

³²⁰ *ibid*, p. 39.

mentioning that the introduction of a Personal Data Protection Inspector has appreciably improved the level of first of all, control and identification of data protection violations and secondly, enforcement of Georgian Law on Personal Data Protection. While some promising practices have been identified, trends in the curtailing of procedural rights raise concern and require further research. The existing substantive provisions cannot be enjoyed by individuals if they are not effectively enforced and face unreasonable delays and setbacks during the process of Judicial Review.

Table of legislation

Provision in [native] language	Corresponding translation in English
საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ, მუხლები 1, 2, 3, 16, 21	Law of Georgia on Personal Data Protection, Article 1, 2, 3, 16, 21
საქართველოს კანონი სახელმწიფო ინსპექტორის სამსახურის შესახებ, მუხლი 16	Law of Georgia on the State Inspector Service, Article 16
საქართველოს სისხლის სამართლის კოდექსი, მუხლი 157	Criminal Code of Georgia, Articles 157, 158 (1, 2), 159 (1, 2), 284 (1)
საქართველოს კონსტიტუცია, მუხლი 15(1)	Constitution of Georgia, Article 15 (1)
საქართველოს კანონი ოპერატიულ-სამძებრო საქმიანობის შესახებ, მუხლები 3, 6	Law of Georgia on Operative-Investigative Activities, Articles 3, 6
საქართველოს კანონი დისკრიმინაციის ყველა ფორმის აღმოფხვრის შესახებ	Law of Georgia on the Elimination of All Forms of Discrimination.
საქართველოს ორგანული კანონი საქართველოს სახალხო დამცველის შესახებ	Organic Law of Georgia on the Public Defender of Georgia

Bibliography

English titles

Legislation

Constitution of Georgia

Law of Georgia on Personal Data Protection

Law of Georgia on the State Inspector Service

Criminal Code of Georgia

Law of Georgia on the Elimination of All Forms of Discrimination.

Organic Law of Georgia on the Public Defender of Georgia

Universal Declaration of Human Rights

Personal Data Protection Inspector's Order

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

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 processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Reports

Report on the activities of the State Inspector's Service, 2018

Report on the activities of the State Inspector's Service, 2019

Analysis of Georgian Labour Legislation – Gender-Based Discrimination in the Workplace and its Legal Implications.

#9 Report of the GYLA

The Effect of Encryption on Lawful Access to Communications and Data, James A. Lewis, Denise E. Zheng, William A. Carter, Report of the CSIS Technology Policy Programme, February 2017.

Report of the Council of Europe experts Joseph A. CANNATACI and Graham SUTTON, Key Points Regarding Access to Personal Data by Law Enforcement and by National Security Agencies, September 2014.

The opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies

Books

Freedom of Expression – Guideline for State Institutions (Second Edition)

BSR | Protecting Human Rights in the Digital Age

van Est, Q. C., Joost Gerritsen, and Linda Kool. "Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality." (2017)

Use of Artificial Intelligence Systems in Georgia: Legislation and Practice, 2021

Council of Europe, Guide on Article 8 of the European Convention on Human Rights

Periodicals

K. Korkelia, Collection of Articles, 2011

Digital resources

<https://www.leighday.co.uk/our-services/human-rights/judicial-review/>

<https://civil.ge/archives/366618>

<https://rm.coe.int/project-summary-fight-against-discrimination-hate-crimes-and-hate-speech/1680924c31>

Case-law

Common Court of Georgia - No. 1/4/693,857

Georgian titles

საქართველოს კონსტიტუცია

საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ

საქართველოს კანონი სახელმწიფო ინსპექტორის სამსახურის შესახებ

საქართველოს სისხლის სამართლის კოდექსი

საქართველოს კანონი დისკრიმინაციის ყველა ფორმის აღმოფხვრის შესახებ

საქართველოს ორგანული კანონი საქართველოს სახალხო დამცველის შესახებ

ადამიანის უფლებათა საყოველთაო დეკლარაცია

კონვენცია პერსონალური მონაცემების ავტომატური დამუშავების დაცვის შესახებ

2016 წლის 27 აპრილის ევროპარლამენტის რეგულაცია პერსონალურ მონაცემთა დაცვის შესახებ

Reports

2018 და 2019 წლების ანგარიშები პერსონალურ მონაცემთა დაცვის მდგომარეობისა და ინსპექტორის საქმიანობის შესახებ

საქართველოს შრომის სამართლის კოდექსის ანალიზი დასაქმებულთა გენდერული ნიშნით დისკრიმინაციისა და მის სამართლებრივ შედეგებთან დაკავშირებით

CSIS - ის 2017 წლის თებერვლის ანგარიში

საიას თბილისისა და ქუთაისის საქალაქო და სააპელაციო სასამართლოებში სისხლის სამართლის სასამართლო პროცესების მონიტორინგის ანგარიში #9

2014 წლის სექტემბრის ევროპის საბჭოს ექსპერტების ანგარიში

Books

გამოხატვის თავისუფლება - სახელმძღვანელო საჯარო დაწესებულებებისთვის (მეორე გამოცემა)

BSR | ადამიანის უფლებათა დაცვა ციფრულ ერაში

ხელოვნური ინტელექტის გამოყენების სისტემები საქართველოში: კანონმდებლობა და პრაქტიკა, 20

ევროპის საბჭოს გაილდანი ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის ადამიანის უფლებები რობოტების ერაში: გამოწვევები, რომლებიც რობოტების შექმნამ განაპირობა, ხელოვნური ინტელექტი, ვირტუალური რეალობა, 2017

Periodicals

კ. კორკელია, სტატიათა კრებული, 2013 წ.

Case-law

საქმე No. 1/4/693,857

ELSA GREECE

Contributors

National Coordinator

Evangelos Avdoulas

National Academic Coordinator

Alexandros Avramis

National Researchers

Konstantinos Apostolos

Chrysi Chatzivasileiou

Maria Vasileia Karampatsoli

Tatiana Kyttaroudi

Maria Oikonomou Makrygianni

Maria Roussi

Vasiliki Tsiompanidou

Dimitra Vasileiadou

Anastasia Nefeli Vidaki

National Technical Editor

Evangelos Avdoulas

National Linguistic Editor

Ilia Danai Tsigkri

National Academic Supervisor

Spiros Tassis

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

With the passing of time, comes evolution. And, truth be told, the most outstanding achievements of humanity have been revolving around technology for decades. From gasoline-powered vehicles and crucial medical inventions to the so-called Internet and Information Technology, the latter rules all aspects of our everyday lives; the way we receive information, the means of communicating with others and the forms of entertainment are only some of the life dimensions influenced by technology. It is dominant for a fair reason, too, as digital innovations help the world move faster and easier. A prime example of this would be the role of technology in the COVID-19 era; it is only relieving to reflect upon how Wi-Fi connections supported whole semesters, school and academic lectures, projects, assignments, and graduations.

As with most things, technology can and is being used both for good and bad. Even warfare has taken advantage of the outrageous technological advancements, incorporating up-to-date drones and unmanned aerial vehicles in battle zones, allowing the most accurate hits without risking the life of any pilot. What is more, cyber warfare is also a well-known fact, emerging at times of elections, targeting governmental platforms or intelligence services. Major scandals concerning the malicious use of technology have shocked the international scene, namely Cambridge Analytica and the numerous incidents of data leaks from the most famous social media platforms. The list could be endlessly continued with no expiration for both the advantages and the disadvantages stemming from technology, as it is renewed each day with new facts and figures.

Pondering on a more specific aspect of the –already- vast topic of technology, Advanced Digital Technologies seem to be the cutting-edge facet of technical modernity. In an effort to come across a definition, one would not be satisfied with the outcome the World Wide Web has to offer; yet, Advanced Digital Technologies are newly emerged, “next-level” methods, systems or devices built for practical purposes³²¹ with few still users, but technical maturity³²². Examples among such technologies include, as expected, Artificial Intelligence (AI), speech and handwriting recognition, smart cards, enhanced user authentication and data mining are only one part of what Advanced Digital Technologies are³²³.

In the post-truth era of global information,³²⁴ alongside Europe, Greece has also been facing newly emerged issues correlated with the use of technology and, more specifically, its negative effects on human rights. While advanced digital technologies have unquestionably paved the way

³²¹ Collinsdictionary.com. 2021. Digital technology definition and meaning | Collins English Dictionary. [online] <<https://www.collinsdictionary.com/dictionary/english/digital-technology>> accessed 22 February 2021.

³²² Gartner. 2021. Definition of Advanced Technology - Gartner Information Technology Glossary. [online] <<https://www.gartner.com/en/information-technology/glossary/advanced-technology>> accessed 22 February 2021.

³²³ *ibid.*

³²⁴ Defining Post-truth: Structures, Agents, and Styles. [online] <<https://www.e-ir.info/2018/10/22/defining-post-truth-structures-agents-and-styles/>> accessed 22 February 2021.

for a more just world, quicker and borderless procedures and responses to human needs and disasters, as well as promising an even brighter future, the downsides are still prominent. Due to their sudden and recent appearance, but also our unfamiliarity with their function, it seems that the main problem revolves around the issue of responsibility³²⁵, deriving from the harm they cause. Technological means' general nature, opacity, and automatic operation render violations hard to detect; nevertheless, the ability to "personalize" their function and their reliance on human input, plead for the –more than likely- human rights' infringement.

The link between Advanced Digital Technologies and human rights' violation is neither always direct nor obvious, nor easily classified as a violation indeed. Even if not categorized as such, one of Greece's most frequent cases has been freedom of speech restrictions on social media platforms, as a result of algorithmic compositions coming from humanly set bans on specific words, symbols or even users.³²⁶ Apart from that, Greece has also encountered numerous cases of privacy and data protection infringements, via bank data leaks, cyber-attack and international hacking efforts on its national servers and governmental platforms.³²⁷³²⁸

In a constitutional democracy, safeguarding and promoting human rights is a pivotal priority and obligation for the State. Societies were created on the premise of anthropocentrism,³²⁹ thus human rights are our co-existence's foundation that, should it be overthrown, democracy will follow, too. The phenomena are, undoubtedly, affecting the national legislator and all consequent legislative efforts, as well as law enforcement practices. Greece still lacks the profound understanding of the technical issues emerging from Advance Digital Technologies, yet no one can doubt that the legal framework seems to catch up with the latest advancements and their effect on society, more specifically on human rights.

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

Personal information is protected in Greek legislation in multiple ways, both at constitutional and common law level. Simultaneously, external instruments, EU and international, also influence and contribute to the protection of personal data in Greece.

2.1. General Protection at EU and international level

To begin with, article 7 of the Charter of Fundamental Rights protects, in general, private life, home and communication and Article 8 protects, more precisely, personal data and establishes that 'such data must be processed fairly for specific reasons and on the basis of the consent of

³²⁵ Yeung, K., 'A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework' [2012] Rm.coe.int. <<https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168094ad40>> accessed 23 February 2021.

³²⁶ Serafeim, K., 'The Impact of Social Media on Press Freedom in Greece: Benefits, Challenges and Limitations' [2012] essachess. <<https://essachess.com/index.php/jcs/article/viewFile/157/142>> accessed 23 February 2021.

³²⁷ Hinchliffe R., 'Greece's major banks cancel 15,000 cards after travel website breach - FinTech Futures' [2020] FinTech Futures. <<https://www.fintechfutures.com/2020/01/greeces-major-banks-cancel-15000-cards-after-travel-website-breach/>> accessed 23 February 2021.

³²⁸ Greek City Times, 'Greek Government Websites Hacked' [2020] Greek City Times. <<https://greekcitytimes.com/2020/01/18/greek-government-websites-hacked/>> accessed 23 February 2021.

³²⁹ Boslaugh, S., n.d. 'Anthropocentrism | philosophy', Encyclopedia Britannica. <<https://www.britannica.com/topic/anthropocentrism>> accessed 23 February 2021.

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’.

Article 16 of Treaty on the Functioning of the European Union provides for the protection of personal data (par.1) and sets out that ‘the European Parliament and the Council ... shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data’ (par.2). According to Article 39 on the Treaty on the European Union ‘the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.’

Finally, at an international level, the European Convention on Human Rights protects the right to private and family life (Article 8 as enacted into the Greek legal order by Law 53/1974) by guaranteeing that ‘everyone has the right to respect for his private and family life, his home and his correspondence’ and that ‘there shall be no interference by a public authority with the exercise of this right’ except for specific reasons (e.g., public safety, protection of health) and in accordance with the law.

i. Specific EU Regulations and Directives regarding personal information.

The general response, at an EU level, in relation to the regulation of big data has been to adopt supranational regulations with the introduction of new rights (e.g., data protection rights) and new enforcement tools with the right to be forgotten originally developed in *Google v Spain*³³⁰ and ultimately codified in Article 17 GDPR as well as to introduce property mechanisms for non-personal data as discussed by the EU Commissioner Breton.³³¹ In other words, EU regulatory efforts have largely focused on protecting personal data, whereas, with regards to non-personal data, the EU has sought to encourage its generation and exploitation, as so-called ‘non-personal’ or industrial data are a growing focus of EU regulatory initiatives, characterised as a key new type of economic asset and the “lifeblood of the global economy”.³³²

Due to rapid technological developments and in order to face new challenges relating to the protection of personal information, Regulation (EU) 2016/679 of the European Parliament and European Council on the ‘Protection of Personal Data’ (repealing the Directive 1995/46) was issued.³³³ Following the Regulation, Directive (EU) 2016/680 of the European Parliament and European Council 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

³³⁰C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317 [88] [99].

³³¹Javier Espinoza & Sam Fleming, ‘Europe urged to use industrial data trove to steal march on rivals’ *Financial Times* (Brussels, 14 January 2020) < <https://www.ft.com/content/8187a268-3494-11ea-a6d3-9a26f8c3cba4> > accessed 2 February 2021.

³³²European Commission, ‘Enter the Data Economy: EU Policies for a thriving data ecosystem’ EPSC Strategic Note Issue 21 (11 January 2017), 1.

³³³General Data Protection Regulation (EU) 2016/679 OJ L 119/1.

prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and Directive (EU) 2016/681 of the European Parliament and European Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime were also issued. It is useful to mention that the role of CJEU in the protection of private information and the clarification of the meaning of several provisions of relevant EU law is crucial.

In brief, the General Data Protection Regulation applies to the processing by 'controllers' (natural/legal persons who determine the purposes and means of personal data processing) and 'processors' (natural/legal persons responsible for processing personal data on behalf of a controller) of 'personal data' (any information relating to a living person that can be used directly or indirectly to identify them, e.g. name, address, physical characteristics, genetic information, etc.) with special protection for 'sensitive' or special category personal data (information concerning a person's health, race, ethnicity, religious beliefs, politics, sexual orientation, biometrics, genetics etc.), for information regarding children and for criminal convictions/offences. The meaning of processing includes the collection, organization, storage, export, use, transmission, dissemination, commitment, deletion, destruction, correlation of personal data.

According to Recital 26 'the principles of data protection should apply to any information concerning an identified or identifiable natural person' and according to Recital 30 'natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags'. It becomes, therefore, clear that GDPR reflecting technological developments adopts a broad approach in relation to which information may be used to identify an individual. The distinction between "identified" and "identifiable" is not straightforward. Nevertheless, it is clear again that a broad approach is favoured. It might be thought that at least the concept of "identified" must make somebody uniquely identifiable via their usual means of identification i.e., their name, whereas, the notion of identifiability encompasses situations where the data held does not itself identify an individual but where it would be possible to link such data with a natural person through combination with other information either now or in the future. In all these cases, the controller must take into account 'all the means reasonably likely to be used' to achieve such identification and in this context "account should be taken of all objective factors, such as the costs or the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments'. Anonymous information is not protected.

The processing of personal information must comply with the requirements of Article 5, which requires that all personal data processing be lawful, fair, transparent and limited to what is necessary (data minimisation) and that personal data are collected for specified, explicit and legitimate purposes, are accurate and, where necessary, kept up to date and in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Simultaneously, personal information must be processed in a manner that ensures appropriate security and the controller shall be responsible for and should

be able to demonstrate compliance with the requirements of the processing. 'Lawful' processing means processing based on either: a) Consent: the data subject has consented to the processor's use of their data for the specific purpose(s). The consent must also be free, unambiguous and informed (Articles 4 and 7); b) Contract: the processing is necessary for the processor's compliance with a contract with a data subject (or steps the data subject has asked the processor to take before entering a contract); c) Legal obligation: the processing is necessary for the processor to comply with a legal duty; d) Vital interests: the processing is necessary to protect someone's life; e) Public Interest: the processing is necessary for the processor to perform a public interest task with a clear legal basis; f) Legitimate interests: the processing is necessary for the processor's legitimate interests and these are not outweighed by the data subject's interests and rights (Article 6). Finally, the processing of sensitive data must satisfy certain additional criteria (Article 9).

The data subjects enjoys, according to the Regulation, certain rights in relation to his personal information, namely the right of information (Articles 12,13 and 14), the right of access (Article 15), the right to rectification (Article 16), the right to erasure (to be forgotten) (Article 17), the right to restriction of processing (Article 18), the right to data portability (Article 20), the right to object (Article 21) and the right not to be subject to a decision based solely on automated processing, including profiling (Article 22). In Article 23 the conditions under which these rights could be restricted are analysed and the obligations of the controllers/processors are regulated in Articles 24 and 30-35.

It is important to note that the purpose of data protection is considerably broader than privacy. According to Article 1, its purpose was rather secure for every individual 'respect for his rights and fundamental freedoms'. This same clause did emphasise that it was "in particular [the individual's] right to privacy" which deserved protection; however, several other internationally recognised rights linked to individuals are certainly covered. At the same time, it is important to remember that protection of personal data is not an absolute right and the idea of fair balance between data subject and data controller is also at the heart of the Directive. This aspect is linked to the focus on free flow of data as stated in Article 1(3): The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. Finally, pursuant to Article 288 TFEU, GDPR is directly applicable in all Member States Members, who are obliged to take the necessary measures for its adjustment of their national legislation.

What is more, at EU level, the 2002 e-Privacy Directive³³⁴ was issued (repealing the 1997 Privacy Directive) establishing privacy rights in relation to electronic communications and specific rules regarding the use of 'cookies. According to Article 1 of the Directive it 'harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the

³³⁴ e-Privacy Directive (2002/58/EC) OJ L 201/37.

Community'. It is useful to add that a new proposal for a regulation on the respect for private life and the protection of personal data in electronic communications (proposal for e-Privacy Regulation) has been published on 10 January 2017. It will replace Directive 2002/58/EC (e-Privacy Directive, as amended by Directive 2009/136) and specify the General Data Protection Regulation (GDPR). The objective of the initiative is to reinforce trust and security in the Digital Single Market, while providing flexible regulatory tools to enable innovation.³³⁵

2.3. Constitutional Protection

At national level, personal information is, first, protected- directly or indirectly- in several provisions of the Greek Constitution. More precisely, before the review of the Constitution in 2001, the protection of personal data was based on the protection of human dignity (Article 2 § 1), the protection of personality (Article 5 § 1), the protection of private and family life (Article 9 § 1 par. b) and the protection of confidential and free communication (Article 19 § 1). Article 19 refers to any form of communication (e.g., written, email) which the right holder wishes it to be confidential; the internet, however, is considered to be primarily a public form of communication and, thus, it is not covered by this provision. Right holders are only natural persons, who are constitutionally protected against insults by the state and public authorities. It is widely supported, nevertheless, that the constitutional provisions develop simultaneously an indirect horizontal legal effect on the relations between individuals and, as a result, civil and criminal law must be interpreted under their light.³³⁶

With the review of 2001, the more specific provision of Article 9A was introduced to the Greek Constitution. According to Article 9A, "everyone has the right to protection from the collection, processing and use, in particular by electronic means, of his personal data, as provided by law". The introduction of said Article followed the signing of Convention 108/1981 as ratified by Law 2068/1992 for Greek legislation to become harmonized with European Directive 95/46/EC. It is important to underline that it not only protects personal data related to private life, but also prohibits the collection, processing and use of all personal data, regardless of their content.³³⁷ The same article provided for the establishment and operation of an independent authority responsible to protect personal information, the 'Data Protection Authority', which is now one of the five independent authorities explicitly enshrined in the Constitution. The 2001 review also established as a constitutional independent authority the 'Authority for Communication Security and Privacy', which had first been established by Law 2225/1994 (then as the 'National Commission for the Protection of the Confidentiality of Communications').³³⁸

i. 2.4. Law 4624/2019.

In the Greek legal order, at common law level, the protection of personal data was initially secured with Law 2472/1997 on the 'Protection of the individual from the processing of

³³⁵ Proposal for a regulation on privacy and electronic communications, European Parliament, <<https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/a-europe-fit-for-the-digital-age/file/jd-e-privacy-reform>> accessed 2 February 2021.

³³⁶ Prodromos D. Dagtoglou, Constitutional Law, Human Rights, (fourth updated student version in Greek, Sakkoulas 2012), 277-278.

³³⁷ Ioannis D. Igglezakis, *Sensitive Personal Data* (Sakkoulas 2003), 57.

³³⁸ Dagtoglou (n 336), 293-299.

personal data', complying with the relevant Community Directive 1995/46 of the European Parliament and European Council dated 24 October 1995 'On the protection of individuals with regard to the processing of personal data and on the free movement of such data', which established for the first time specific rules for the protection of individuals with regard to the processing of their personal data. Following the adoption of the GDPR, Law 4624/2019 was issued, which incorporates into the national legal order the Directive no. 2016/680, for the protection of natural persons against the processing of personal data by the competent law enforcement authorities, while Directive 1995/46 (Article 1 of Law 4624/2019) and Law 2472/1997 are now explicitly repealed, subject to certain provisions (Article 84 Law 4624/2019). According to Article 1, L. 4624/19 applies to natural persons (not legal entities or deceased persons) and regulates the automated and not automated processing of personal data from public or private bodies (Article 2), with the exception of the processing of personal data by a natural person in the course of a purely personal or household activity (Article 2b). Article 3 clarifies that it applies *rationae loci* to all public bodies and private entities, if a) the controller or the processor processes personal data within the Greek Territory, b) the personal data are processed in the context of the activities of an establishment of the controller or the processor within the Greek Territory, or if c) although the controller or processor do not have an establishment in a Member State of the European Union or in another Contracting State of the European Economic Area, it falls within the scope of GDPR (see, for instance, Recitals 23 and 24 GDPR).

What is more, public authorities should designate a Data Protection Officer (Article 6) whose responsibilities are set out in Article 8 (e.g., to inform and advise the public body and the employees carrying out the processing, to monitor compliance with the provisions of this and any other legislation on the protection of personal data, etc.). According to Article 9 'the supervision of the application of the provisions of the GDPR, of the present and other regulations concerning the protection of the individual against the processing of personal data in the Greek Territory is exercised by the Authority (i.e., the independent Data Protection Authority) which enjoys personal, functional (Article 11) and financial independence (Article 19) and has powers of investigation, corrective powers and sanctions, and authorization and advisory powers (Articles 13 and 15). Nevertheless, 'the Authority is not competent to control the processing of personal data carried out by judicial and prosecutorial authorities in the context of their judicial functions and duties, as well as the processing of classified personal data carried out for reasons of national security' (Article 10.5). The powers of investigation, corrective powers and sanctions, and authorization and advisory powers that it enjoys are crucial for the successful application and have helped clarify important aspects of the legislation relating to the protection of personal information such as the right to be forgotten³³⁹, the notion of consent as legal basis for lawful processing³⁴⁰ etc. Equally important are the several advisory opinions and guidelines

³³⁹ E.g., Decisions 82/2016, 83/2016, 84/2016 Hellenic Data Protection Authority.

³⁴⁰ E.g., Decision 66/2018 Hellenic Data Protection Authority, the first decision applying the GDPR in Greece, Decision 26/2019 Hellenic Data Protection Authority on the lawfulness of consent in the context of professional relations, the first fine imposed following the GDPR provisions in Greece.

issued by the Data Protection Authority in matters relating to the protection of personal data, such as the guidelines relating to teleworking³⁴¹ and the guidelines on the processing of personal data in the context of the Covid-19 pandemic.³⁴² The Authority has also issued an Opinion on L.4624/2019 that deserves attention.³⁴³

More precisely, the Data Protection Authority underlined that some provisions of L.4624/2019 require further clarification or appear to be contrary to the GDPR. For instance, according to said Opinion, several provisions introducing exceptions from the data protection regime (e.g., Articles 24-28) lack legal basis and endanger the core of personal information protection as established in the EU legal order. At the same time, other provisions of L.4624/2019 constitute simple repetitions of the relevant Articles of the Regulation or the Directive, without clarifying, specifying or adapting them accordingly to the national legal order and, thus, violating the EU rule, which does not allow the replication of GDPR provisions in national law (e.g., Article 5).

Article 21 refers to the special conditions that apply in relation to the protection of personal information belonging to minors. Articles 22 et seq. contain more specific provisions regarding the protection of special categories of personal data. Article 22 provides that by way of derogation, the processing of sensitive data is allowed from public and private authorities for the exercise of rights deriving from the right to social security and social protection and for health / public health reasons, and from public authorities if (a) it is absolutely necessary for reasons of essential public interest; (b) it is necessary to prevent a significant threat to national security; or (c) it is necessary for humanitarian action. In the cases of the previous paragraphs, all appropriate and special measures are taken to safeguard the interests of the data subject, which may include the pseudonymization of personal data, the encryption of personal data, etc. The processing of genetic data for health and life insurance purposes is prohibited (Article 23). Whereas Articles 24 and 25 analyse when the processing of personal data for a different purpose than the purpose of their initial collection is allowed by public and private authorities accordingly (e.g., for the prosecution of criminal offenses, for the prevention of threats against national security or public safety).

Article 27 contains specific provisions for the protection of personal data in the context of a professional relation and, derogating from the relevant GDPR provisions, provides that: the processing of specific categories of personal data for the purposes of the employment contract is permitted, if necessary for the exercise of rights or the fulfillment of legal obligations arising from labor law, social security law and social protection and there is no reason to consider that the legal interest of the data subject compared to the interest in favour of processing is paramount. Article 28 deals with the processing of personal data which is the result of the right to freedom of expression and information, including processing for journalistic purposes and for the purposes of academic, artistic or literary expression and states that this is allowed under specific circumstances (e.g., the data subject has given his consent). By way of derogation from

³⁴¹ Guidelines for teleworking (15/04/2020), Hellenic Data Protection Authority.

³⁴² 5/2020 Guidelines for the processing of personal data in the context of COVID-19 (18/03/2020), Hellenic Data Protection Authority.

³⁴³ Opinion 1/2020 of the Hellenic Data Protection Authority.

Article 9 (1) of the GDPR, the processing of specific categories of personal data, shall be permitted when necessary for archiving purposes in the public interest (Article 29) or when it is necessary for the purposes of scientific or historical research or collection, and the keeping of statistics (Article 30). In both cases, the controller is obliged to take appropriate and specific measures to protect the legal interests of the data subject. The rights of the data subject to information concerning and access to his personal data are restricted in certain specific cases analyzed in Articles 31-33.³⁴⁴ The right to be forgotten of the data subject is also restricted in Article 34 and the right of objection (against a public authority) in Article 35.

It is important to note that with Articles 44 seq the provisions of said Directive regarding definitions, basic guidelines in relation to the processing of personal data, special categories of personal data, consent, the right to information, the right to access, the right to rectification, the right to data portability and the duties of the data controller or processor, have been specified and incorporated in the Greek legislation. Finally, the infringement of the rights of the data subject entail criminal (Articles 38 and 81) and administrative (Articles 39, 82) penalties. Any public authority, acting as a controller/processor of personal data, who has illegally caused damage to the data subject is liable for monetary compensation or compensation due to moral damage (Article 80).

ii. 2.5. Law 3471/2006.

The e-Privacy Directive (2002/58/EU) was incorporated to the Greek legal order with Law 3471/2006 on the “Protection of personal data and privacy in the field of electronic communications”. According to Article 1: The purpose of the provisions of Articles 1 to 17 of this Law is to protect the fundamental rights of individuals and in particular the right of privacy and to establish the conditions for the processing of personal data and the confidentiality of communications in the field of electronic communications. Article 2 contains similar definitions to Article 2 of said Directive, including the definitions of ‘traffic data’ as ‘data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof; including number, address, login or terminal identity of the subscriber or user, passwords’ etc. and ‘location data’ as any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. Electronic communications services are defined as services normally provided for a fee and consist, in whole or in part, of the transmission of signals on electronic communications networks, including telecommunications services and broadcasting services used for broadcasting networks. Law 2472/1997 (A`50), as in force, applies to the processing of personal data carried out in the context unavailable to the public electronic communications networks and services (Article 3 par.1).

Furthermore, the violation of personal data is defined as: ‘violation of security leading to accidental or unlawful destruction, loss, alteration, unauthorized dissemination or access of personal data transmitted, stored or otherwise processed in connection with publicly available electronic communications service’. According to Article 4: Any use of electronic

³⁴⁴ E.g., it would endanger national or public security (Articles 31c, 32bb).

communications services provided through a public communications network and the availability of electronic communications services to the public, as well as related traffic and location data, as defined in the provisions of Article 2 of this law, is protected by the confidentiality of communications. The removal of secrecy is permissible only under the conditions and procedures provided for in Article 19 of the Constitution and under some other exceptional circumstances, such as:

- in par.3: It is permitted to record conversations and related traffic data, when carried out during a lawful professional practice for the purpose of providing evidence of a commercial transaction or other professional communication, provided that both parties are notified in advance and they provide their consent.
- In par.4: Subject to compliance with the obligations arising from the protection of confidentiality, in accordance with this law, the storage of technical nature, which is necessary for the transmission of the communication, is allowed
- In par.5: The storage of information or access to information already stored on the subscriber's or user's terminal equipment is permitted only if the subscriber or user has given his / her consent.

The processing of personal information must be the absolutely necessary and it is permitted only if: a) the subscriber or the user, after being informed of the type of data, the purpose and extent of the processing, the recipients or the categories of recipients has agreed, or b) the processing is necessary to execute a contract in which the subscriber or user is a party, or to pre-contractual stage, at the request of the subscriber (Article 5).

Regarding traffic data it is provided that: Traffic data, which are processed and stored by the provider of the public network or publicly available electronic communications service, upon the termination of the communication are destroyed or become anonymous, without prejudice to Law 3917/2011 (A`22), as well as paragraphs 2 to 6 of this Article (Article 6.1). Regarding location data it is provided that: Data indicating the geographical location may be processed only after they are rendered anonymous or with the consent of the data subject and for the duration required to provide a value-added service. (Article 6.4). Exceptionally, without the prior consent of the subscriber or user, the processing of location data by public service providers or publicly available electronic communications service may be provided to emergency authorities, such as first aid and fire services, the necessary information for the location of the caller and only for this specific purpose (Article 6.5).

What is more, Article 8 incorporates Article 8 of the Directive in relation to the presentation and restriction of calling and connected line identification. Article 9 regulates after Article 11 of the Directive the automatic call forwarding. Article 10 incorporates Article 12 of the Directive regarding directories of subscribers and Article 11 regulates the unsolicited communication as laid down in Article 13 of the Directive. Article 12 specifies that the electronic communications services provider must take the appropriate technical and organizational measures to protect the security of its services as well as the security of the public electronic communications network. These measures, if necessary, shall be taken jointly with the provider of the public electronic

communications network and shall guarantee a level of security commensurate with the existing risk, considering the most recent technical possibilities and the cost of their implementation. In case of violation of personal data, the provider of electronic communications services available to the public shall immediately notify the ‘Data Protection Authority’ and the ‘Authority for Communication Security and Privacy’ (par.5). When the breach of personal data may have an adverse effect on the personal data or privacy of the subscriber or another person, the provider shall also promptly inform the affected subscriber or the affected data subject (par.6).

According to Article 13 ‘the responsible Independent Authorities that oversee the application of the provisions of this law are the Data Protection Authority and for Authority for Communication Security and Privacy. An opinion of the Hellenic Telecommunications and Post Commission is also necessary for certain relevant issues. Finally, both supervisory Independent Authorities can impose administrative sanctions. Violation of the provisions of L.3471/06 also entails civil liability (full compensation and compensation of moral damages) (Article14) and criminal liability (Article15).

2.6. Protection in the Greek Civil Code

Personal information is also protected in the Civil Code, with a general action for the protection of one’s personality against any ‘unlawful’ intrusion, invasion, or infringement. More precisely, article 57 provides for the protection of personality: ‘a person who has suffered an unlawful infringement on his personality has the right to claim the cessation of such infringement as also the non-recurrence thereof in the future. A claim for compensation, according to the provisions about tort, is not excluded’. The Greek Civil Code does not define the exact perimeters of the concept of personality. It is generally said that personality encompasses all the tangible and intangible elements, which constitute one’s physical, emotional, intellectual, moral, and social existence. The notion of ‘personality’ also includes, therefore, personal information that an individual has the exclusive right in relation to their processing and communication.³⁴⁵ It must be noted that the right of article 57 is a personal right attributed solely to the data subject. Others who are linked with the data subject and are, thus, indirectly offended by the infringement of the personality right are not granted protection.³⁴⁶

As mentioned above, the infringement of the personality right gives rise to a claim for the cessation of such infringement and for its non-recurrence in the future (article 57 par. 1.a), to a claim for compensation under the provisions about torts (Art.75 par.2) and to an action for the satisfaction of moral damage of the person whose right was infringed (Article 59). Simultaneously, the offended party has the right to ask for a declaratory relief (article 70 of the Code of Civil Procedure) and for the adoption of interim measures (articles 682 et seq Code of Civil Procedure), which often provide for a more efficient protection.³⁴⁷ Every infringement of the right is unlawful, unless certain other conditions apply, for example, when there is valid consent of the data subject or when it is the result of the enforcement of another right. In the

³⁴⁵ Apostolos S. Georgiadis, *General Principles of Civil Law* (4th eds, Law & Economy-PN. Sakkoulas 2012) 175.

³⁴⁶ *ibid*, 176.

³⁴⁷ Georgiadis (n 345), 182.

latter case, there is an ad hoc examination of the competing rights in question for the Court to conclude ad hoc on the unlawfulness.³⁴⁸

It is useful to add that apart from the protection of the personality of natural persons, article 57 also covers - up to a certain extent, i.e., as far as it is compatible with their nature - the 'personality' of legal entities too.³⁴⁹ Moreover, the right to personality, as a personal right, terminates with death (article 35 of the GCC). However, the GCC also provides for the protection of the memory of a deceased person (article 57 par 1b). The claim may be filed by any close relative of the deceased person against anyone violating their memory demanding the cessation of the offence, its non-recurrence in the future, compensation as well as moral damages. No time limit exists under Greek law for the protection of the right.

Finally, in the context of a contractual relationship, the general principles of Civil Law, i.e., good faith and honest commercial practices (articles 197,198,288 of the Civil Code) impose, among others, the obligation of confidentiality at both pre-contractual, contractual and post-contractual stage.

2.6. Protection in the Greek Criminal Code

Personal information is also protected in several provisions of the Greek Criminal Code. To begin with, the Greek Criminal Code protects a person's honor and reputation under articles 361 to 367. Article 361 provides that a person who, by words or acts, injures another's reputation shall be punished by imprisonment or pecuniary penalty. Article 362-363 provide that a person who alleges or disseminates information that may harm another's honor or reputation shall, also, be punished by imprisonment or pecuniary penalty. If the information is untrue and the responsible party knows it or the untrue information is disseminated in public, e.g., via the internet, the penalty is heavier (Article 363). Article 366 contains the exceptions under which the acts of article 362 are not unlawful (e.g., if the information of article 362 is true, the act goes unpunished, unless it concerns only family or private relations that do not affect the public interest), whereas Article 367 contains certain other exceptions that render the aforementioned acts lawful.

With the recent review³⁵⁰ of Criminal Code, the protection of data through criminal sanctions because of the violation of the right to privacy and secrecy of communications, was reinforced (Chapter 22, articles 370 et seq). The influences from the General Regulation of Personal Data Protection are obvious. More precisely, Article 370, is modernized and expanded, so that the offense of the violation of the privacy of postal communication now contains the unlawful and illegal access to another's electronic communication (e-mail), even setting a distinct type of infringement committed by a person having a special capacity, i.e., employee of an organization or company providing postal, telegraphic or electronic services. Article 370A regulates the consequences of violating the confidentiality of telephone communication and oral conversation. Even more specific forms of violation are regulated in the following provisions: Article 370 B (illegal access to information or data systems), Article 370C (misappropriation / copying of state,

³⁴⁸ *ibid* 178.

³⁴⁹ *ibid* 177.

³⁵⁰ Law 4637/2019.

scientific and professional secrets, etc.), Article 370D (copying of computer programs and personal information contained in them, etc.), and Article 370E (monitoring and recording data transmissions, electromagnetic emissions, interferences for the purpose of information, etc.).

Other provisions of the penal code relating to the protection of personal information are Article 241 'Violation of the right to residential asylum' and Article 292 A 'Crimes against the security of telephone communications'.

A relevant issue regarding the protection of personal information, and more specifically the protection of the communication of personal data, is the regulation within the Criminal Code of official and professional secrecy. Official secrecy is a type of public secrecy, which is the responsibility of public bodies and officers in the exercise of public authority or function. Judicial and tax secrecy are considered types of official secrecy. Examples of the regulation of official secrecy are Articles 251 Criminal Code 'Violation of judicial secrecy' and Article 252 Criminal Code 'Violation of official secrecy by an official who, in breach of his duties, discloses to another confidential entrusted to him or known to him because of his service'. Furthermore, Article 371 Criminal Code regulates the professional secrecy for various categories of employees, such as e.g., lawyers, doctors and other officials or professionals, who are usually trusted with private information because of their profession or capacity.

Finally, in addition to the Criminal Code, official/professional secrecy is regulated by several other laws. Typical examples are the Banking Secrecy which is regulated mainly by Law 1059/1971 (as amended). Banking secrecy is defined as the obligation of professional secrecy by banking institutions in relation to all kinds of transactions and relations (personal and financial) of the customer with the bank.³⁵¹ Other similar examples of provisions regarding professional secrecy are for lawyers article 32 of the Code of Conduct of Lawyers, for pharmacists' article 13 of the Code of Greek Pharmaceutical Ethics etc. In fact, the Code of Criminal Procedure in article 212 prohibits the examination of certain categories of witnesses who are bound by this obligation of secrecy.

2.7. Protection of personal information in the context of judicial proceedings

Personal information is also protected in the context of civil, criminal, or administrative proceedings. On a constitutional level, according to Article 19 par.3: 'The use of evidence obtained in violation of this article and articles 9 and 9A is prohibited'. This provision is reflected in Article 177 par. 2 of the Code of Criminal Procedure: 'Evidence obtained because of an act that is a criminal offense is not considered in criminal proceedings'.

These provisions, nevertheless, conflict with other constitutionally protected rights and, more specifically, with article 20 par. 1 of the Constitution which provides for effective judicial protection. The right to privacy/protection of private information is therefore not absolute, but like any other constitutional right, can be restricted.³⁵² As a result, both jurisprudence and the case law accept that, in the context of criminal proceedings, the prohibition of Article 19 par. 3, must be interpreted in accordance with the principle of proportionality and in favor of the

³⁵¹ Spiros Psychomanis, *Banking Law, Law of Banking Contracts* (5th eds, Sakkoulas 2001), 195.

³⁵² Dagtoglou (n 336), 133 et seq.

defendant, when this evidence is the only evidence capable of proving his innocence. It is the court that must proceed ad hoc to this evaluation.³⁵³ In relation to civil proceedings, again both the theory and the case law, seem to be in favor of the permissibility, in certain cases, of the use of illegal evidence.³⁵⁴ Following the position of the Data Protection Authority that the use before the court of personal data collected without the prior consent of the person concerned is legitimate if the intended purpose of the protection of rights cannot be achieved by other more lenient means, it has been established that the use of personal information obtained unlawfully is only permitted when it is absolutely necessary in an effort to secure a balance between the right to personal data protection and the right to judicial protection.³⁵⁵

The protection of personal information is also linked with the regulations that place restrictions on the rule of the ‘publicity of the trial’. Article 93 par.2 of the Constitution provides that: ‘The hearings of each court are public, unless the court decides that this publicity is contrary to the accepted principles of morality or that there are special reasons for protecting the private or family life of the parties’. Pursuant to Article 93, similar exceptions for the purpose of protecting personal information can be found in article 330 of the Code of Criminal Procedure and in article 37 of the Code of Administrative Procedure.

It is important to add that according to Article 9f of the GDPR processing of sensitive personal data is allowed when it “is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity”. Even though Art.9 refers only to special categories of data it is accepted that the same provision applies also in relation to regular personal data.

2.7. Protection of personal information and Media (Freedom of the Press)

Of significant theoretical and practical importance is the issue of restrictions on the freedom of the press arising from the protection of privacy and personal data, rights which are infringed whenever personal data is disclosed without the consent of the person concerned. The freedom of the press is enshrined in Article 14 of the Greek Constitution. However, this freedom is subject to certain restrictions and does not include, for instance, the freedom to disclose legally protected secrets.³⁵⁶

Private individuals, who have not entered the public domain, in principle enjoy greater protection of their privacy rights. Some of their actions, nevertheless, may take them into the public sphere, which is why journalists can under circumstances report about them, even without their consent. Public figures inevitably and knowingly lay themselves open to scrutiny by both journalists and the public. Their right to keep their private life protected is therefore more restricted. Certain private actions of public figures can also be regarded as public on account of their potential wider impact and of the public’s interest in being informed.³⁵⁷

³⁵³ E.g., Decision 653/2013 Areios Pagos Supreme Civil and Criminal Court of Greece.

³⁵⁴ E.g., Decision 1/2017 Areios Pagos Supreme Civil and Criminal Court of Greece

³⁵⁵ Newlaw, ‘Παράβιαση Προσωπικών Δεδομένων με Παράνομα Αποδεικτικά Μέσα; Τώρα Γίνεται’ [2017] Newlaw.gr <https://www.newlaw.gr/gr/cms_articles/art_new?id=207> accessed 4 February 2021.

³⁵⁶ Dagoglou (n 336), 425-427.

³⁵⁷ Guidelines on safeguarding privacy in the media, Council of Europe (2019), 12-13.

Law No. 1178/1981 (applying to printed and electronic media) introduces strict liability for content providers for libelous content, produced by a third person, usually an employee, that is disseminated through newspaper, magazine, or electronic media. According to paragraph 1 of the law, the owner of a mass medium is obliged to fully indemnify the unlawful pecuniary and moral damage that is culpably caused by a publication offending the honor or the reputation of any person, even if the culpability of the unlawful act can be attributed only to the writer, newscaster or TV presenter. Hence, if such content also violates the right of publicity, publishers or media content providers could be held liable according to the above-mentioned provisions. Special penal laws for media liability were abolished in 1994.

A relevant decision of the European Court of Human Rights concerned the infringement of the privacy right. In *Reklos and Davourlis v. Greece*, taking pictures of a new-born baby without the consent of his parents (in the intensive unit to which only hospital staff should have had access) was considered to be a violation of the right to privacy even though the pictures were not published.³⁵⁸

2.9. Best practices/guidelines

In addition to the adoption of specific Directives, EU efforts have also concentrated on issuing codes of best practices and guidelines aiming to protect personal information more efficiently. Namely, two such instruments are the ‘Guidelines on Safeguarding Privacy in the Media’³⁵⁹ and the ‘Guidelines on artificial intelligence and data protection’.³⁶⁰ The ‘Guidelines on Safeguarding Privacy in the Media’ comprise a collection of standards of the Council of Europe and the European Court of Human Rights concerning the protection of privacy of public figures and private individuals in the media including as well data protection principles based on various regulatory instruments and best practices, which ‘target journalists and other media professionals and aim to help them with the practical application of the mentioned standards to the individual ethics-related dilemmas’.³⁶¹ The ‘Guidelines on artificial intelligence and data protection’ propose various measures that should be respected in the field of AI in order ‘to ensure that AI applications do not undermine the human dignity and the human rights and fundamental freedoms of every individual, in particular with regard to the right to data protection’.³⁶² These guidelines are considered valuable advice-giving tools which could help both individuals (e.g., service providers, AI developers, journalists) and governments better understand and enforce data protection.

At a national level, apart from the legislative efforts to establish a comprehensive regulatory framework regarding personal information and, with the same objective as the numerous European guidelines/codes of practices, national codes of practices have been issued. One such example constitutes the Study/Guidelines of the Hellenic Federation of Enterprises focusing on two main issues: a) presenting the key points of the GDPR Regulation and (b) guiding

³⁵⁸ *Reklos and Davourlis v. Greece*, No. 1234/05, 15 January 2009 ECOHR.

³⁵⁹ Guidelines (n 357).

³⁶⁰ Guidelines on Artificial Intelligence and Data Protection, Council of Europe (2019).

³⁶¹ Guidelines (n 357), 5.

³⁶² Guidelines (n 360), 7.

companies in their compliance efforts and in taking advantage of the opportunities presented by the Regulation.³⁶³ The Code of Conduct for the processing of personal data by Lawyers, Law Firms and Bar Associations is also under review and will be issued shortly. In brief, the Code aims, pursuant to article 40 GDPR, to adapt and to specify the rules, principles and obligations contained in the General Regulation of Data Protection and Law 4624/2019, in the context of the exercise of the legal profession, contributing, thus, to their correct application.³⁶⁴

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?

The data protection is self-regulated by the private and public sector to a great extent in Greece. Many companies in the private sector create their own Binding Company Rules, like “Code of Conduct for the processing of personal data”, which clearly define the specific details of their operation according to the data protection. Key legislation of these “Codes of Conduct” is the European General Data Protection Regulation (EU GDPR) 679/2016 and the National Legislation of 4624/2019 about personal data.

3.1. Definitions

Binding Company Rules (BCRs) are internal rules (such as a Code of Conduct) adopted by multinational corporate groups, that define their global policy regarding the international transfer of personal data within the same group to entities located in countries which do not provide an adequate level of protection.

Code of Conduct is prepared by a business association which has been approved by a Data Protection Authority. A Code of Conduct may be given EU-wide validity through an implementing act of the Commission.

Certification mechanism is operated by one of the certification bodies that have received accreditation from a Data Protection Authority or a national accreditation body or both, as decided in each EU Member State. Both codes of conduct and certification are optional instruments and therefore it is up to the company or the organization to decide whether to adhere to a given code of conduct or to request certification.³⁶⁵

The Binding Company Rules are used by multinational corporations to provide adequate safeguards and to protect the privacy and fundamental rights and freedoms of individuals in all transmissions of personal data protected under European Law. To this extent, these rules ensure that all data transfers within the group enjoy an adequate level of protection and are an

³⁶³ The new General Regulation for Data Protection (GDPR), Application and challenges for business in the age of digitization, Hellenic Federation of Enterprises (SEV) (2018), p.171.

³⁶⁴ ‘Προσωπικά δεδομένα και δικηγόροι: Σε διαβούλευση ο Κώδικας Δεοντολογίας για την επεξεργασία δεδομένων από Δικηγόρους, Δικηγορικές Εταιρείες και Δικηγορικούς Συλλόγους’ [2020] Lawspot.gr <<https://www.lawspot.gr/nomika-nea/prosopika-dedomena-kai-dikigoroi-se-diavoyleysi-o-kodikas-deontologias-gia-tin>> accessed 10 February 2021.

³⁶⁵ European Commission, ‘How can I demonstrate that my organisation is compliant with the GDPR?’ <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/how-can-i-demonstrate-my-organisation-compliant-gdpr_en> accessed 10 February 2021.

alternative solution for groups, instead of signing standard contractual clauses whenever data needs to be transferred to one of their members. Once adopted in the framework of the European Union cooperation process, the rules provide a sufficient level of protection for companies to obtain approval for the transmission of data from the competent national authorities Data Protection Authorities.

3.2. Advantages of Binding Company Rules

The advantages of Binding Corporate Rules are that all data transmissions within the group covered by the scope of the rules:

- harmonizing practices on the protection of personal data within a group,
- preventing the risks arising from the transfer of data to third countries,
- avoiding the need to draw up a new contract for each transfer made,
- the transparency of the company's personal data protection policy,
- the existence of an internal guide for employees in relation to the management of their personal data,
- the integration of data protection as an integral part of the way in which the company conducts its activities.³⁶⁶

3.3. Transport of data outside the European Union

Especially if an organization transfers data outside the EU, an option is the adherence to a code of conduct or certification mechanism together with obtaining binding and enforceable commitments from the recipient to apply the appropriate safeguards to protect the transferred data.

There are large amounts of cross-border transfers of personal data, which are sometimes stored on servers in different countries. The protection offered by the General Data Protection Regulation (GDPR) travels with the data, meaning that the rules protecting personal data continue to apply regardless of where the data lands. This also applies when data is transferred to a 'third country', a country which is not a member of the EU.

The GDPR provides different tools to frame data transfers from the EU to a third country:

- sometimes, a third country may be declared as offering an adequate level of protection through a European Commission decision ('Adequacy Decision'), meaning that data can be transferred with another company in that third country without the data exporter being required to provide further safeguards or being subject to additional conditions. In other words, the transfers to an 'adequate' third country will be comparable to a transmission of data within the EU.
- in the absence of an Adequacy Decision, a transfer can take place through the provision of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals. Such appropriate safeguards are included:

³⁶⁶ 'Δεσμευτικοί Εταιρικοί Κανόνες (Binding Corporate Rules)' [2015] Lawspot.gr <<https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/desmeytikoi-etairikoi-kanones-binding-corporate-rules>> accessed 11 February 2021.

- in the case of a group of undertakings, or groups of companies engaged in a joint economic activity, companies can transfer personal data based on so-called binding corporate rules.
- contractual arrangements with the recipient of the personal data, using, for example, the standard contractual clauses approved by the European Commission.
- adherence to a code of conduct or certification mechanism together with obtaining binding and enforceable commitments from the recipient to apply the appropriate safeguards to protect the transferred data.
- finally, if a transfer of personal data is envisaged to a third country that isn't the subject of an Adequacy Decision and if appropriate safeguards are absent, a transfer can be made based on a number of derogations for specific situations for example, where an individual has explicitly consented to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer.³⁶⁷

3.4. Procedure for creation of Codes of Conduct

The codes of conduct are set out in Article 40 of the GDPR and are intended to facilitate the effective implementation of the GDPR by regulating the specific obligations of both controllers and processors for specific areas of activity. Therefore, codes of conduct are not developed by individual controllers or processors, but by associations or other entities representing categories of controllers or processors. Therefore, this concept of the Code of Conduct in Article 40 of the GDPR is different from any other Code of Conduct already established by a controller for the processing of personal data which he carries out.

Codes of conduct are not mandatory but optional. However, the Authority clearly encourages their elaboration, in the sense that they may constitute a set of specific rules / practices to comply with the general conditions for the lawful processing of personal data set by the GDPR, taking into account the specific characteristics of the various processing sectors (recital 98).

When drawing up a code of conduct or amending or extending such a Code, associations and other bodies representing categories of controllers or processors should consult stakeholders, including data subjects, where applicable. It is possible to consider all the comments submitted, and the views expressed in this consultation. Other elements that are considered when compiling a code are described in article 40 par. 2 GDPR.

The draft of such a code must be submitted to the Authority, which will give an opinion on whether the code is in line with the GDPR and approves it, if it considers that it provides sufficient guarantees.

In addition, in accordance with Article 83 (2) GDPR when deciding on the imposition of an administrative fine, as well as on the amount of the administrative fine for each individual case, due regard shall be paid, inter alia, to the adoption of approved codes of conduct.

³⁶⁷ European Commission (n 365).

When the draft code or its amendment or extension is approved and when the relevant code of conduct is not related to processing activities in more than one Member State, the Authority shall register and publish the code (Article 40 (6) GDPR). Where the Code relates to processing activities in more than one Member State, the procedures described in paragraphs 7, 8 and 9 of Article 40 of the GDPR shall be followed.

A code of conduct should include mechanisms that allow a specific independent body - having the appropriate level of expertise in the subject matter of the code - to monitor compliance with its provisions by controllers or processors that have undertaken to implement it.

It is noted that this body ('monitoring body') must be specifically accredited by the Authority. The monitoring bodies have specific obligations in case they find a violation of the code (article 41 par. 5 GDPR). The Authority may revoke the accreditation of a monitoring body at any time, if it considers that the criteria based on which it was accredited, are no longer met or if the body does not comply with its obligations.

The Code of Conduct for the monitoring body does not apply to the processing carried out by public authorities and public bodies, for which there is no need for a monitoring body. However, in any other case of a code of conduct, it must be monitored by an independent monitoring body - and therefore the code of conduct to be submitted for approval should have a provision to that effect.

The Authority, by Decision 9/2020, decided to define requirements for the accreditation of monitoring bodies, as defined in Article 41 of the GDPR, and which relate to a code of conduct for which the Authority is responsible in accordance with Article 55 of the GDPR.

The final requirements of the Authority for the accreditation of the bodies monitoring the codes of conduct, as amended based on the decision 20/2020 of the GDPR, are published by the Authority by publication on its website, in accordance with article 57 par. 1 of the GDPR and with article 15 par. 10 of law 4624/2019.

If the draft code of conduct concerns the processing of personal data in different Member States, then the association that forms it submits it to a competent supervisory authority (documenting why that supervisory authority was deemed competent). The competent supervisory authority then submits the draft, prior to its approval, to the European Data Protection Council, which gives an opinion on the compliance of the draft with the GDPR.³⁶⁸

3.5. Paradigms of Codes of Conduct and Data Protection policies in Greek public and private sector

Furthermore, many companies and many public and private organizations have their own Data Protection Policies, which determine their regulation. Few paradigms are banks and financial companies, medical associations, insurance companies, media companies, public entities like Municipalities etc.

3.5.1. Code of Conduct in the banking system

³⁶⁸ Data Protection Authority, Κώδικες Δεοντολογίας <https://www.dpa.gr/el/foreis/kwdikes_deodologias> accessed 2 February 2021.

According to Article 40 of GDPR “The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.”

The article 40 of GDPR gives the opportunity to associations of similar companies to draw up Codes of Conduct to facilitate the effective implementation of GDPR. Moreover, the drawing up of a Code of Conduct determines the specific characteristics and requirements of the operation of these companies. *Mutatis mutandis* there is a “Code of Conduct”, which enacts legal framework about the specific characteristics and requirements about the operation of banking system and financial enterprises.

As a result, the Code of Conduct about banking systems is a guarantee of transparency and security of personal data of clients and third parties. Basic principles of accountability, responsibility and transparency are adopted. There is no contract of the banking system, which hasn't got the minimum security of personal data, that is defined by the Code of Conduct of Banking system. The contracts which define a higher level of security of personal data of their clients are remaining strong, but if there is legislation gap about personal data this will be covered by the articles of Code of Conduct of Banking System.

Credit institutions which operate legally in Greece, may be subject to that Code of Conduct or have their registered office in Greece, including cooperative banks, either these are branches of foreign credit institutions that operate in Greece, as well as the Deposits Fund and Loans, if they send a relevant written declaration of accession in this Code of Conduct.

The Code of Conduct in banking systems is revised at least once in two years. It determines the purposes of the processing, crime detection and prevention through recording with cameras and audit trails, but it is ensured that the employees' work will not be evaluated by the bank through the cameras. Strict controls are vital to be conducted because of prevention and repression of money laundering from criminal activities and terrorist financing.

Minimum time of processing

Personal data is kept for the time required to fulfill the purpose of their processing, otherwise for the minimum time required by the current legislation that governs the operation of credit institutions and in any case for no more than (20) twenty years from the expiration of the contract or transaction, which is the time of the general limitation period according to article 249 of the Civil Code of claims.

Automated processing- Profiles' creation

When an automated decision is fully received by a profile, prior consent is not required of the client - subject if this is necessary for the drawing up or executing the contract. However, the subject has the right to express an opinion on the decision and to challenge it, as well as ensure that the credit institution reviews the case with human intervention.

Cross-border transfer of personal data by credit institutions to third countries or international organizations

Cross-border transfer of personal data by credit institutions to third countries or international organizations is allowed, without the need for a special permit, if there is a decision of European Commission, according to which adequate level of protection by the third country or by a specific third party sector country or by the international organization is ensured. This, among other things, applies to recipients participating in the "EU-US Privacy Shield" in the USA, under more specific conditions laid down in the relevant adequacy decision of European Commission. In the absence of an adequacy decision of the European Commission, the credit institution may transmit personal data in third countries or international organizations only if the credit institution, before the transmission, has provided the appropriate guarantees and effective remedies for their protection, such as the right to exercise effectively administrative or judicial action and claim for compensation, on the third country. These appropriate warranties may consist of the use of a legally binding instrument between public authorities, binding corporations rules, standard contractual data protection clauses that are adopted by or approved by the European Commission, or contractual clauses, certification mechanisms and codes of conduct approved by a competent supervisory authority.

Credit institutions can enter binding company rules with their subsidiaries in third countries, for international transfers to their group companies, which exercise joint economic activity. These company rules are approved by competent supervisory authority and must comply with its requirements Regulation.

Enacting a Code of Conduct is not mandatory but the Personal Data Protection Authority encourages organizations to develop Codes of Conduct, considering the specific characteristics of the different processing sectors (Recital 98 GDPR). Codes of conduct are not drawn up by individual controllers or processors, but by associations or other entities representing categories of controllers or processors.

The draft of such a code should be submitted to the Authority, which shall issue an opinion on whether the code is in line with the GDPR. Compliance with approved codes of conduct by controllers or processors shall be duly considered during the Data Protection Impact Assessment (DPIA).³⁶⁹

3.5.2. ERT Public Media

Public Media of Greece which is constituted by the channel ERT has its own Code of Conduct which is being revised annually. This code applies to all employees, heads of departments, independent partners, including suppliers and contractors of the company. It presupposes the periodic education and the complete knowledge of the present text, but also the understanding of compliance. Any third parties related to the Company, in the context of its business activity, must recognize and accept this code and its basic principles.

ERT does not engage in activities with competitors and suppliers that impede fair competition. In the context of corporate social responsibility and charitable-cultural activities of the company, ERT subsidizes with transparency, avoiding supporting illegal activities.

³⁶⁹ *ibid.*

ERT carries out internal audits / inspections three times a year for the compliance of the Company with the General Regulation of Data Protection. The inspections are carried out by the Data Protection Officer, an Administrative Officer appointed by the Chief Executive Officer and two executives from the Legal Service and the IT, respectively.³⁷⁰

It is ensured that external partners, suppliers, consultants and contractors are suitable for cooperation through a Data Processing Contract, this relationship is regulated under the jurisdiction of the Greek courts and under the requirements of the Code of Conduct, our corporate policies, the General Regulation Data and related laws.

The Code of Conduct ensures that any discrimination is forbidden in the working environment.

3.5.3 Ministry of Development & Investment

The website www.mindev.gov.gr belongs to the Ministry of Development & Investment. This website, through its technologically advanced web infrastructure and open source software applications, offers information services and technological applications of the Ministry of Development & Investment under the following terms of protection of personal data.

During the visit of the user / visitor of the websites of the Ministry of Development & Investment, it may be required to provide his/her (personal) data (name, occupation, email address, date of birth, etc.) in order to activate corresponding services of the website (periodic online updates, contests, sending information material to mobile phones and / or fixed electronic media etc. Therefore, personal data (e.g. usernames, etc.) that appear anywhere on the websites and services of the website of the Ministry of Development & Investment are intended solely to ensure the operation of the respective service and may not be used by any third party.³⁷¹

3.5.4 Data Protection Policies of the Region of Central Macedonia

It informs the visitors of the website about the basic terms and roles of GDPR and clarifies that the legal basis for the processing of personal data is consent when visiting the website and when collecting email addresses, as well as when using the contact form. It determines the time of processing and that the data are automatically deleted after 6 months. The contact details are deleted after the request of the subject of personal data.³⁷²

3.5.5 Data Protection Policies of the Ministry of Digital Governance

The Ministry of Digital Governance, processes the following personal data: 1) IP address, which is assigned to the device with which the "user" connects to the "service", 2) Navigation data within the "website" through the installation of data mining programs type "cookies", 3) Timestamp of the use of the "service", 4) Connector components (operating system, browser software).

³⁷⁰ Greek Public Radio and Television, Κώδικας Δεοντολογίας Δεδομένων
<<https://www.ert.gr/kodikas-deontologias/>> accessed 2 February 2021.

³⁷¹ Ministry of Development and Investments, Data Protection Policy
<<http://www.mindev.gov.gr/politiki-prostastias-dedomenon/>> accessed 2 February 2021.

³⁷² Region of Central Macedonia, Data Protection Policy
<<http://www.pkm.gov.gr/default.aspx?lang=el-GR&page=945>> accessed 2 February 2021.

The set of information contained in the document (application or responsible statement or authorization) submitted by the "user".³⁷³ The "Cookies" type files used on the website do not collect information that identifies users personally and do not access any document or file from the users' computer. The personal data is stored in the Public Cloud (G-Cloud).

3.5.6. Data Protection Policies of Newspapers

Newspaper websites define in detail in the Data Protection Policies of their Personal Data the use of cookies as well as the types of cookies they use, but also the rights of the data subjects.³⁷⁴

3.5.7. Insurance Companies

The Insurance Companies create profile compilation of their clients, according to General Data Protection Regulation. The company prepares profiles for the analysis of the aspects of the subjects that concern the evaluation of their performance at work, their financial situation, health, their personal preferences, their interests, their reliability, their behavior, their movements, in order to deal more effectively with the case they assign to the company but also for promotional actions or for reasons of social decency.³⁷⁵

3.5.8. Medical Association

To be able to provide more directly the services desired by the users of this forum, Medical Association may share their personal data with the following recipients:

Forum hosting providers, Security technicians and security service providers only in specific cases, Companies approved by the subject of data, such as social networking sites.

Personal information posted on the forum by users or affiliate applications may be made available online over the world. The present forum and subsequently the Medical Association are unable to prevent the use or misuse of this information by other persons. In any case, the transfer to third countries will be made in accordance with the conditions of the Regulation.³⁷⁶

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

The right of data privacy is protected in the Greek Constitution in the Article 9A, since the constitutional review of 2001. It states that "all persons have the right to be protected from the collection, processing, and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law". Before its separate definition and provision, the protection of personal data was based on either article 9 para. 1 (protection of private life of a

³⁷³ Digital Gate of Public Administration (gov.gr), Data protection Policy <<https://www.gov.gr/info/politiki-aporritou>> accessed 2 February 2021

³⁷⁴ Tovima.gr, Data Protection Policy <<https://www.tovima.gr/politiki-prostasias-dedomenon-prosopikou-xaraktira/>> accessed 2 February 2021.

³⁷⁵ Life's easy service Ltd., Code of and Data Protection Policy <<https://www.lifes.gr/wp-content/uploads/2018/06/Private-Policy-GDPR.pdf>> accessed 2 February 2021.

³⁷⁶ Panhellenic Medical Association, Data Protection Policy <https://forum.pis.gr/privacy_terms> accessed 2 February 2021.

person) or article 5 (free development of a person's personality) -or on a combination of them- of the Greek Constitution.³⁷⁷

The right to restriction of processing and the right to object to data processing are only a few of the most fundamental rights of any individual under the personal data protection legislation.

Regarding the restriction of the data processing, the data subject has the right to restriction of processing, enshrined in article 18 of the GDPR. According to article 18, there are only a few cases, in which the data subject can obtain the restriction of data processing and these include: 'the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims; the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject'. However, 'where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State'. Hence, important exceptions from the right to restrict the data processing are enshrined in the GDPR.

Concerning the objection to the data processing, the data subject has this right under article 21 of the GDPR. Against this background, the data subject 'shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications'. Nevertheless, 'where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is

³⁷⁷ Grigoris Lazarakos, 'The right to the protection of personal data against the unlawful processing of personal data' in Spyros Vlachopoulos (ed), *Fundamental Rights* (1st edn, Nomiki Bibliothiki 2016).

necessary for the performance of a task carried out for reasons of public interest'. Thus, significant exceptions from the right to objection are recognized as well.

Article 23 of the GDPR provides that restrictions on these rights may be imposed 'when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: national security; defense; public security; the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security; the protection of judicial independence and judicial proceedings; the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); the protection of the data subject or the rights and freedoms of others; the enforcement of civil law claims'. Moreover, according to article 29 para. 4 of Law 4624/2019 both these rights 'shall be restricted where their exercise is likely to render impossible or seriously impair the achievement of the objectives referred to in paragraph 1 and where such limitations are deemed to be necessary for the achievement of such objectives'. These objectives include cases 'where the processing of special categories of personal data within the meaning of Article 9(1) of the GDPR shall be allowed and is necessary for archiving purposes in the public interest. The controller shall have the obligation to take suitable and specific measures to protect the data subject's legitimate interests. Such measures may include, as far as possible, in particular: (a) access rights restrictions to controllers and processors; (b) pseudonymisation of personal data; (c) encryption of personal data; (d) designation of a DPO'. Likewise, according article 30 para. 2 of Law 4624/2019 it also includes cases in which "the processing is necessary for scientific or historical research purposes, or for the collection and maintenance of statistical information, and the interest of the controller is overriding the interest of the data subject in not having his or her personal data processed". In connection with that, Law 4624/2019 provides that the right to object to the processing of personal data, enshrined in article 21 para. 1 of the GDPR, 'may not be applicable before public entities, in cases in which such processing is required for the public interest, when the latter prevails over the interests of the data subject'. As a result, Law 4624/2019 is in line with the GDPR and sets some further details and requirements for restrictions to the abovementioned rights to be imposed.

On the ground of article 34 of the GDPR, when an incident of a data protection breach occurs or '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 without undue delay'. Furthermore, 'the communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)'.

In addition, based on article 34 and the principles of necessity and proportionality, exceptional conditions, under at least one of which the above mentioned communication to the data subject shall not be required, are the following: “the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner”. At any case, “if the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met”. Similarly, article 33 para. 5 of Law 4624/2019 prescribes that “the obligation to notify under Article 34 of the GDPR, with the exception of the exemption referred to in Article 34(3) of the GDPR, shall not apply to the extent that the obligation to notify would entail the disclosure of information which, according to the law or by reason of its nature, in particular due to overriding legitimate interests of third parties, should remain confidential. By way of derogation from the previous subparagraph, the data subject must be informed, in accordance with Article 34 of the GDPR, where his or her interests, in particular taking into account imminent damage, override the interest relating to maintaining confidentiality”. All these exceptional grounds, exhaustively described in both pieces of legislation (European and Greek), seem to take into serious consideration and strike an optimal and satisfactory balance between the rights at stake, while sufficiently pursuing the principles of necessity and proportionality.

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

Data breaches are under review –judicial or administrative- to ensure the application of Greek and European legislation. The question is whether this review could be considered sufficient and efficient in terms of protection of data subjects’ rights or is leaving gaps. Due to understanding purposes, some clarifications need to be made to answer this question. More specifically, in this part of the research, it is presented which bodies have adopted the role to supervise and protect personal data rights, which is the judicial process in case of infringement and which are the remedies provided by the Greek legislation. Following these logical questions, it should be easier to assess the effectiveness of review on cases of data privacy violations.

5.1 Hellenic Data Protection Authority

The Greek legislation provides the function of a specialized body to supervise the protection of personal data in cooperation with the judicial review. This body is called the Data Protection Authority (DPA) and it is an independent administrative authority whose mission is the protection of personal data. It was established with the law number 2472/1997, which embodied the Directive EU 95/46 in the Greek legislation. It has the jurisdiction to accept complaints by individuals which concern violations of the national legislation. More specifically, the DPA

investigates the complaints about violations of the rights mentioned in the articles 15-22 of GDPR. The DPA receives a significant number of cases each year but it does not conduct a research on every single of them. Complaints that are anonymous, indefinite, unfounded, abusive –especially repetitive-, or do not include all the required elements, are being archived by DPA. DPA can investigate cases of data breaches either based on lodged complaints or on its own initiative.³⁷⁸ When the authority finds that a violation of data privacy has taken place, can impose corrective measures (including fines) but it has no the competence to impose reimbursement. If the individual seeks compensation, they should follow the legal proceedings. However, the decisions of the DPA could be challenged. The regulatory actions of the DPA, such as the imposition of fines, can be applied for annulment in front of the Council of State of Greece.³⁷⁹

According to the law 4624/2019, DPA has the authority to impose administrative fines up to 10.000.000 Euros to public sector bodies if they commit data breaches. This decision made by DPA, must be reasoned and the Authority should take into consideration –among other factors- the duration, the nature, and the size of the damage to specify the level of the penalty. The general principle of Proportionality is dominant in Article 39 as the DPA has the discretion to decide the amount of the imposed fine, following the criteria given by the law.

Another important figure in the system of review of data breaches is the Data Protection Officer (DPO), the person responsible for the compliance of the process of the personal data with the data protection rules. They are appointed by the organization which processes the personal data of individuals, to handle complaints and queries. The data protection subject, who thinks that their rights have been violated, can submit his remarks to DPO. If the problem is not resolved, the subject submits their complaint at the DPA for the protection of their personal data.³⁸⁰ It is important to clarify that the evaluation conducted by the DPO is not a prerequisite of the DPA's review, but it has an optional and supplementary function. In the articles 6-8 of the Greek law 4624/2019, the role of the DPO in the public institutions is being described as advisory and not as decisive and is the “contact point” with the DPA.

5.2 Is the provided by the DPA protection effective?

The question that arises at this point is whether this kind of protection is effective. Before the law 4624/2019 –and the GDPR- the data protection system was defined by the law 2472/1997 which embodied the Directive EU 95/46 in the Greek legislation. This system was mostly focused on prevention and risk assessment but, in practice, it had led to an extremely augmented number of complaints, to a costly system of supervision and to unbearable administrative burdens. As a result, the Hellenic DPA had faced difficulties in handling the system of data protection compliance.

³⁷⁸ Dr. Vasiliki Christou, “Data Protection and Privacy in Greece” [2019] Lexology <<https://www.lexology.com/library/detail.aspx?g=c732305d-960b-46c7-9f8c-cfeaece7f0ed>> accessed 27 February 2021.

³⁷⁹ Law 4624/2019 Article 20 ‘Judicial Protection against DPA’.

³⁸⁰ Data Protection (DPO)’, European Data protection Supervisor <https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en> accessed 27 February 2021.

The system that is established by the GDPR and has been adopted in Greece with the law 4624/2019, manages to create a framework where the DPA can function more effectively as the obligation of applying the rules is transferred to the Data Processors and the DPA conducts an ex-post control. This new system seems to be more effective in numbers. According to a survey conducted by DPA, in 2018 there were fewer complaints than in 2017. The percentage of the cases that were processed by DPA grew around 90% since the previous year. This outstanding result is related to the filing of many cases due to the loss of interest. The lower number of complaints and the huge augmentation of processed cases demonstrate that the DPA works effectively and can respond to the subjects' needs. In the same year, the DPA conducted research in 65 data subject collectors/processors. Most of them were engaged online in financial markets, e-commerce, in insurance services and in the public sector. Fines of a total of 689.000 Euros were imposed on 13 of them.³⁸¹

5.3 Judicial Review-Civil Proceedings

The establishment and the overall effective workings of DPA do not mean that judicial review is not needed. The person whose personal data have been violated can submit their complaint at the DPA or in front of a court. They can appeal against DPA or the data collector/processor. It is important to remember that DPA can only impose administrative fines to perpetrators and not any form of compensation to the data subjects. In addition, the Council of State is the court with the jurisdiction to annul DPA's decisions after an appeal.

According to article 82 of European Union Regulation 2016/679, a data subject can claim compensation from data controller or processor, for material and non-material damages, due to infringement of his personal data rights.³⁸² The Greek legislation is compatible with the Regulation and, in the art.40 of law 4624/2019, it is mentioned that the data subjects who think that their rights have been infringed, can lodge their legal actions against the data controller or processor in front of the civil court of the region where the data processor or controller is installed. The law also offers the data subjects the possibility to lodge their action in front of the court where they have their permanent residence. This legal provision establishes a double jurisdiction which enables the data subject to claim compensation for material or non-material damages.

The data subject can lodge action against the public authority, which illegally provoked damage – as a data processor- according to art. 105 and 106 of introductory law of Civil code (2783/1941).

Data breaches could be legally associated with actions for moral damages. A data subject can lodge a complaint against a bank, if the bank – as a data collector- has shared his or her personal data to a third party without any previous notification.³⁸³ In many similar cases, the data subjects,

³⁸¹ 'Προσωπικά δεδομένα: Πρόστιμα 689.000 ευρώ και λιγότερες καταγγελίες το 2018, σύμφωνα με την έκθεση της ΑΠΔΠΧ' [2020] <[https://www.lawspot.gr/nomika-nea/prosopika-dedomena-prostima-689000-eyro-kai-ligoteres-kataggelies-2018-symfona-me-tin](https://www.lawspot.gr/nomika-nea/prosopika-dedomena-prostima-689000-eyro-kai-ligoteres-kataggelies-2018-symfona-me-tin-ekthesi-tis-apdptx)> Lawspot.gr, accessed 2 January 2021.

³⁸² 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.

³⁸³ Monomeles Protodikeio of Athens 11358/2019.

whose data were exposed to other companies, without their consent, succeed to gain reimbursement. The court finds that in those cases, there has been an infringement of personality rights which include a person's honor and reputation. When a bank delivers to a third company the personal data of its clients –without informing them-, it interferes illegally in their personal sphere. The third company is usually calling the clients who have delay to repay their debts or their monthly disbursement of the loans and is asking when this transaction will take place. These clients – as data subjects - feel frustrated, angry, and ashamed as the personal data, that they give confidentially to the bank, are being shared and employees of another company call them at home and demand answers on personal financial matters. Therefore, the court finds this case as an infringement of personality rights³⁸⁴ and imposes to the data collector the obligation to pay remuneration³⁸⁵ to data subjects who have been affected, based on moral damages.³⁸⁶

5.4 Penal Sanctions

The Article 38 of law 4624/2019 includes the penal sanctions imposed to those who commit data breaches. More specifically, the person who interfere, copy, archive, distort or subtract personal data information, without authorization, is given a prison sentence up to one (1) year. However, if this person transfers, announces or exposes to the public the data, the personal sentence reaches to five (5) years. If this act concerns special categories of personal data, the person responsible is sentenced up to one (1) year in prison and is imposed a penalty payment of up to 100.000 Euros. Moreover, if the person has intent to harm others financially or seeks personal financial gain, is sentenced up to ten (10) years to prison. If national security is put in danger due to the above-mentioned acts, the penalty payment may reach to 300.000 Euros. The Court of appeal –by three judges- (Τριμελές Εφετείο Κακουργημάτων) has the jurisdiction to judge those crimes.

The legal protection in front a penal court seems to ensure that the individuals, whose data are being violated, can seek justice. The legislation covers a great range of acts of infringement and includes not only financial penalties but also imprisonment. These penalties create a strict framework which can have a deterrent effect.

5.5 Judicial representation and class actions

Another interesting provision concerning the judicial procedure is the article 41. The law 4624/2019 offers to the data protection subject the possibility to assign his legal representation to a nonprofit making entity, organization, club or union without legal personality, which engages in the protection of human rights/ data subjects' personal data.³⁸⁷ This legislative initiative ensures that the data subject, whose rights have been violated, can seek effective judicial protection by the help of the organizations mentioned above. They have the authorization given by the law to lodge a complete complaint to DPA on behalf of the data subject, according to art. 77 of GDPR for the rights mentioned to the art.78 of GDPR and art. 20 of Law 4624/2019.

³⁸⁴ Civil Code 456/1984 Article 57 "Personality Right".

³⁸⁵ *ibid*, art 914 'Delict'.

³⁸⁶ *ibid*, art 932 'Compensation for non-material damage'.

³⁸⁷ Law 4624/2019 Article 41 'Representation of data subjects'.

The specialization, the legal knowledge and the experience in this field make those organizations capable of effectively representing the data subjects. The assignment of the representation to any of those organizations is given through written and specialized authorisation,³⁸⁸ which can be entirely, or partly withdrawn.

The assignment of the legal representation to a not-for-profit body or organization paves the way for class actions. The GDPR does not establish a procedure for class actions but it allows each Member State to define the conditions under which these actions would be admissible in front of a national court. However, the lack of a harmonized or common framework about class actions and overall, judicial proceedings does not seem to serve the principle of consistency which is the main purpose of the Regulation.

In certain Member States, some class actions have been conducted as the data subjects have been represented by the organizations mentioned in the article 80 of the GDPR. It needs to be highlighted, though, that the data class actions are a new chapter to European litigation and the figures enabled to represent these types of cases are still low at numbers. In Greece, no data class action trial has taken place so far and the law 4624/2019 does not provide any guidelines about this topic. However, it is expected that the data class actions will become more common and relevant in the next few years due to the increasingly augmented number of the data infringement cases³⁸⁹. Under this point of view, in the future, the Greek legislation might implement more specialized measures and regulations about the data privacy trials which would possibly include details about class actions.

The European Commission published on 25.01.2018 a report³⁹⁰ on the injunctive and compensatory collective redress mechanisms in the European Union and it concluded that 19 Member States –including Greece– have available redress mechanisms, but in most of them, they are limited to consumer claims. In Greece and other Member States, representative collective actions are also established for obtaining compensation.

Especially in Greece, according to the law 2251/1994, which regulates the protection of consumers, the consumer associations have the legal right to represent their members in front of the court (art. 10§15) and more than one association can jointly submit collective class actions (art.10§17). These actions can include –among others– the violation of consumer's personal data and privacy.

According to the Directive 2020/1828 –also known as Collective Redress Directive³⁹¹– in every Member State, there should be established representative action mechanisms for the protection

³⁸⁸Administrative procedure code 2690/1999, A'45 Article 11§1.

³⁸⁹ Mathilde Gérot, "The future of personal data class actions in Europe" [2020] FINTECH DIRECT <<https://www.fintechdirect.net/2020/02/11/the-future-of-personal-data-class-actions-in-europe/>> accessed 11 February 2020.

³⁹⁰ Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the implementation of the Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union law (2013/396/EU) COM/2018/040 final, 25.01.2018.

³⁹¹ Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC OJ L 409/1.

of the collective interests of consumers. In the recital (13) of the Directive, it is explained that these consumerist rights include the protection of personal data due to the digitalized character of the European market³⁹². At article 24, the Directive calls the Member States to adopt all the necessary measures, to be compatible with the Directive, by 25.12.2022.

To conclude, the European and national legislation are already moving into the right direction, but a more specialized provision on data class actions would still be welcomed. The creation of a framework that would allow and facilitate the data collective actions would be an effective tool to enhance the judicial review of data breaches and the protection of data subjects' rights.

5.6 How the Council of State review a case (1957/2019)

One case that got the attention of Greek media was the decision 1957/2019 of Council of State. According to the facts of the case, two companies were processing personal data of more than five million Greek taxpayers, without their consent. These data include –among others– information about the income of these individuals, which could only have leaked from the General Secretary of Informative Systems. Moreover, in one of the companies, they tried to sabotage the research conducted by DPA. Finally, DPA fined 100.000 Euros to one company and 15.000 Euros to the other one. Both companies lodge an application in front of the Council of State for annulment for this DPA's decision.

In the application for annulment, it was claimed that the decision made by the DPA was based on illegal means of evidence (email correspondence between the company and its clients) according to art.9A and 19§1 and 3 of Constitution. However, the court dismissed 14/2/2021 these claims because the DPA's decision was not based solely on these emails. It also pointed out that the emails mentioned above, are not protected by the confidentiality of communications of art. 19§1 of Constitution. The confidentiality lasts until the receipt of the email by the receiver. In this case, the emails were already received, so they are no longer under the meaning of “communication”.³⁹³

Another legal issue of this case was the level of the penalty. The companies claimed that the principle of proportionality was infringed, because the DPA did not take under consideration factors such as the financial state or damage of the companies. The fine of 100.000 Euros was close to the maximum level of 150.000 Euros. However, the Council of State dismissed this claim as invalid because DPA took under consideration all the criteria required by the law. In conclusion, the principle of proportionality was not infringed.

5.7 Data processing conducted by judicial authorities

Although the Greek courts have tried to be compatible with European legislative models and technological advancements, some improvements still need to be made. One worth-mentioning issue is the processing of personal data by judicial authorities. A significant difference could be

³⁹² Melissa Heikkilä, <<A wave for class actions is coming for Big Tech>> [2021] POLITICO, <<https://www.politico.eu/article/class-actions-big-tech-apple-tiktok-facebook/>> accessed 02 February 2021.

³⁹³ Προσωπικά δεδομένα: Επικυρώθηκαν πρόστιμα 115.000 ευρώ σε εταιρείες για την υπόθεση της διαρροής φορολογικών δεδομένων από τη ΓΓΠΣ', [2019] Lawspot.gr <<https://www.lawspot.gr/nomika-nea/prosopika-dedomena-epikyrothikan-prostima-115000-eyro-se-etairies-gia-ti-n-ypothesi-tis>> accessed 2 December 2019.

noticed at this point, between the European Courts and the Greek ones. While the Courts of the European Union are establishing internal control mechanisms, the Greek legislation does not have any similar provision.

Specifically, the data processing of the Court of Justice of the European Union (CJEU) –when acting in its judicial capacity- is not covered by the supervisory competence of the European Data Protection Supervisor (EDPS)³⁹⁴. This provision is justified with the principle of judicial independence and the need for independent decision-making. However, according to the recital (74) of the Regulation 2018/1725³⁹⁵, the CJEU should establish independent supervisory internal mechanisms. With the Decision 2019/C 383/02 of the CJEU³⁹⁶ made on 01.10.2019, a **Committee**, with a special role on personal data protection, is established and is activated when the Court acts in its judicial capacity. According to article 1, when a natural person applies to the Registrar of the CJEU to decide as data processor, the decision must be taken in two months. The natural person has the right to lodge a complaint in respect of this decision, in front of the Committee. The Committee has the right to check the legal provisions and the relevant facts of the case and to even annul the decision mentioned above. The same provision is included in the Decision 2019/C 383/03 of the General Court of EU, on 16.10.2019.³⁹⁷

It's important though, to examine the guidelines provided by the EU Legislation about the supervision of the national courts. The Directive 2016/680 – also known as the Law Enforcement Directive 'LED'- deals with cases that fall out of the scope of the GDPR protection, and especially with the processing of personal data by controllers who are competent authorities and conduct the process for law enforcement purposes. As it is referred to in the recital (80) of the Directive, the protection of personal data by supervisory authorities covers the processing conducted by national courts and other judicial authorities, but with the exemption of where they are acting in their judicial capacity.³⁹⁸ This exemption serves the need for safeguarding the independent performance of the national courts. According to the recital (20) of the GDPR, the Member States could establish procedures related to data processing by their national courts. These procedures could be supervised by specific bodies within the judicial system of the Member State. These bodies could deal with the lodged complaints about the data processing and ensure the compliance of the procedures with the Regulation.

³⁹⁴ 'The protection of personal data processed by the Court of Justice of the European Union' Court of Justice of the European Union- CURIA, < https://curia.europa.eu/jcms/jcms/p1_2699101/en/ > accessed 2 February 2021.

³⁹⁵ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC L 295/39.

³⁹⁶ Decision 2019/C 383/02 of the Court of Justice of 1 October 2019 establishing an internal supervision mechanism regarding the processing of personal data by the Court of Justice when acting in its judicial capacity, OJ C 383/2.

³⁹⁷ Decision 2019/C 383/03 of the General Court of 16 October 2019 establishing an internal supervision mechanism regarding the processing of personal data by the General Court when acting in its judicial capacity, OJ C 383/4.

³⁹⁸ 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 [2016] OJ L119/89.

However, in the law 4624/2019, there is no provision for a committee or other supervision body.³⁹⁹ The Greek legislation differentiates itself from GDPR Regulation and Directive 680/2016. In the draft law, there was provision for authorities which would supervise courts and prosecutor services, but it was left out of the context of the finally voted law. According to the final text of the law 4624/2019, which embodied the Directive 2016/680, the data subjects can submit their complaint to the DPA, if they believe that the data processing done by public authorities violates their rights. However, according to article 58, this norm does not apply when the judicial and prosecutorial authorities who process personal data, are acting in their judicial capacity. This creates a confusion concerning which body should adopt the role of the supervision of courts and it raises questions about the next legislative steps in Greece.

5.8 Is the review on data privacy efficient?

In conclusion, if an answer would be needed to be given on the question about the efficiency of the review in Greece, it would be “yes with some reservation”. The establishment of a national legal framework, in compliance with the GDPR, is providing administrative and judicial procedures for the review of cases related to data violations. The enhanced role of the DPA, the deterrent effect of the penal sanctions and the compensation for both material and moral damages are playing a crucial role in the protection of personal data. Even though the law 4624/2019 is offering a sufficient level of protection against the data infringements, there are still a few legislative gaps that may leave some initiatives to be desired. With the ongoing advancement of technology, the Greek legislation will have to make some improvements and provide more detailed guidelines on specialized issues about the litigation and the data review in general. Some of these issues might be the data class actions and the review on the national courts when they are processing personal data. Taking these thoughts under consideration, the efficiency of the review on data privacy breaches seems to be of the utmost importance in the protection system of personal data.

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

6.1. Introduction

Greece, over the last decades, has demonstrated significant progress in tackling several aspects of discrimination. A powerful instrument towards this goal is the judicial review of anti-discrimination cases. After examining the main legal texts and the bodies responsible for applying them, it is essential to evaluate their effectiveness, especially in the context of potential or already-existing technical advances, so as to conclude whether judicial review can be considered as effective or not.

6.2. Main Legal Texts

6.2.1. Constitutional level

³⁹⁹ ‘Προστασία προσωπικών δεδομένων στα δικαστήρια: Βιοι παράλληλοι για τα Δικαστήρια της ΕΕ και της Ελλάδος;’ [2019] Lawspot.gr, <<https://www.lawspot.gr/nomika-nea/prostasia-prosopikon-dedomenon-sta-dikastiria-vioi-paralliloi-gia-ta-dikastiria-tis-ee>> accessed 16 December 2019.

The Greek Constitution declares the principle of equality at Article 4 ('All Greeks are equal before the law'. 'Greek men and women have equal rights and equal obligations'). Article 5(2) prohibits discrimination ('All persons living within the Greek territory shall enjoy full protection of their life, honor and liberty irrespective of nationality, race or language and of religious or political belief'). Furthermore, Article 116 founds the obligation of the State to undertake measures for the elimination of inequalities, to the detriment of women. It should also be mentioned that Article 13 stresses that the enjoyment of civil rights and liberties does not depend on the individual's religious beliefs, thus stressing that no discrimination is permitted on the ground of religion. The principle of equality has been argued to apply not only in relations between state and individuals, but to display effects between individuals as well. Finally, Relevant Article 9A prescribes that all persons have the right to be protected from the collection, processing, and use, especially by electronic means, of their personal data, as specified by law.

6.2.2. International Law

The European Convention on Human Rights establishes at Article 14 the principle of non-discrimination. Secondly, the International Covenant on Civil and Political rights declares in Article 26 that 'all persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status'. Greece is a member of both international Conventions and is thus bound by the non-discrimination principle.

6.2.3. EU legal order

The right to non-discrimination is guaranteed under Article 21 of the Charter of Fundamental Rights. Within EU anti-discrimination law, it is important to distinguish between legislation relating to discrimination on specific protected grounds (such as race, gender, or age) and the general protection of equal treatment. Most anti-discrimination laws distinguish between direct and indirect discrimination.

Specifically, Directive 2000/43/EC⁴⁰⁰ prohibits all forms of discrimination based on race or ethnic origin in several areas (Race Equality Directive). Directive 2000/78/EC⁴⁰¹ prohibits all forms of discrimination in employment and occupation based on religion or convictions, handicap, age, and sexual orientation (the Framework Directive). Thirdly, EU anti-discrimination law includes the Gender Equality Directive 2006/ 54/EC⁴⁰² and the Gender Goods and Services Directive 2004/113/EC.⁴⁰³

⁴⁰⁰ Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L 180/ 22.

⁴⁰¹ Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation [2000] OJ L 303/ 16.

⁴⁰² 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), [2006], OJ L 204/ 23.

⁴⁰³ Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services [2004] OJ L 373/37.

6.2.4. Greek legal order

The promotion of the right to fair treatment and the confrontation of any form of discrimination due to race, nationality, colour, ethnic origin or descent, religious or other beliefs, age, social or family circumstances, sexual orientation, chronic health condition or infirmity, identity or gender characteristics are prescribed in Law 4443/2016,⁴⁰⁴ which implements three EU Directives into Greek Law (Directive 2000/43/EC, 2000/78/EC and 2014/54/EU).⁴⁰⁵

As far as gender equality is concerned, Law 4097/2012⁴⁰⁶ establishes a legal frame for the implementation and the promotion of the fair treatment between men and women during their business or profession. Additionally, Law 3896/2010⁴⁰⁷, as last amended by Law 4604/2019,⁴⁰⁸ transporting Directive 2006/54/EC, sets the legal ground for the establishment of the principle of equal opportunities to both men and women in their professional sector. Finally, Law 3769/2009⁴⁰⁹ stands for legally combating gender discrimination with regards to access to goods or services. This Law transports Directive 2004/113/EC to the Greek legal order and prescribes in article 7 that any person who considers that he or she has been harmed by non-compliance with the principle of equal treatment has the right to judicial protection and the right to appeal to the competent administrative authorities.

Among the legislative documents mentioned above, the most important is Law 3896/2010 on the Implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment, which broadened the competences of the Greek Ombudsman in order to include issues concerning gender equality at work. The purpose of the Law is to ensure equal opportunities and equal treatment of men and women in matters of employment and occupation as regards: a) access to employment, including promotion, and to vocational training; b) working conditions, including pay; and (c) occupational social security schemes, as provided for in Directive 2006/54/EC. Under Article 25 of the Law, the Greek Ombudsman constitutes the competent body for the implementation, monitoring and promotion of the principle of equal opportunities and fair treatment of men and women both in the private and the public sector. Natural or private legal persons, including banks come within the jurisdiction of the Greek Ombudsman. An important innovative mechanism of this specific law is found in Article 25(7); if the Ombudsman receives reports of gender discrimination, the already started investigation should not be stopped or hindered if the applicant initiates legal proceedings. In fact, its mediation activities should continue, to resolve the problem until the hearing of the case or the examination on request for temporary judicial protection.

Finally, turning to procedural issues, the Law contains an important rule regarding the reversal of the burden of proof. According to article 24, in case of a claim of gender discrimination, the

⁴⁰⁴ Law 4443/2016, GG 232/A/09-12-2016.

⁴⁰⁵ Directive 2014/54/EU of the European Parliament and of the Council of 16 April 2014 on measures facilitating the exercise of rights conferred on workers in the context of freedom of movement for workers Text with EEA relevance [2014] OJ L 128/8.

⁴⁰⁶ Law 4097/2012, GG 235/A/03-12-2012.

⁴⁰⁷ Law 3896/2010, GG 207/A/8-12-2010.

⁴⁰⁸ Law 4604/2019, GG 50/A/26-03-2019.

⁴⁰⁹ Law 3769/2009, GG 105/A/01-07-2009.

applicant must submit evidence, showing that a discriminating act is possible to have taken place, while the respondent is responsible for proving the lack of preconditions of such discrimination. The described procedure is applied to cases before civil and administrative courts, but also before every competent authority, such as, but not limited, to the Greek Ombudsman. However, in criminal proceedings this is not the procedure followed.

6.3. Bodies of Review

6.3.1. Court of Justice of the EU and EU institutions

All EU countries must designate a national equality body responsible for promoting equal treatment. These bodies must provide independent assistance to the victims of discrimination, conduct surveys and studies, and publish independent reports and recommendations. If a national authority violates the Charter when implementing EU law, national judges (under the guidance of the European Court of Justice) have the power to ensure that the Charter is respected. The Charter also protects individuals and legal entities against actions by the EU institutions that infringe fundamental rights. If this occurs, the European Court of Justice has the power to review the legality of the act in question.

6.3.2. European Court of Human Rights

Individuals can, as a last resort, after exhausting all remedies available in their own country - bring an action before the European Court of Human Rights in Strasbourg if an EU country has violated a fundamental right guaranteed by the European Convention on Human Rights.

6.3.3. National bodies

1) National Courts

All persons have a right of access to court and the right to initiate the administration of justice, as well as the subsequent right to be heard (Article 20 paragraph 1 of the Constitution). There is no special competent court in Greece before which to seek redress in the event of a violation of fundamental rights. Depending on the nature of the violating act, redress may be sought before national civil, criminal, or administrative courts (Article 8 of Law 4443/2016). Whether or not a fundamental right has been violated is determined based on national substantive law. The procedure to be followed before the competent (civil, criminal, or administrative) court is provided for in national procedural (civil, criminal, or administrative) law.

Significantly, legal entities, associations or organizations, including social partners and trade unions, with the aim of promoting compliance with the principle of equal treatment may represent the injured party before the courts and before any administrative authority or administrative body, with their consent (Article 8 (3) of Law 4436/2016). This can constitute significant help for victims who may not have the means for legal representation. It is worth noting that in civil and administrative courts, when the harmed party claims that the principle of equal treatment was violated and establishes, before the court, the facts from which the latter can deduce direct or indirect discrimination, the opposing party or the administrative authority bears the burden of proving in court that there was no breach.

To seek redress against acts of public administrative bodies, the competent courts are the administrative courts and, mainly, the Council of State (Article 94, 95 of the Constitution). Public administrative bodies *stricto sensu* are the bodies that exercise sovereign administration with privileges of public power, that is, they have the power to unilaterally impose obligations. These bodies take the form of legal entities under public law and are governed by administrative law. Important decisions have been taken by the highest administrative court in Greece, the Council of State especially in cases concerning inequality of social security treatment, inequalities in the workplace, quotas in public bodies. The Council of State decides, according to paragraph 1 (a) of Article 95 of the Constitution, on applications for annulment against the executive acts of the administrative authorities. Presidential Decree 18/1989 prescribes that application for annulment must be exercised within 60 days, starting from the notification or the publication of said act.

2) Specialised human rights bodies

Apart from seeking redress at the courts, for the restitution of material or moral damage to their legal interests caused by an administrative act, victims can request from the administrative authority that issued the act, its revocation or modification, or, from the authority presiding over the one that issued the act, its annulment, according to Article 8 of Law 4443/2016.

At this point, a detailed individual overview of the competent bodies is required:

The Ombudsperson is an authority anchored in the Constitution. Specifically, it is an Independent Authority operating under Article 103 of the Constitution. It is responsible for upholding the principle of equality where this principle has been violated by public administrative authorities.

The institution of the Ombudsperson was established under Law 2477/1997⁴¹⁰ and has been in effect since 1 October 1998. The legislative framework for its operation is provided by Law 3094/2003.⁴¹¹ The Ombudsperson's services are free of charge. The Ombudsperson examines individual administrative acts or cases of failure to act by public service bodies in violation of the rights or legitimate interests of natural or legal persons. Any citizen applying to the Ombudsperson must have first contacted the public service involved in the case. Only if such contact has failed to resolve the problem may the citizen apply to the Ombudsperson. The Ombudsperson's mission is to mediate between citizens and public services to protect civil rights, combat maladministration and uphold the rule of law. The Ombudsperson is responsible for monitoring and promoting implementation of the principle of equal opportunities and equal treatment of men and women within the scope of the Law (Article 25 of Law 3896/2010). As a mediator, the Ombudsperson gives advice and recommendations to public administrative authorities. It does not impose sanctions or annul illegal administrative acts.

Ombudsperson for the rights of the child

The Ombudsperson examines actions or cases of failure to act by public authorities in violation of children's rights. To protect children's rights, the Ombudsperson is also responsible for acts by private individuals, legal or natural persons in violation of children's rights.

⁴¹⁰ Law 2477/1997, GG 59/A/17-04-1997.

⁴¹¹ Law 3094/2003, GG 10/A/22-01-2003.

Labor Inspection Corps

In matters relating to employment and labor, the Labor Inspection Corps (“SEPE”) is responsible for upholding the principle of equality where this principle has been violated by natural or legal persons other than those mentioned und.

National Confederation of Disabled People of Greece (NCDP)

NCDP is an organisation supporting and representing disabled people and people with chronic diseases in Greece. It was founded in 1989 by organizations of people with disabilities, chronic diseases, and their families. Discrimination against people with disabilities is pertinent to the discussion about AI and technical developments; accessibility and availability of such products to disabled people has often been limited, according to a report by the NCDP,⁴¹² and their needs have been ignored during the technological design.

The National Committee for Human Rights

The Greek National Commission for Human Rights (GNCHR) was established by Law 2667/1998⁴¹³ as the independent advisory body to the Greek State in accordance with the UN Paris Principles, adopted by the United Nations,⁴¹⁴ and is the national institution for the protection and promotion of human rights in Greece. It plays an important role in the effective implementation of human rights, constantly monitoring developments related to human rights in Greece and abroad, providing ongoing advisory to the competent bodies of the State. It also assesses the reports submitted by national competent authorities for compliance with international, regional and/or and European human rights standards. One example of its action against discrimination is a statement on the implementation in Greece of the Convention on the Elimination of All forms of Discrimination against Women.⁴¹⁵ The Statement emphasizes certain gaps in the legislation and in current practices which limit women’s labor rights, such as the high unemployment rate for women, the dismissals of pregnant women in the private sector and the continuous reduction of the already insufficient day-care structures for children and dependent persons. In this regard, the Commission recommends the transposition in national law of the Directive 2019/1158/EU⁴¹⁶ on work-life balance for parents and carers, which will contribute to the achievement of gender equality in employment. Moreover, the Commission, considering the lack of continuity and coherence characterizing the measures and services in favour of disabled persons, regardless of gender, recommends an essential horizontal inclusion of the dimension of disability at the designing of social policies.

Data Protection Authority

⁴¹² Report on New Technologies and Disability: Equal chances or new forms of exclusion of people with disability? The report in Greek < <file:///C:/Users/User/Downloads/meletiprosdiorismos13.pdf> > accessed 29 April 2021.

⁴¹³ Law 2667/1998, GG 281/A/18-12-1998.

⁴¹⁴ General Assembly A/RES/48/134, Resolution, National institutions for the promotion and protection of human rights [1993].

⁴¹⁵ GNCHR Oral Statement on the implementation of the Convention on the Elimination of All forms of Discrimination against Women (CEDAW), 9 November 2020, 79th Virtual Pre-Sessional Working Group.

⁴¹⁶ Directive (EU) 2019/1158 of the European Parliament and of the Council of 20 June 2019 on work-life balance for parents and carers and repealing Council Directive 2010/18/EU, PE/20/2019/REV/1 [2019] OJ L 188/ 79.

The Hellenic Data Protection Authority is a constitutionally established independent public authority according to Article 9A of the Greek Constitution. It was formed under Law 2472/1997,⁴¹⁷ transposing Directive 95/46/EC.⁴¹⁸ It is responsible for upholding and enforcing the right to privacy in Greece, as provided for in Laws 4624/2019⁴¹⁹ and 3471/2006.⁴²⁰ The chief aim of the Data Protection Authority is to protect citizens from illicit processing of personal data and to assist them whenever their privacy has been violated in any way. Acting *ex officio* or following a complaint, the DPA conducts administrative examinations of data stored in both the public and the private sector. Examinations involve ensuring that bodies comply with the requirements of Law 3471/2006 (regarding notification, information, or other obligations as applicable). This is followed by an examination of the IT system, including the basic characteristics of the system, the nature of the data and the level of security ensured by the organisational and technical data protection measures taken by the data processor. The conclusions of the examination are presented in a report, which is submitted to the DPA. The Data Protection Authority also carries out an independent review of the national section of the Schengen Information System, pursuant to Article 114(1) of the Convention Implementing the Schengen Agreement,⁴²¹ and Law 2514/1997⁴²². It acts as national supervisory authority as laid down in Article 23 of the EUROPOL Convention⁴²³ and Law 2605/1998⁴²⁴ and as a national supervisory authority as laid down in Article 17 of the Convention on the Use of Information Technology for Customs Purposes and Law 2706/1999⁴²⁵.

The Data Protection Authority examines complaints and questions relating to legal enforcement and protection of applicants' rights when these are violated by data processing, and issues relevant Decisions. It also imposes administrative sanctions on data processors or their representatives, for breach of their duties. Finally, the Authority may report violations of data protection legislation to the competent administrative and judicial authorities.

Non-Governmental Organisations (NGOs)

There are various NGOs which may be contacted for assistance in the event of a fundamental rights violation. EPANODOS is a non-profit public service organisation governed by private law, under the supervision of the Ministry of Justice, Transparency and Human Rights. Its primary objective is social rehabilitation of ex-offenders, through vocational training, promotion

⁴¹⁷ Law 2472/1997, GG 88/A/16-05-1997.

⁴¹⁸ 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 L 281/31.

⁴¹⁹ Law 4624/2019, GG 137/A/29-08.-2019.

⁴²⁰ Law 3471/2006, GG 133/A/28-06-2006.

⁴²¹ The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2019] OJ L 239/19.

⁴²² Law 2514/1997, GG 140/A/27-06-1997.

⁴²³ Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) [1995] OJ C 316/1.

⁴²⁴ Law 2605/1998, GG 88/A/22-04-1998.

⁴²⁵ Law 2706/1999, GG 77/A/13-04-1999.

of working skills, counselling, and psychological support. Moreover, KETHI is the Research Centre for Gender Equality (KETHI), a Legal Entity under Private Law of the Ministry of Labor and Social Affairs, which was founded in 1994, and supervised by the General Secretariat for Family Policy and Gender Equality. Another example is 'Praksis', an independent Civil Society Organisation.

Hellenic League for Human Rights (HLHR)

The Hellenic League for Human Rights (HLHR) is the oldest human rights organization in Greece. Nowadays, in view of globalisation and immigration, HLHR plays the role of the guardian of human rights by organizing various activities, by taking part in national, European and international bodies and by undertaking regular public interventions with press releases, documentation texts, legislative proposals and reports. Since 2007, HLHR has implemented the project RAXEN. RAXEN is the national body for the registration and reporting of racism and discrimination against immigrants and minorities. The reports are submitted to the Fundamental Rights Agency of the EU (FRA) and provide data for the comparative study at a European level.

6.4. Evaluation of Effectiveness

According to the country report on non-discrimination, Greece belongs to most of the EU Member States which, prior to the adoption of the two Directives, did not have a special legislative framework establishing equal treatment and prohibiting discrimination. Given that Law 4443/2016 was introduced prior to the CJEU decisions in *Egenberger*⁴²⁶ and *IR v. JC*,⁴²⁷ it is vague and needs to be clarified and brought into line with the findings in these cases. Moreover, the sanctions as foreseen by Greek law cannot be effective, dissuasive, and proportionate, and are therefore in violation of the directives. As highlighted by the Greek National Commission for Human Rights (GNCHR) in its observations on Law 4443/2016, in order for Article 11 (corresponding to Article 15 Directive 2000/43 and Article 17 Directive 2000/78) to be effective in cases of discrimination perpetrated by public servants and workers for legal persons under public law, the relevant provisions of the Code of Public Servants (namely Article 107(1) of Law 3528/2007)⁴²⁸ must extend the scope of disciplinary sanctions to cover violations of the principle of equal treatment.

Secondly, as highlighted by the GNCHR⁴²⁹ in its observations on Law 4443/2016, the relevant Articles of the Code of Administrative Procedure before the Administrative Courts as well as the legislation on the court procedure before the Greek Council of State have to be amended to include a shift in the burden of proof for equal treatment violations. As they stand, these legal

⁴²⁶ ECJ, C-414/16, *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V.* [2018], ECLI:EU:C:2018:257.

⁴²⁷ ECJ, C-202/18 and C-238/18, *Ilmārs Rimšēvičs and European Central Bank v Republic of Latvia* [2019], ECLI:EU:C:2019:139.

⁴²⁸ Law 3528/2007, GG 26/A/09-02-2007.

⁴²⁹ GNCHR, Observations on the Draft Law of the Ministry of Justice, Transparency, and Human Rights, 'Application of the principle of equal treatment irrespective of race, colour, ethnicity or ethnic origin, creed, religious or other beliefs, disability or chronic illness, age, family or social status, sexual orientation, gender identity or characteristics, and other provisions', September 2016, available in Greek at: http://www.nchr.gr/images/pdf/apofaseis/isothta_fullwn/EEDA_SxN_Isi_Metaxeirisi_2016.pdf accessed 29 April 2021.

texts maintain that the burden of proof is on the side of the applicant. If these provisions are not amended, judicial interpretation will be needed. This means that the applicant will have to invoke the relevant Article of Law 4443/2016 during the written proceedings, reminding the judge that the burden of proof is shifted to the respondent. The judge may not be aware of the exception and might apply the general rule of burden of proof in administrative cases.

The report went on highlighting the lack of case law, which is a permanent problem in the Greek legal order, since victims are not usually informed about their rights and civil society is weak compared with other Member States. With regard to barriers to justice, based on Joint Ministerial Decision 123827,⁴³⁰ the fee which must be paid to the police in order to register a criminal complaint was increased by 900 % (EUR 100 instead of EUR 10), which appears to be a deterrent to seeking redress. Moreover, there are no detailed statistics on the cases that reach the courts, since each court must compile its own data, without standardised criteria. What is more, discrepancies in the Civil Code need to be addressed, especially concerning the lack of provisions which link non-discrimination law to actions for damages.

There is also concern about the implementation of the principle of equal treatment in Greece, even more so since the economic crisis. For example, the minimum age for retirement was extended by a couple of years. These measures can lead to unfavourable treatment based solely on age, since, in practice, younger generations may not have access to employment (given that positions will still be occupied by older persons), and they may constitute direct, non-justifiable discrimination in violation of Directive 2000/78/EC.⁴³¹

The most important problem related to equality bodies seems to be related to their budget and resources (personnel and facilities). The Greek Ombudsman, for instance, has multiple mandates, which leads to an increased caseload.

The Report drafted by the Ombudsman is also indicative. Despite some individual positive developments, there are still serious deficits, which are out of step with the progress anticipated since the adoption of common European legislation (Directives 2000/43/EC, 2000/78/EC, 2006/54/EC). Even when taking into consideration the consequences of the financial crisis and its impact on the ability to eliminate or restrict inequalities, progress has been slight even for measures unrelated to financial costs. Complaints submitted to the Ombudsman in 2019 represent a 30% increase over the previous year, the largest rise since 2016, when the Department of Equal Treatment was activated. The largest increase was observed in cases of discrimination between men and women and those related to disability and chronic disease.

Regarding discrimination between men and women, a significant deficit in the protection of pregnant women and young parents can still be observed, with serious divergences in the duration of protection provided between the private and public sectors. The view that a pregnant employee is a 'burden' for private companies remains widespread, leading to attempts at

⁴³⁰ Joint Ministerial Decision 123827/23-12-2010.

⁴³¹ Κουκούλη-Σπηλιωτοπούλου, Σ. (2014), *Μέτρα λιτότητας στην Ελλάδα και ανθρώπινα δικαιώματα*, ΕΔΚΑ 2014, σελ. 194 και επ. (Spiliotopoulou, S. (2014), 'Austerity measures in Greece and human rights: judgments of international bodies, EU Law and examples of Greek jurisprudence', *Review of social security law* 2014), pp. 173, 181, 182 and 189.

‘relieving’ them of the ‘burden’ through quasi-legal means. Irrespective of the fact that the gender-based distribution of social roles continues to mostly place disproportionate burden on the working woman for the care of family members, the need for an equal share of looking after the family and to ensure equal participation of the sexes in professional life is imperative if the goal of achieving a work life balance is to be realised. Regarding this area, the transposition of Directive 2006/54/EC into Greek law by 2022 allows us to re-examine and re-plan all those measures which will permit fundamental changes. This renders greater vigilance and cooperation with social and citizens’ bodies, the competent Labour Inspectorates, and social partners, necessary to provide more comprehensive information and more effective protection. When it comes to discrimination on grounds of age, the subject returns once again on the setting of an age limit on notices for vacancies or job advertisements, without these limits, in many cases, being accompanied by the necessary justification, as required by law. The Ombudsman, in implementing the relevant legislation and case law of the CJEU, reflects in its intervention’s specific directions on the legality of introducing age limits in employment based on their appropriateness and necessity. As regards discrimination towards LGBTQ+, the issue of administrative procedures for registering civil partnership agreements between homosexual couples and the difficulties they face was of prominence in 2019. Other pertinent areas include combating discrimination on grounds of gender identity, intervention is called for in relation to administrative procedures or notarial deeds in which corrections in gender registration are not made in compliance with the necessary guarantees of secrecy and confidentiality.⁴³²

Finally, a survey conducted by Greece’s National Center for Social Research (‘EKKE’), published on 7 December 2018 casts light on the issue of multiple discrimination. “Most incidents of multiple discrimination take place in the workplace, and they usually involve gender bias”. Other pretexts mentioned in the report were disability or chronic illness (19%), marital status (12%), age (9%), race or color (5%). According to the findings, 56.6% said that Greece faces a serious multiple discrimination problem. More specifically, 70.7% said they face discrimination at work. A smaller percentage complained of discrimination at public services (49.1%), in healthcare (47.4%), on public transport (42%), or at courts (37.2%).

6.5. Role of Technical Aspects that Result in discrimination

There is no doubt that technical developments, such as profiling and automated data processing techniques can contribute to the amelioration of our everyday lives. On the other hand, there is an increasing awareness that biased algorithms that systematically discriminate against one group raise considerable concerns, not just for the individual users, but also for society. Biased data can result either from the incorrect handling of training data, or from the incorporation of historical bias.⁴³³ This risk is especially relevant in the context of the processing of sensitive personal data.

⁴³² Equal Treatment, Special Report 2019, (Article 25 paragraph 8 Law 3896/2010 and Article 19 paragraph 6 Law 4443/2016).

⁴³³ Philipp Hacker, ‘Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law, (2018)’, 55 Common Market Law Review 1143-1186.

Many individuals suffering social, political, or economic discrimination share one or more protected traits from the categories listed in Article 9(1) GDPR.⁴³⁴

At present, there is no specific legislation in Greece overseeing non-discrimination issues on the online space, either in the form of hard law, or in the form of guidelines and soft law. This gap would currently have to be filled either by general anti-discrimination law, or by data protection.

6.5.1. Anti-Discrimination Law

The legal anti-discrimination framework predates most of the machine learning applications in use today and cannot easily be extended to them. More precisely, Greek anti-discrimination law seems ill-equipped to deal with discrimination in algorithmic decision making for three reasons. First, algorithmic processes will sometimes bypass the material and personal scope of existing anti-discrimination legislation. For instance, under Greek civil law, it seems doubtful that AI systems can be considered legal subjects, rendering it hard to allocate responsibility to them for breach of anti-discrimination legislation. Furthermore, while it may multiply instances of indirect discrimination, the purported predictive accuracy of machine learning models provides an easy justification for these effects. Finally, to refute these claims, victims would have to prove the model wrong – a difficult task in the face of models that are often inscrutable even to their developers. Ordinary discovery rules in Greece seem to be insufficient to assist claimants in gathering that information. Institutions such as the Ombudsman have yet to encounter such cases and it would be hard to establish a case of discrimination by AI at either administrative bodies or courts, given the ordinary standard of proof borne by the claimant. Moreover, the inherent weaknesses of these systems of review, including the lack of resources and absence of legal clarity, as analysed above, would further hinder the effective protection of users.

Another issue is that individual data subjects are parts of complex systems, whose emergent properties betray sensitive traits from non-sensitive data. When some legitimate variables are correlated with sensitive characteristics, they may thus act as a proxy for the sensitive characteristics, e.g., a zip code may carry racial information; if race is removed, discrimination may continue based on zip code. The *Test-Achats* judgment of the ECJ held that sex must not be a direct input for insurance conditions. However, a debate has arisen on the extent to which risk factors merely correlated with gender may continue to be used – and this is precisely the case of indirect proxy discrimination.

6.5.2. Solutions in Data Protection

The enforcement tools included in the GDPR may constitute a forceful mechanism for overcoming these deficiencies in machine learning contexts. More specifically, the GDPR at Article 9 poses special requirements for the processing of sensitive data. Furthermore, Article 22 establishes the right ‘not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her’. Pattern recognition and profiling must also comply with principles of

⁴³⁴ 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) (Text with EEA relevance) [2016] OJ L 119/1.

lawfulness, fairness, transparency, purpose limitation, data minimization and accountability. To increase transparency regarding the risks of processing, Article 15 grants data subjects the right to access to their personal data and to additional information on how it is processed. Arguably, pattern recognition would be a part of ‘the purpose of the processing’ (Article 15(1)(a)). Regarding the risks of profiling, Article 15(1)(h) requires that data subjects are informed about the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4). Furthermore, the GDPR ‘Data Protection Impact Assessments’ constitute a new co-regulatory requirement that requires companies to factor in safeguards to prevent the potential harmful effects that data processing could have on individuals. Article 35(1) explicitly refers to the processing of personal data ‘using new technologies’ as a factor that is relevant when a controller is making this assessment.

As a Regulation, the GDPR is directly applicable to the Greek legal order. Furthermore, Law 4624/2019 further applies the GDPR to the Greek legal order. Article 22 of that law contains more specific provisions regarding the protection of special categories of personal data and provides that by way of derogation of Article 9 GDPR the processing of sensitive data is allowed from public and private authorities for the exercise of rights deriving from the right to social security and social protection and for health / public health reasons.

Moreover, the EU report ‘Statement on AI, Robotics and Autonomous Systems’⁴³⁵ notes that unrepresentative datasets can produce biased results and sets out a series of ethical principles based on the values of the EU Charter of Fundamental Rights and the EU Treaties. The report notes the importance of ensuring that data sets are fair and not prejudicial⁴³⁶. It also includes a number of other principles, such as human dignity.⁴³⁷ Furthermore, it enforces the system of Data Protection Impact Assessments; these function as a means to strengthen the individual’s right to data protection by enhancing the accountability of those organisations involved in ‘risky processing’ in order to identify these risks in advance and bring forward solutions.

In response to calls for greater clarity on what may constitute these legal effects or similarly significant effects, the (then) Article 29 Working Party produced guidelines and further criteria in ‘order to provide a more concrete set of processing operations that require a DPIA’ and determining whether processing is “likely to result in a high risk” for the purposes of GDPR.⁴³⁸ One relevant criterion includes the processing of sensitive data by AI programs, such as Virtual Personal Assistants (VPAs) which constitute AI applications that systematically collect, process, and share significant amounts of both personal data and ‘special category’ data concerning their users, and that of other natural persons who interact (intentionally or not) with said VPA(s).

6.6. Epilogue

Greece has made significant progress in combating discrimination by adapting and enriching its legislation and establishing numerous bodies responsible for review of discriminatory cases. The

⁴³⁵ European Commission, European Group on Ethics in Science and New Technologies, ‘Statement on Artificial Intelligence, Robotics and ‘Autonomous Systems’ (2018):

<https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf> accessed 29 April 2021.

⁴³⁶ *ibid*, Principle (d), ‘justice, equity and solidarity’, 17.

⁴³⁷ *ibid*, Principle (g), 18-19.

⁴³⁸ Article 29 Working Party, ‘Guidelines on data protection impact assessments (DPIAs).

main evident danger is the polymerisation of monitoring which might lead to incoherence and discontinuity of such a control. Individuals must, at the same time, be encouraged by the authorities to overcome any hesitation or fear. This can be achieved by ensuring protection or anonymity. Thus, if co-operation and exchange of knowledge, expertise and good practices between the competent bodies is ensured, the future of the fight against anti-discrimination in the case of Greece seems to be brighter than anticipated some years ago. It should also be mentioned that there currently is no legislation regulating non-discrimination in an online environment in Greece. This gap is currently being filled by general anti-discrimination law and data protection. However, the weaknesses of the non-discrimination system of judicial review are exacerbated when dealing with technical aspects that result in discrimination.

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 Internet of Things (IoT), Artificial Intelligence (AI), big data and encryption have already played an important role in enacting significant changes in numerous fields, including the legal one. Undoubtedly, such technological advances will require a re-evaluation of basic principles of the Greek legal order, for an optimal balance between predictability of the regulatory environment and adaptability to scientific and technological progress to be achieved. A step towards this goal has been made by Law 4727/2020,⁴³⁹ aiming to regulate and codify digital governance issues in the public sector, as well as to set the ground for a Digital State.

7.1. Artificial Intelligence (AI)

The Council of Europe defines AI as “a set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being. Current developments aim, for instance, to be able to entrust a machine with complex tasks previously delegated to a human”.⁴⁴⁰ If no definitional scheme exists that can embrace all possible uses and applications of this technology, then the introduction of flexible instruments is necessary to keep pace with rapid technological developments. What is most pertinent here is the legal status and personhood of AI. In the Greek legal order, the Civil Code contains no specific mention of AI and the creation of such a legal fiction does not seem to meet the traditional criteria of personhood (Article 34 of the Greek Civil Code, which defines natural persons as any “human” capable of bearing rights and obligations). Questions thus arise regarding AI liability under civil and criminal law, as well as contract law. The shortcomings of the existing legal framework become apparent in the area of contractual liability, to the extent that contractual rules cannot apply to machines designed to select their counterparties, negotiate contractual terms, enter into contracts and decide whether and how they will execute them. Furthermore, the extent of the AI’s autonomy seems to contradict their understanding as a representative (agent) or an assistant

⁴³⁹ Law 4727/2020 (GG 184/23.09.2020)

⁴⁴⁰ COE AI Glossary < <https://www.coe.int/en/web/human-rights-rule-of-law/artificial-intelligence/glossary> > accessed 08 March 2021.

under Article 211.⁴⁴¹ To the extent that an AI program is "merely a program and a machine without his own will", it cannot be understood as a representative. It has been enquired if artificial intelligence can constitute an accomplice under Article 334 of the Greek Civil Code; however, a by-analogy application of Article 334 of the Civil Code to artificial intelligence raises a variety of questions from a dogmatic point of view.⁴⁴²

The European Parliament proposed in a draft report in 2017 to give smart machines the status of "electronic persons" which would be recognized as a subject of law.⁴⁴³ The Parliament adopted the relevant Resolution, on 16 February 2017, without considering the recognition of electronic personality in intelligent robots as the only way, to address the relevant issue of civil liability (liability for compensation).⁴⁴⁴ Moreover, the Resolution on civil law rules on robotics – comprising a code of ethical conduct for robotics engineers, a code for research ethics committees and a license for users, can serve as a governance model for a detailed, process-based architecture of technology ethics in the AI field.

7.1.1. Legislation and Soft Law Instruments

It should be clarified that hard-law legislation will be examined alongside several soft law instruments. EU institutions were hesitant to adopt hard-law documents and preferred to employ soft law instruments to anticipate technological trends. Although these texts are not legally binding, they contain provisions that are useful in regulating AI. A second caveat is the lack of AI-specific national provisions. The Greek legislator has largely refrained from directly tackling the issue of AI, which is why most of the documents stem from EU law.

7.1.1.1 Main system in Greece

At a constitutional level, the Greek Constitution declares the principle of equality at Article 4 ("All Greeks are equal before the law"). Article 5 (2) prohibits discrimination. Furthermore, Article 9A prescribes that all persons have the right to be protected from the collection, processing, and use, especially by electronic means, of their personal data, as specified by law.

The main legislative document that engages with AI is N 4624/2019 which applies the General Data Protection Regulation to the Greek legal order. It should be recalled that as a Regulation, GDPR is directly applicable, and thus Article 22 GDPR regulates automated decision making (see more below). The Greek law does not elaborate on Article 22, and a proposed exception to Article 22 was deleted following public consultation. Furthermore, Article 52 of N 4624/2019 transposes into national law Directive 680/2016 and it prescribes that a decision based solely on

⁴⁴¹ Stavros Kitsakis, *Artificial Intelligence and contract law; an introduction*, (2018), Vol 6, "Εφαρμογές αστικού δικαίου & πολιτικής δικονομίας".

⁴⁴² Karanasiou/Pinotsis, *Towards a Legal Definition of Machine Intelligence: The Argument for Artificial Personhood in the Age of Deep Learning*, Conference Paper, 2017.

⁴⁴³ Draft Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) Committee on Legal Affairs Rapporteur: Mady Delvaux.

⁴⁴⁴ European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), Article 59 (f): 'creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently'.

automated processing, which produces adverse legal effects on the data subject or significantly affects it, is allowed only if provided by law.

In terms of institutions, the National Bioethics Commission is now evolving into a National Bioethics and Techno-ethics Commission, to face the new ethical challenges associated with technological development. The draft law entitled "National Accessibility Authority, National Commission for Human Rights and National Bioethics and Technoethics Committee" was put to public electronic consultation on 31 December 2020. According to the explanatory memorandum, this development aims at rendering the Commission more up to date with the development of deep learning and AI.

The other relevant body is the Greek Data Protection Authority. For instance, although the outcome is inconclusive, the Authority was consulted on an issue related to an AI program. Specifically, Interamerican notified the Authority of a new passenger car insurance plan called "Smart Drive", in which the pricing of the coverage provided is linked to the driving behavior of the insured through a special application. The Authority invited both Interamerican and OSEVEN, which provides the mobile application for this insurance plan, to state their views. It is worth noting that the Authority asked Interamerican to prepare and submit a data protection impact assessment (DPIA) and requested and received an updated Impact Assessment Study. The decision of 31 December 2019 noted that: (a) the question of the appropriate legal basis for the processing operations contained in the present case is included in part in the forthcoming guidelines of the European Council on Data Protection (NAPs) for "Connected Vehicles"; (b) the text of these guidelines at the time of the Authority's conference is expected to be finalized in 2020 with their approval by the NSRF, and thus decided to postpone the decision until the above guidelines are approved by the NSRF, in order to be taken into account.

7.1.1.2 EU institutions

The European Commission set out an AI strategy on 25 April 2018 addressing the socioeconomic aspects in parallel with an increase in investment in research, innovation, and AI-capacity across the EU. It set out a Coordinated Plan, agreed upon by the Member States to align strategies. The Commission also established a 'European AI Alliance' in 2018 tasked with compiling ethical guidelines on AI development for the EU. The Commission further established a High-Level Expert Group that published Guidelines on trustworthy AI in April 2019. Moreover, on 19 February 2020, the European Commission launched a Consultation on Artificial Intelligence. This White Paper on Artificial Intelligence presents policy options to enable a trustworthy and secure development of AI in Europe, in full respect of the values and rights of EU citizens.⁴⁴⁵ It aims at providing a legal framework for new technologies and for obtaining a sufficient volume of digital data to be stored in the future on small 'smart' devices connected to the Internet, which it will achieve through the creation of a data market by supporting European companies wishing to exploit this data. In creating a partnership between the private and the public sector, the aim of the framework is to mobilise resources to achieve an

⁴⁴⁵ EU Commission, 'White Paper on Artificial Intelligence: Public consultation towards a European approach for excellence and trust' (2020).

‘ecosystem of excellence’ along the entire value chain, starting in research and innovation, and to create the right incentives to accelerate the adoption of solutions based on AI.

When it came to the European Parliament, on 20 October 2020 it adopted proposals on how to regulate AI. These are amongst the first detailed legislative proposals to be published internationally. The proposals cover three areas: ethics framework for AI, liability for AI causing damage, intellectual property rights. The European Commission has said in response that it will publish draft legislation the following year. The Parliament sets out a framework of ethical principles and legal obligations for the development, deployment and use of AI, robotics, and related technologies. There are specific obligations for ‘high-risk’ AI to be developed and used in a way that guarantees human oversight, provides adequate cybersecurity, includes ‘fall-back plans’ in case of safety or security issues, makes it clear to users that they are interacting with AI systems; does not create bias or discrimination and respects social responsibility and equality.

Regarding liability for AI, the liability proposals also adopt a two-tier approach with regimes for operators of (1) ‘high-risk’ AI systems, and (2) other AI systems. Operators of ‘high-risk’ AI systems would be strictly liable for any harm or damage caused by an activity, device or process driven by that AI system. Claimants would not need to establish that the operator was at fault. Any attempt to exclude liability in agreements with users would be void.

7.1.1.3 Council of Europe

An important document relating to AI is the European Ethical Charter on the use of artificial intelligence in judicial systems adopted by the Council of Europe. The Charter can guide policy makers, legislators, and justice professionals when they grapple with the development of AI in national judicial processes. Furthermore, the Commissioner for Human Rights published a Recommendation⁴⁴⁶ which stresses the importance of Human rights Impact Assessment on AI systems: public authorities should be required to conduct a self-assessment of existing and proposed AI systems, which should evaluate the potential impact of the AI system on human rights. It also strengthens the principles of participation and transparency and the obligation of independent oversight. As to the latter, it cautions Member States to apply ‘the highest level of scrutiny when using AI systems in the context of law enforcement, especially when engaging in methods such as predictive or preventive policing’.

7.1.1.4 Sectoral applications

After this outline of more general legislative initiatives regarding AI, this study will now move on to examine regulatory provisions related to AI in specific sectors and areas of law:

1. Data Protection

Firstly, GDPR Article 22(1) sets out a general prohibition on solely automated individual decision-making with legal or similarly significant effects. Exceptions are provided if (a) necessary for the performance of or entering into a contract; (b) authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or (c) based on the

⁴⁴⁶ Unboxing Artificial Intelligence: 10 steps to protect Human Rights- Recommendation of the Commissioner for human rights.

data subject's explicit consent. Article 22(4) prohibits automated decision-making and profiling based on sensitive data, unless there is an applicable Article 22(2) exemption and point (a) or (g) of Article 9(2) applies. Under Article 22(2)(b) the Member or Union State law that authorises the processing must also incorporate appropriate safeguarding measures. Such measures should include as a minimum a way for the data subject to obtain human intervention, express their point of view, and contest the decision.⁴⁴⁷ Other relevant GDPR provisions include data protection principles, mainly data minimization and transparency. There are also discipline provisions, such as the obligation to conduct an impact assessment (Article 35). Finally, data subject rights can be important, especially the right to explanation and the right to object. These provisions are directly applicable in the Greek order.

The Article 29- Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 adopted on 2 October 2017 can also be helpful.⁴⁴⁸ Controllers can carry out profiling and automated decision-making as long as they meet all the principles and have a lawful basis for the processing. Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling, defined in Article 22(1). The required safeguarding measures include the right to be informed (addressed in Articles 13 and 14), the right to obtain human intervention and the right to challenge the decision (addressed in Article 22(3)). Any processing likely to result in a high risk to data subjects requires the controller to carry out a Data Protection Impact Assessment (DPIA). Article 35(3) (a) highlights the need for the controller to carry out a DPIA in the case of: a systematic and extensive evaluation which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning a natural person.

The second instrument is Directive (EU) 2016/680 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.⁴⁴⁹ Greece transposed the Directive with Law 4624/2019. Article 52 prescribes the prohibition of automated decision making. It should however be mentioned that in an Opinion given by the Greek Data Protection Authority (Opinion 1/2020), which evaluated the Greek transposal of Directive 2016/680, the DPA argued that paragraph 1 improperly incorporated Article 11 par. 1 of the Directive because the reference to the "appropriate safeguards for the rights and freedoms of the data subject, and at least the right to ensure human intervention by him" is omitted.⁴⁵⁰

⁴⁴⁷ See also GDPR Recital 71; suitable safeguards should also include specific information to the data subject and the right to obtain an explanation of the decision reached after such assessment and to challenge the decision

⁴⁴⁸ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> accessed 14 February 2021.

⁴⁴⁹ 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.

⁴⁵⁰ Hellenic Data Protection Authority, Opinion 1/2020.

The third instrument is the modernised Council of Europe Convention for the Protection of Individuals regarding Automatic Processing of Personal Data ('Convention 108+'). Greece signed the Protocol amending the Convention in presence of the Secretary General Mr Thorbjørn Jagland on 6 September 2019. Subsequently, the Ministry of Justice proceeded to create a scientific committee and to entrust to it the preparation of a draft law ratifying the Amending Protocol and any adaptation of Greek legislation to its provisions. The Protocol strengthens the proportionality and data minimisation principles and extends the types of sensitive data. It calls for greater transparency of data processing, stronger accountability of data controllers and a clear regime of transborder data flows. In addition to the modernized Convention, the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data issued Guidelines on AI and Data Protection on 25 January 2019, which constitute a set of baseline measures that governments, AI developers, manufacturers, and service providers should follow to ensure that AI applications do not undermine the human rights and freedoms of every individual, in particular with regard to the right to data protection. AI developers, manufacturers and service providers should adopt a human rights by-design approach and avoid any potential biases, including unintentional or hidden. Regarding bias, committees of experts from a range of fields may represent the best setting in which to discuss and address questions of the impact of AI on individuals and society, compensating for the limited viewpoint of the AI developers.

2. Judicial System and Law Enforcement

The most important document is the afore-mentioned European Ethical Charter on the use of artificial intelligence in judicial systems. It is illustrating that according to a Study of the University College of London based on 584 decisions of the ECtHR, 79% of decisions were anticipated by an AI program. The CEPEJ has identified the core principles to be respected in the field of AI and justice, including the principle of respect of fundamental rights, the principle of non-discrimination, the principle of quality and security, the principle of transparency, impartiality, fairness and 'user control'.

In Greece, in February 2019 the Ministry of Justice set up a scientific committee to examine the effects on the judiciary of the introduction of artificial intelligence.⁴⁵¹ Furthermore, the Greek Competition Authority, in the context of enhancing its transparency and procedural efficiency, is completing a Code of Procedure, which, among other things, will provide for the simplification of procedures. This Code of Procedure will engage with the use of AI in the robo-advising service prepared by the Competition Authority to integrate artificial intelligence technologies in the public sector in Greece. On the planned platform (the HCC Economic Intelligence Platform), there are search tools and filters available, based on economic theory and algorithms, which will have the potential to improve the Authority's ability to find cartels.

3. Liability

⁴⁵¹ Ministerial Decision no 8056, published in the Government Paper 431, 14 February 2019
https://drive.google.com/file/d/1QKekHanvyWOebaCfGU7DN8w1TpUO_aHz/view accessed 4 March 2021.

Given the complexity in the process of decision making, a clear understanding of the interactions between the machine and the human agent is necessary not only for attributing responsibility for the outcome of the decision, but also to determine causality, intent and risk assessment. Greece does not have specific rules regulating liability from damage caused by AI. The existing rules on contract/tort law are not adequate to cover the breadth of possibilities of AI-caused damage, mainly due to the following dogmatic issues; on the one hand, the appropriate measure of imputation, and on the other, the problem of the importance of the division of labor, which takes place between man and intelligent agent. The problem lies in the fact that it remains unpredictable to what extent the input of the algorithm designer was translated into the output of its operation and, if not, what led to the specific result. In case of a pathological evolution of the contractual obligations of the user of the algorithm, it is difficult under existing Greek laws to attribute this pathology to the user as liable.

4. Health

AI can play a significant role in medicine, pharmacology, and clinical trials. Importantly, it is taking center stage in combating the COVID-19 pandemic. In this context, the European Commission adopted, on 8 April 2020, a Recommendation to support exit strategies through mobile data and apps.⁴⁵² The Recommendation sets out key principles for the use of these apps and data related to social distance measures, prevention, contact tracking, and their interface with data security and EU fundamental rights such as privacy and data protection.

5. Equality and Non- Discrimination

The EU report ‘Statement on AI, Robotics and Autonomous Systems’⁴⁵³ notes that unrepresentative datasets can produce biased results and sets out a series of ethical principles based on the values of the EU Charter of Fundamental Rights and the EU Treaties. The report notes the importance of ensuring that data sets are fair and not prejudicial.⁴⁵⁴ It also includes several other principles, such as human dignity.

7.1.2 Private Initiatives

Self-assessment for private companies

The EU has recognized the importance of the role of private companies and their self-assessment and thus on 17 July 2020, the High-Level Expert Group on Artificial Intelligence (AI HLEG) presented their final Assessment List for Trustworthy Artificial Intelligence.⁴⁵⁵ Following a process where over 350 stakeholders participated, a tool was created to support AI developers and deployers in developing Trustworthy AI. The tool supports the key requirements

⁴⁵² Commission, ‘Recommendation (EU) 2020/518 of a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data’, (8 April 2020).

⁴⁵³ European Commission, European Group on Ethics in Science and New Technologies, ‘Statement on Artificial Intelligence, Robotics and ‘Autonomous Systems’ (2018):

<https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf>

⁴⁵⁴ *ibid*, Principle (d), ‘justice, equity and solidarity’, 17.

⁴⁵⁵ Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment

<https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>

outlined by the Ethics Guidelines for Trustworthy Artificial Intelligence (AI), presented by the High-Level Expert Group on AI (AI HLEG) presented to the European Commission, in April 2019 (see below). The Ethics Guidelines introduced the concept of Trustworthy AI, based on seven key requirements: human agency and oversight; technical robustness and safety; resilience to attack, accuracy, fall back plans; privacy and data governance; transparency, traceability, explainability; diversity, non-discrimination and fairness; accessibility and universal design; environmental and societal well-being and accountability.

1. Insurance Europe

Insurance Europe is the European insurance and reinsurance federation. Greece participates in Insurance Europe via the Hellenic Association of Insurance Companies. The views of the European Insurance Industry on AI were expressed in its response to a consultation by the European Commission on ethical and legal requirements for trustworthy AI in the EU.⁴⁵⁶ The declaration stresses that AI carries great potential for the insurance industry. It suggests the ethical use of AI should be supported by voluntary and/or non-legislative instruments as far as possible. Voluntary certifications have traditionally proven to be an effective means of ensuring high and transparent standards (e.g. around IT security, industry-developed codes of conduct or guidelines).

2. Partnership on AI

The PAI is an international collaboration between key industry figures (including Amazon, Apple, DeepMind, Facebook, Google, Microsoft) academia, policymakers, and civil society that seeks to shape best practices, research, and public dialogue about AI's benefits for people and society. These policy commitments include the aim to conduct open research and dialogue and engage with representation from stakeholders in the business community.⁴⁵⁷

7.1.3. Other External Influences

Data Protection

The 40th International Conference of Data Protection and Privacy Commissioners in October 2018 published a Declaration on ethics and data protection in artificial intelligence. According to the Declaration, AI and machine learning technologies should be designed and used in respect of fundamental human rights and in accordance with the fairness principle, and, thus, a permanent working group is established addressing the challenges of artificial intelligence development.

Autonomous Driving

A report by the Joint Research Centre (JRC) and the European Union Agency for Cybersecurity (ENISA) looks at cybersecurity risks connected to artificial intelligence (AI) in autonomous vehicles and provides recommendations for mitigating them. The report was published on 11 February 2021. Autonomous vehicles use AI systems, which employ machine-learning techniques to collect, analyse and transfer data, to make decisions that in conventional cars are

⁴⁵⁶ Views of the EU insurance industry on artificial intelligence, <<https://www.insuranceeurope.eu/sites/default/files/attachments/Views%20of%20EU%20insurance%20industry%20on%20AI.pdf>> accessed 3 March 2021.

⁴⁵⁷ Partnership for AI, Tenets <https://www.partnershiponai.org/tenets/> accessed 3 March 2021.

taken by humans. A systematic validation of AI models and data is essential to ensure that the vehicle always behaves correctly when faced with unexpected situations or malicious attacks. Moreover, continuous risk assessment processes supported by threat intelligence could enable the identification of potential AI risks and emerging threats related to the uptake of AI in autonomous driving.

Interface with IP

The World Intellectual Property Organization (WIPO) has devised a new framework for the understanding of developments in the field; machine learning is the dominant AI technique disclosed in patents and is included in more than one-third of all identified inventions (134,777 patent documents). Furthermore, WIPO points out the use of AI in IP Administration; AI applications are being increasingly deployed in the administration of applications for IP protection. WIPO Translate and WIPO Brand Image Search, which use AI-based applications for automated translation and image recognition, are two examples of such AI applications. WIPO especially mentions the hotly debated technology for deep fakes, or the generation of simulated likenesses of persons and their attributes.

7.2. Big data

According to the Gartner IT dictionary, big data is defined as ‘high-volume, high-speed, high-variety information that requires innovative and cost-effective forms of information processing to improve decision-making’. The data can come from many different sources. They can be generated by machines and collected through sensors on objects connected to the internet of things, including smart cars, factories, GPS, and satellites that collect meteorological data, etc. They can also be produced by humans in mobile applications, on the internet, including social media and commerce, in e-government files.

One of the central rights engaged is privacy. When data, such as a cookie number, is assigned to a subject, it is difficult to decouple it. Another issue that arises from big data processing is predictive analytics facilitated by big data, with significant implications for subjects who exhibit sensitive characteristics, such as those in GDPR Article 9. Highly targeted advertisements raise concerns about possible manipulation and exploitation of the characteristics of consumers. Additionally, automated evaluations based on big data could lead to the categorization of individuals or groups, which could lead to their exclusion from various opportunities, goods, and services such as business opportunities or medical coverage.

7.2.1. Legislation and Soft Law Instruments

In the regulation of big data, it can be observed that thus far, there has not been a comprehensive and specific legislative document. It should also be highlighted at the outset that Greece hasn’t so far regulated the issue of big data specifically. Therefore, most documents mentioned below are of EU-origin.

7.2.1.1 EU Law

On 25 November 2020, the European Commission issued a Proposal for a Regulation on European data governance (Data Governance Act). The instrument aims to foster the availability

of data by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. In addition, to further ensure the EU's leadership in the global data economy, the European strategy for data intends to further adopt legislative measures on data governance, access, and reuse. For example, it aims to prescribe business-to-government data sharing and to make data more widely available by opening high-value publicly held datasets across the EU.

Secondly, as part of the European Strategy for Data, the Directive on open data and the re-use of public sector information, also known as the 'Open Data Directive', functions as a common legal framework for government-held data (public sector information) and is geared towards two key concepts in the European market: i.e. transparency and fair competition.⁴⁵⁸ The Directive entered into force on 16 July 2019. It replaces the Public Sector Information Directive, also known as the 'PSI Directive'⁴⁵⁹ which dated from 2003 and was subsequently amended by the Directive 2013/37/EU.⁴⁶⁰ Once fully transposed on the national level, the new rules will stimulate the publishing of dynamic data and the uptake of Application Programme Interfaces (APIs). They will also limit the exceptions which currently allow public bodies to charge more than the marginal costs of dissemination for the re-use of their data.

Thirdly, the EU General Data Protection Regulation (GDPR) enables controllers and processors to mitigate the potential risks brought using big data. At the same time, users can rely on strengthened and new rights to protect their personal data, which include the 'right to be forgotten' (Article 17). The right to erasure means that the data subject can ask the controller to erase the personal data. Moreover, the GDPR provides a comprehensive system of information disclosure and effective protection. It also imposes strict rules for obtaining consumers' consent to process their data. Another important aspect that grants consumers real choice is their right to withdraw their consent. Furthermore, the GDPR establishes a strict regime for processing personal data for marketing purposes: controllers must prove that such processing serves a legitimate interest that does not override the rights and freedoms of consumers. However, it should be mentioned that a significant amount of big data used is anonymised. According to GDPR Recital 26, anonymised data does not fall within the GDPR because data is no longer considered "personal data". To achieve anonymisation under GDPR, re-identification of a data subject must be impossible. A caveat is that according to the A29 Working Party, even anonymisation can include the risk of linkability or inference and lead to singling out individuals.⁴⁶¹ Unlike anonymization, pseudonymized data falls within the GDPR's regulatory reach. Article 25 lists pseudonymization as an 'appropriate technical and organizational measure' to meet the requirements of the GDPR.

Fourthly, the 2002 e-Privacy Directive aims at ensuring a level of protection for fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of

⁴⁵⁸ Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

⁴⁵⁹ Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.

⁴⁶⁰ Directive 2013/37/EU of the European Parliament and of the Council.

⁴⁶¹ Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques'.

personal data in the electronic communication sector. Article 5(3) of the e-Privacy Directive requires that any party that stores or accesses information on a user's device obtain the user's informed consent. It applies to many tracking technologies such as tracking cookies.

Furthermore, the proposed e-Privacy Regulation will bring an additional layer of protection by guaranteeing the confidentiality of communications and shelter consumers from online tracking and unsolicited commercial communications.⁴⁶² It would repeal the ePrivacy Directive and would be *lex specialis* to the GDPR. Key fields of the proposed regulation are the confidentiality of communications, privacy controls through electronic consent and browsers, and cookies. The proposed Regulation will apply to new players providing electronic communications services such as WhatsApp, Facebook Messenger, and Skype. Once consent is given for communications data (content and/or metadata) to be processed, traditional telecom operators will have more opportunities to provide additional services and to develop their businesses. The proposed Regulation also provides simpler rules on cookies, which will be more user-friendly, as browser settings will provide for an easy way to accept or refuse tracking cookies and other identifiers.

Finally, the Distance Marketing Directive for financial services (DMD) protects consumers from unsolicited products (Article 9). The use by a supplier of the automated calling systems without human intervention shall require the consumer's prior consent.

7.2.1.2 Greek Law

The e-Privacy Directive (2002/58/EK) was incorporated to the Greek legal order with Law 3471/2006 'Protection of personal data and privacy in the field of electronic communications'. The processing of personal information must be absolutely necessary and it is permitted only if: a) the subscriber or the user, after being informed of the type of data, the purpose and extent of the processing, the recipients or the categories of recipients has agreed, or b) the processing is necessary to execute a contract in which the subscriber or user is a party, or to pre-contract stage, at the request of the subscriber.⁴⁶³

Secondly, following the adoption at the EU level of the GDPR, Law 4624/2019 was issued, which incorporates into the national legal order both the Regulation and the Directive 2016/680, for the protection of natural persons against the processing of personal data by the competent law enforcement authorities.⁴⁶⁴ The rights of the data subject to information and access to personal data are restricted in certain specific cases analyzed in Articles 31-33. The right to be forgotten of the data subject is also restricted in Article 34.

In terms of non-legislative documents in Greece, the National Bioethics Commission on 9 November 2017 examined the ethical issues arising from the use of big data in health. Undoubtedly, big databases offer significant advances in health the Commission notes the

⁴⁶² 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).

⁴⁶³ Law 3471/2006 Article 5.

⁴⁶⁴ 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

increased risk of leakage during the processing of sensitive data in large collections, precisely because of their volume. The ability of "deep data mining" that can lead to the disclosure of subject identity, even in anonymous data, due to the possibility of multiple correlations might also be problematic. Finally, the third ethics issue raised is the handling of "incidental findings" that concern the health of the person. To this end, the Commission has formulated specific proposals for the use of big data on health.⁴⁶⁵ Specifically, it supports maintaining either general consent or anonymization as conditions for the processing of collections of big health data within the discretion of the national legislator.

Finally, Law 4305/2014 on Open disposal and re-use of documents, information and data of the public sector, amendment of Law 3448/2006 (AD 57), adapts national legislation to Directive 2013/37/EU of the European Parliament and of the Council, further enhancing transparency. According to Article 1, the aim of the law is to establish the principle of open access and re-use of documents, information and data held by public sector bodies. It prescribes that according to Directive 2013/37, documents, information and data of the public sector are available from the moment of their posting, publication or initial distribution, free for further use and use for commercial or non-commercial purposes, without requiring any action of the interested party or act of the administration (principle of open distribution and re-use of public information).

7.2.2. Private Initiatives and Industry Response

‘SEV’, the Hellenic Federation of Enterprises has expressed its opinion strongly supporting the use of big data in industry.⁴⁶⁶ It supports the introduction of openness policies in the use of public data and proposes initiatives such as the interconnection of public registers, the data of which are particularly useful in the business world and the economy and could increase the standardization, reliability and security of the data.

7.3. IoT

Under the notion of the Internet of Things (IoT) the interconnection via the internet of devices embedded in everyday objects is understood, which enables these objects to exchange data. Wireless IoT may also be realised through electronic communications services based on cellular technologies, which normally make use of licensed spectrum. Wireless IoT applications serve a wide range of industrial sectors such as energy or automotive and rely on spectrum availability⁴⁶⁷. It merges physical and virtual worlds, creating smart environments and represents the next step towards the digitisation of our society and economy, where objects and people are

⁴⁶⁵ Hellenic National Bioethics Commission, Opinion, ‘Big Data in Health’
<http://www.bioethics.gr/images/pdf/GNOMES/OPINION_Big_Data_FINAL_EN.pdf> accessed 17 March 2021.

⁴⁶⁶ Hellenic Federation of Enterprises,<
<https://www.sev.org.gr/grafcio-typou/arthrografia-synentefxeis-se-mme/ta-anoichta-dedomena-einai-to-petrelaiou-21ou-aiona-arthro-tou-aki-skertsou-genikou-diefthynti-sev-stin-kathimerini-14-10-2018/>> accessed 3 March 2021.

⁴⁶⁷ Commission Implementing Decision (EU) 2018/637 of 20 April amending Decision 2009/766/EC on the harmonisation of the 900 MHz and 1 800 MHz frequency bands for terrestrial systems capable of providing pan-European electronic communications services in the Community as regards relevant technical conditions for the Internet of Things [2018] OJ L105/27.

interconnected through communication networks and report about their status and/or the surrounding environment.

7.3.1. Legislation and Soft Law Instruments

7.3.1.1. Greek Law

Although, there might be no strictly national provision regulating the IoT, the EU has enacted Regulations that cover data, networks/security, and devices. In May 25th, 2018, the General Data Protection Regulation (GDPR)⁴⁶⁸ came into application, radically transforming the level playing field for businesses in the field of data protection. Personal data include any data that can be referred to individuals, which implies that the concept of individual data can extend to vast areas of IoT.

Other instruments are the EU Directive 2013/40/EU⁴⁶⁹ which deals with cybercrime. It provides definitions of criminal offences, and sets proper sanctions for attacks against information systems, to which IoT systems are included, which was transported by the Law 4411/ 2016⁴⁷⁰ as well as the EU NIS Directive⁴⁷¹, concerning cybersecurity issues. The aim of the latter is to provide legal measures to assure a common overall level of cybersecurity in the EU, and an enhanced coordination degree among EU Members and was transported under the Law 4577/2018⁴⁷². Finally, Directive 2014/53/EU⁴⁷³, which focuses on the standardization issue, is important for the joint and harmonized development of technology in the EU, including the one related to the IoT. It was transported in the legal order of Greece through the Presidential Decree 98/2017⁴⁷⁴.

7.3.1.2 European Law

A set of supporting policy actions have been adopted by the European Commission to accelerate the take-up of IoT and to unleash its potential in Europe for the benefit of European citizens and businesses at a policy and a research level.

The EU commenced activity in the IoT area in 2005 by launching ‘2010: A European Information Society for Growth and Employment’ that defined policies for the development of the ‘European Information Space’ and involved innovation and investment in research and development (R&D) for including better services and better quality of life actions.

EU Connected Communities Initiative concerns the IoT development infrastructure and aims to collect information from the market about existing public and private connectivity projects that

⁴⁶⁸ Regulation (EU) of the European and the Council 2016/679 of 27 April 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 L 119/1.

⁴⁶⁹ Directive (EU) of the European Parliament and the Council 2013/40/EU of 12 August on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218/8.

⁴⁷⁰ Law 4411/ 2016 (GG 142/ A/03-08-2016).

⁴⁷¹ Directive (EU) of the European Parliament and of the Council 2016/1148 of 6 July concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.

⁴⁷² Law 4577/2018 (GG A/199/3-12-2018).

⁴⁷³ Directive (EU) of the European Parliament and of the Council 2014/53/EU of 16 April on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ L 153/62.

⁴⁷⁴ Presidential Decree 98/2017 (GG A/139/20-9-2017).

seek to provide high speed broadband (more than 30 Mbps). It also attempts to identify technical assistance needs of local communities and provides targeted support to promoters of more advanced projects. The initiative brings different local communities/municipalities together to help them find and obtain financial support for developing business models to deliver broadband to their area.⁴⁷⁵

In March 2015 the Alliance for Internet of Things Innovation was launched by the European Commission to support the creation of an innovative and industry driven European Internet of Things ecosystem. The European Commission is working closely with AIOTI and all IoT stakeholders and actors towards the establishment of a competitive European IoT market and the creation of new business models. Today the Alliance for Internet of Things Innovation is the largest European IoT Association.

As part of 'Digitising European Industry' initiative and the EU has already described its vision⁴⁷⁶ on the future of IoT which is based on three pillars, a thriving IoT ecosystem, a human-centred IoT approach and a single market for IoT.

The European data economy initiative also contributed to the creation of a European single market for IoT. This initiative proposed policy and legal solutions concerning the free flow of data across national borders in the EU, and liability issues in complex environments such as the IoT one. Liability was decisive to enhance legal certainty around the IoT products and services. To provide a first mapping of liability challenges that occur in the context of emerging digital technologies, including IoT, the European Commission published a staff working document on liability for emerging digital technologies.

Innovation Europe was an ambitious initiative that provided a framework program for funding novel projects (IoT and other) such as the 'Horizon 2020'.⁴⁷⁷ One of the seven parts of the Europe 2020 strategy for smart, sustainable, and inclusive growth is the 'Innovation Union' (IU). The IU involves several actions towards achieving success in making Europe one of the world-class science performers, setting free the innovation from obstacles such as expensive patenting, market fragmentation, and skills shortages and revolutionize the way public and private sectors cooperate and enhance partnerships between European institutions, authorities (national and regional), and business.

A strong European initiative on IoT is IERC:⁴⁷⁸ the European Research Cluster on the Internet of Things. IERC aims among other things at establishing a cooperation platform for IoT activities in Europe and becoming a major worldwide contact point for IoT research, defining an

⁴⁷⁵ EU Connected Communities. Available online:

<https://ec.europa.eu/digital-single-market/events/cf/connected-communities-experience-sharing/item-display.cfm?id=15644> accessed 29 April 2021.

⁴⁷⁶ Commission Staff Working Document SWD(2016) 110 final of 19 April 2016 advancing the Internet of Things in Europe, Accompanying the document, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee on the Regions, Digitising European Industry, Reaping the full benefits of a Digital Single Market [2016].

⁴⁷⁷ Europe 2020 'Innovation Europe'. Available online:

<http://ec.europa.eu/research/innovation-union/index_en.cfm?pg=home> accessed 29 April 2021.

⁴⁷⁸ IERC: Internet of Things Research. Available online: www.internet-of-things-research.eu/about_ierc.htm accessed 29 April 2021.

international strategy for cooperation in the IoT field of research and innovation, coordinating the cooperation activities with other similar EU clusters and projects on IoT and information and communication technology (ICT) and organizing workshops and debates leading to a deeper understanding of IoT, future Internet, 5G, and cloud technology. IERC participants include over 50 EU-funded projects, and over 10 stakeholders of closed projects. Another EU IoT initiative is the 'IoT European Platforms Initiative' (IoT-EPI), which funds many projects covering security, privacy, data protection, and IoT trust issues.

A potential obstacle for the achievement of a single market for the IoT has to do with issues linked to the capacity to handle a large diversity and very large volumes of connected devices, and the need to securely identify them and be able to discover them so that they can be plugged into IoT systems. In this context it is important to promote an interoperable IoT numbering space for a universal object identification that transcends geographical limits, and an open system for object identification and authentication. However, the outcome remains to be seen.

7.4. Encryption

Encryption is the process of converting data to an unrecognizable form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet. It is also used to secure data sent over wireless networks and the Internet.

In today's world, encryption technology is increasingly used in all areas of public and private life. It is seen as a vehicle to protect individuals, civil society, critical infrastructures, media and journalists, industry and governments by ensuring the privacy, confidentiality, data integrity and availability of communications and personal data: it is evident that all parties benefit from encryption technology. Encryption has been identified by EU data protection and cybersecurity authorities as an important tool contributing for instance to the protection of personal data transferred outside the EU but subject to the requirement of an essentially equivalent level of protection, which according to the Court of Justice is a legal requirement for data transfers⁴⁷⁹.

7.4.1. Legislation and Soft Law Instruments

7.4.1.1. Greek Law

Electronic Communications

There is no explicit provision on the provision of encryption keys to the state. Encryption is only required as a technical measure to enhance the protection of electronic communication operators against security incidents and violation of communications privacy.

The Hellenic Authority for Communication Security and Privacy (ADAE) was established in 2003 as prescribed by Article 19 (2) of the Greek Constitution which calls for the establishment of an independent authority with a mission to ensure the confidentiality of mail and other forms of free correspondence or communication. Considering the information provision ADAE had issued Regulation 165/2011⁴⁸⁰ 'for the assurance of confidentiality in electronic

⁴⁷⁹ ECJ, Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems, ECLI:EU:C:2020:559.

⁴⁸⁰ Regulation 165/2011 (GG 2715/B/17-11-2011).

communications'. The provisions of this Regulation concern all persons involved in providing electronic communications networks and/ or services. These entities are obliged to have and to implement a Security Policy for the Assurance of Communications Confidentiality, with a content which must be in accordance with the provisions of the Regulation. Article 13 of the Regulation under the title 'Encryption Policy' prescribes the following.⁴⁸¹

The encryption policy must lay down the obligation of the provider to use suitable algorithms and encryption systems to adequately protect communication data or other information which could lead to the disclosure of the communication data of subscribers or users of the networks or services provided (such as passwords and information and Communication Systems-ICS-structural data) during the storing and transmission of these data on/to ICS, as well as the minimum security characteristics of encryption systems. The Encryption Policy shall apply to all the provider's ICS.

The provider must implement encryption systems to ensure the sufficient protection of communications data during their storage or transmission via networks. Encryption must be applied to ICS based on the results of the risk assessment prepared in accordance with the principles set out in Article 3 of the Regulation. Where algorithms and encryption systems are used, including digital signature algorithms, international, widely accepted standards must be considered. The length of the key used must consider international, widely accepted standards depending on the encryption algorithm used, and the results of the risk assessment prepared. The provider is obliged to prevent unauthorized access to keys being used for encryption, authentication, or digital signature purposes. Where asymmetric encryption algorithms are used for a logical access to the ICS, for encryption or for digital signatures purposes, each public/private key pair must correspond to a unique user and the corresponding private key must be known only to the specific user to whom it corresponds. Digital service provider complies with the relevant legislation. Where the provider generates and manages encryption keys used on ICS, he must prepare and comply with appropriate procedures for the creation, certification, distribution, and withdrawal of the encrypted keys. The provider is obliged to keep a file that records the details of how the requirements of the paragraph are implemented.

Electronic Signatures

As far as electronic signatures are concerned, encryption is a part of them. More specifically, for them to be obtained and verified public-key cryptography, or asymmetric cryptography is used. The latter is a cryptographic system which uses pairs of keys: public keys (which may be known to others), and private keys (which may never be known by any except the owner). The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions. Effective security requires keeping the private key private, while the public key can be openly distributed without compromising security

⁴⁸¹ Permanent Mission of Greece in Geneva, Note verbale, Reference no 6171.1/7/234.

Rules for electronic signatures are set out in the eIDAS Regulation,⁴⁸² which came into direct effect to all EU member-states, including Greece. Greece generally stands for the concept of a Qualified Electronic Signature (QES), meaning that an independent accreditation for these signatures by an approved certification body is required. Although Recital 49 of the eIDAS Regulation allows Member States to set requirements regarding the type of electronic signature that will be required in certain circumstances, no such law has been voted in Greece. Regarding the accreditation itself, Greece follows the European Telecommunications Standards Institute standards for the technical requirements of the Qualified Electronic Signatures, as well as the Decision of the Hellenic Telecommunications & Post Commission, which offers a list of Qualified Trust Service Providers publicized at its own site.

It should be noted, however, that, although electronic signatures have been increasingly used in the public sector, QES have not been extensively used in the private sector in practice with the exception of certain industries, such as but not limited to finance and banking. Thus, its acceptance by the courts, tax authorities, business registry, labour and social security authorities has not been accordingly tested. According to eIDAS Regulation, the provisions set therein do not affect the national law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form. This means that certain cases are not typically appropriate for electronic signatures, including documents that need to be notarized or hand written (indicatively, among others, contracts to purchase or transfer real property, grants/donations, certain deeds governed by the law of succession, etc.). Furthermore, companies and individuals that wish to participate in public tenders are obliged to use digital signature (Qualified Electronic Signature). To be able to use a QES, the individual interested would have to be certified by a Qualified Trust Service Provider (QTSP) and use qualified signature creation devices (QSCD).

Personal Data

At the same time, encryption could assist the protection of personal data. In this field, numerous legal instruments co-exist in the Greek national legal system. Specific obligations for electronic communications network/service providers regarding data protection are contained in Law 3471/2006⁴⁸³ regarding the protection of personal data in electronic communications, which transposed Directives 2002/58/EC⁴⁸⁴ and 2009/136/EC⁴⁸⁵ into the Greek legal order.

As far as the security of data processing goes, Article 12 of the Law above enacts the following obligations. When the data security breach may have unpropitious consequences to the personal

⁴⁸² Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257 /73.

⁴⁸³ Law 3471/2006 (GG 133/A/28-06-2006).

⁴⁸⁴ 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) [2002] OJ L 201/37.

⁴⁸⁵ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) [2009] OJ L 337/11.

data or the private life of the subscriber or third parties, the provider shall notify without undue delay the affected subscriber or the affected third party. The notification shall at least include (a) a description of the nature of the personal data breach, (b) the contact points, from which further information can be obtained, as well as (c) recommendations that can limit potentially unfavourable effects from the breach. The notification of the affected subscriber or third party is not necessary, if the provider has proved to the competent authorities in a satisfactory manner that he/she has applied the appropriate technical security measures and that these measures were applied for the data related to the security breach. These measures shall at least include secure data encryption, so that unauthorized access is not possible.

To maintain security and to prevent processing, the General Data Protection Regulation in its Recital 83 invites the controller or processor to evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. In Articles 6, 32 and 34 of the Regulation it becomes clear that the encryption constitutes a safeguard regarding data processing. In addition, Law 4624/2019⁴⁸⁶ enacts supplemental measures for the application of the General Data Protection Regulation (“GDPR”) and incorporates Directive (EU) 2016/680⁴⁸⁷. On August 29th 2019, 15 months after the Regulation, the long-awaited Greek Law regarding the protection of personal data was published. The new Law includes provisions in certain areas which are left by the GDPR to the discretion of member-states and dissolves the legal uncertainty caused by the delayed supplementation of the Regulation and the parallel validity of Law 2472/1997⁴⁸⁸. According to its provisions, the processing of personal data is permitted without the consent of the data subject, provided that it is necessary for scientific or historical research or for purposes related to the collection or retention of statistics, on the condition that appropriate measures are taken, such as anonymity and encryption.

7.4.1.2. EU Law

Apart from the Regulations and Directives already transported in Greek Law, EU’s soft law has been a compass towards the regulation and, in the long run, the establishment of encryption. Encryption is regarded as an effective way of ensuring the protection of cybersecurity, data protection and privacy. It can help citizens and businesses to defend themselves against the abuse of IT technologies, such as hacking, identity and personal data theft, fraud, and the improper disclosure of confidential information. Moreover, consumer devices increasingly make use of full disk encryption. However, encryption can also be used by criminals, which may complicate competent law enforcement authorities’ criminal investigations.

As technologies are becoming easier to access and use, even without any technical skills can use encryption to avoid detection. According to the 2018 Europol Internet Organised Crime Threat

⁴⁸⁶ Law 4624/2019 (GG 137/A/29-08-2019).

⁴⁸⁷ Directive (EU) of the European Parliament and of the Council 2016/680 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 [2016] OJ L 119/89.

⁴⁸⁸ Law 2472/1997 (GG 50/A/10-04-1997).

Assessment (iOCTA)⁴⁸⁹, law enforcement authorities increasingly encounter encryption in their criminal investigations. It is one of the major challenges to address, as it denies access to essential intelligence and evidence.

The use of encryption is essential to ensure cybersecurity and the protection of personal data. EU legislation specifically notes the role of encryption in ensuring appropriate security for the processing of personal data. At the same time, in the context of criminal investigations, law enforcement and judicial authorities increasingly encounter challenges posed using encryption by criminals. This affects the ability of law enforcement and judicial authorities to obtain the information needed as evidence in criminal investigations, and to prosecute and convict criminals. The use of encryption by criminals, and therefore its impact on criminal investigations, is expected to continue to grow in the coming years.

The Commission had since the beginning perceived the important role that encryption will play not only in the context of criminal investigations, but also in the whole function of the Digital Single Market. If it appears that the Commission was not planning to prepare legislation on encryption soon, it went on propose⁴⁹⁰ 6 concrete non-legislative measures to support law enforcement authorities in overcoming challenges posed by encryption. These measures respect the safeguarding of strong encryption, required for the functioning of the Digital Single Market and do not in any way prohibit, limit, or weaken encryption.

These measures aim to strengthen Europol's (EC3's) technical capabilities to deal with encryption and establish a network of centres of expertise. It is vital to point out that there is no intention to substitute those national centres with a supranational structure, but rather the creation of a collaborative space where experts may meet and discuss issues being encountered on the ground and share good practices. Under Europol's co-ordination the collection of best/good practices provided by member- states so as to establish a toolbox of legal and technical instruments is another goal. Moreover, the need to provide training to LEAs and the judiciary especially on encryption at all levels, developed jointly by ECTEG and CEPOL and delivered by CEPOL, is recognised. Finally, the establishment of both a forward-looking observatory to monitor legal and technical developments and of a structured dialogue with industry and with civil society organizations under the umbrella of the EU Internet Forum is highly advised.

Following these discussions with Member States and stakeholders and based on their input, the Commission concludes that the following set of measures to support law enforcement and judicial authorities when they encounter the use of encryption by criminals in criminal investigations should be implemented. This includes, on the one hand, legal measures to facilitate access to legal framework for cross-border access to electronic evidence. Law enforcement authorities often face the challenge of access to evidence located in another country. In parallel, the Commission is implementing a set of practical measures to improve cross-border access to

⁴⁸⁹ Internet Organised Crime Threat Assessment (IOCTA) Report 2018, Europol.

⁴⁹⁰ Communication from the Commission to the European Parliament, the European Council and the Council (EU) COM(2017) 608 final of 18 October Eleventh progress report towards an effective and genuine Security Union [2017].

electronic evidence for criminal investigations, including funding for training on cross-border cooperation, the development of an electronic platform to exchange information within the EU, and the standardisation of judicial cooperation forms used between Member States. On the other hand, technical measures are taken into consideration. The Commission will support Europol to further develop its decryption capability. In order, also, to support law enforcement and judicial authorities at national level, a network of points of expertise would be established. These authorities should have a toolbox of alternative investigation techniques at their disposal to facilitate the development and use of measures to obtain needed information encrypted by criminals. Attention should be paid to the important role of service providers and other industry partners in providing solutions with strong encryption, while training programmes for law enforcement and judicial authorities should ensure that responsible officers are better prepared to obtain necessary information encrypted by criminals.

The Council of the EU recently adopted a Resolution⁴⁹¹ on encryption, highlighting the need for security through encryption and security despite encryption. In this resolution, the Council underlines its support for the development, implementation and use of strong encryption as a necessary means of protecting fundamental rights and the digital security of citizens, governments, industry, and society. Furthermore, the Council notes the need to ensure that competent law enforcement and judicial authorities are able to exercise their legal powers, both online and offline, to protect our societies and citizens due to the fact that law enforcement authorities and the judiciary mostly depend on access to electronic evidence to effectively fight terrorism, organised crime, child sexual abuse, and a range of other cybercrime and cyber-enabled crimes. As a result, such access is essential to the success of law enforcement and criminal justice in cyberspace. However, there are instances where encryption renders access to and analysis of evidence extremely challenging or impossible in practice.

In the light of those recent developments as described above, the EU is striving to establish an active discussion with the technology industry and with stakeholders stemming from research, academia, industry or civil society, so as to strike the right balance between ensuring the continued use of strong encryption technology and guaranteeing the powers of law enforcement and the judiciary to operate on the same terms as in the offline world. It has become obvious that potential technical solutions will need to respect privacy and fundamental rights and preserve the value that technological progress brings to society. The need to develop a regulatory framework across the EU that would allow competent authorities to carry out their operational tasks effectively while protecting privacy, fundamental rights and the security of communication could be further assessed.

7.5. Epilogue

The analysed technological evolutions are about to play a crucial role in the future of everyday life of each citizen in the entire world. As soon as national governments perceive their importance and enhance their regulation, it is expected that all the negative aspects that might

⁴⁹¹ Council Resolution on encryption (EU) 1384/1/20 of 24 November Security through encryption and security despite encryption [2020].

tremendously affect human rights might be minimized. According, in case of a multinational or even an international co-operation in this field, it is estimated that these developments will turn out to be helpful tools instead of possible threats. It is high time to understand the importance of these advances and follow the path towards their adoption and harmonization with our legal system.

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

8.1. Introduction

With the fight for privacy intensifying day by day, multiple communication platforms, such as WhatsApp,⁴⁹² Viber⁴⁹³ and even Zoom,⁴⁹⁴ have begun incorporating end-to-end encryption to their messaging platforms to ease their users' privacy concerns. The question arising, though, in the minds of many is what encryption in messages means and what does it entail.

In short, end-to-end encryption is the process of disarranging information contained in messages, texts or even files and media in a way that only the intended recipients can properly access and understand them, as a way of protecting the content of the users' messages.⁴⁹⁵ At the same time, encryption can be used to verify the sender's identity, validating the respective digital signature.⁴⁹⁶ Encryption can be viewed as a method of pseudonymisation of data, since in order for them to be read, an encryption key kept separately is required.⁴⁹⁷ Of course, encryption is not only allowed within the legal orders of the E.U.'s Member-States, therefore in Greece as well, but it is also encouraged in the Union's main data protection instrument⁴⁹⁸, the General Data Protection Regulation.⁴⁹⁹

⁴⁹² WhatsApp Frequently Asked Questions, "About end-to-end encryption", <https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=en>> accessed 23 February 2021.

⁴⁹³ Viber Support Centre, "Viber Account Security and Encryption" <<https://help.viber.com/en/article/viber-account-security-and-encryption>> accessed 23 February 2021.

⁴⁹⁴ Max Krohn, "Zoom Rolling Out End-to-End Encryption Offering" (Zoom Blog, 14 October 2020) <<https://blog.zoom.us/zoom-rolling-out-end-to-end-encryption-offering/>> accessed 23 February 2021.

⁴⁹⁵ 'A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?' (Surveillance Self-Defense, 29 November 2018) <<https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work>> accessed 20 February 2021.

⁴⁹⁶ 'Decryption Methods' (IBM Knowledge Center) <https://www.ibm.com/support/knowledgecenter/en/SSEQTP_8.5.5/com.ibm.websphere.base.doc/ae/rwbs_ws_decryptalgorithms.html> accessed 20 February 2021.

⁴⁹⁷ European Union Agency for Fundamental Rights, 'Handbook on European data protection law - 2018 edition' (April 2018), <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> accessed 20 February 2021.

⁴⁹⁸ Ioannis Dalakouras, "The protection of confidential data, according to Articles 370B-370E of the Greek Criminal Code. Substantial and Judicial Approach" (2020) <http://www.cybercc.gr/m/filer_public/2014/06/30/igglezakhs_dedomena_prosopikou_xaraktira.pdf> accessed 21 February 2021.

⁴⁹⁹ Article 6, 32 <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>> accessed 21 February 2021.

As a result, any data transmitted is rendered unintelligible to third parties, as well as anyone intercepting the data if they have not been provided with the decryption key.⁵⁰⁰ Any intermediary can only see metadata, in other words the data used to vaguely describe the content,⁵⁰¹ such as the subject line, dates and the parties engaged in the communication.⁵⁰² Taking that into consideration, it is not surprising that encryption of personal data is widely regarded as a key factor in harmonising innovative technologies with the right to privacy.⁵⁰³

While that may seem self-evident, in practice most platforms do not offer that option, meaning that even though they do in fact encrypt messages, but at the same time they still hold the decryption key. The reasons behind such practices may vary from convenience purposes of transmitting data more easily to complying with states' legislations to even utilising the data for advertising and profit purposes.⁵⁰⁴

As already explained, encrypted messages are not entirely protected from unwanted third parties, as they can still be decrypted as long as one holds the decryption key, that is generated for each message separately only in the device of the sender and that of the recipient.⁵⁰⁵ Decrypting private messages can be realised for illegitimate purposes, as well as on the basis of a legal court decision, extracting the key from the software or hardware used, or for law enforcement purposes, where there are usually systematic "backdoors" implemented in the encryption, providing access to the governmental bodies responsible for maintaining legal order.⁵⁰⁶

Especially as far as law enforcement all over the globe is concerned, they have vehemently opposed the use of encrypted technologies since their emergence, arguing that the public interest of solving crimes justifies restricting citizens' right to private communications.⁵⁰⁷ Since law enforcement officials in the current digital society heavily rely on electronic surveillance to combat and prevent serious crimes such as terrorism, organized crime, drug and human trafficking, they constantly highlight the possible implications to providing utmost privacy. While each government's stance against decrypting private messages varies, the common ground seems

⁵⁰⁰ Kuan W. Hon, Eleni Kosta, Christopher Millard and Dimitra Stefanatou, "Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation" (2014) Queen Mary School of Law Legal Studies Research Paper No. 172/2014, Tilburg Law School Research Paper No. 07/2014

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405971> accessed 20 February 2021.

⁵⁰¹ Mike Chapple, "What Is Metadata?" (Lifewire, 04 January 2020)

<<https://www.lifewire.com/metadata-definition-and-examples-1019177>> accessed 20 February 2021.

⁵⁰² *ibid.*

⁵⁰³ Prof. Dr. Gerald Spindler and Philipp Schmechel, "Personal Data and Encryption in the European General Data Protection Regulation" 7 (2016) JIPITEC 163 para 1 <<https://www.jipitec.eu/issues/jipitec-7-2-2016/4440>> accessed 21 February 2021.

⁵⁰⁴ Assaf Cohen, "A Guide To End-To-End Encryption And Why Major Cloud Storage Providers Don't Like It" (Forbes, 24 September 2020)

<<https://www.forbes.com/sites/forbestechcouncil/2020/09/24/a-guide-to-end-to-end-encryption-and-why-major-cloud-storage-providers-dont-like-it/?sh=75ea8abb24ea>> accessed 20 February 2021.

⁵⁰⁵ Google Support, "How end-to-end encryption in Messages provides more security"

<<https://support.google.com/messages/answer/10262381?hl=en>> accessed 20 February 2021.

⁵⁰⁶ Bart van der Sloot, Dennis Broeders & Erik Schrijvers "Exploring the boundaries of Big Data" (2016) Amsterdam University Press / WRR <<https://www.ivir.nl/publicaties/download/1764.pdf>> accessed 20 February 2021.

⁵⁰⁷ Robert J. Anello and Richard F. Albert, "The International Encryption Debate: Privacy Versus Big Brother" (Lexology, 12 June 2019)

<<https://www.lexology.com/library/detail.aspx?g=41bce78b-f790-4901-ba88-7b9f6ffdd488>> accessed 21 February 2021).

to be that there should be effective means of accessing protected content should the need arise.⁵⁰⁸

8.2. The Greek legal framework on decrypting private messages

In the Greek legal order, encrypted information is regulated by the law concerning the protection of the confidentiality of communications. Therefore, any decryption required must abide by the process of removal of confidentiality. Specifically, protection of confidentiality and, thus, encrypted messages are protected both by article 8 of the ECHR and article 7 of the Charter of fundamental rights of the European Union, as well as by article 19 of the Greek constitution.

As Greece has ratified the European Convention on Human Rights, the latter's provisions have become part of the national legal order based on article 28 of the Greek Constitution. Article 8 of the ECHR guarantees the right to privacy as a human right, providing that "Everyone has the right to respect for his private and family life, his home and his correspondence"⁵⁰⁹. At the same time, the Charter of Fundamental Rights is binding for the Greek state when its authorities are called upon applying union law. Article 7 of the Charter of fundamental rights stipulates that 'every person has the right to respect for his private and family life, his home and his communications'.⁵¹⁰

As far as Article 8 ECHR is concerned, it is worth noting that the European Court of Human Rights, in the case *Halford v. The United Kingdom* has interpreted the confidentiality of communications as an aspect of the right to privacy.⁵¹¹ A while later, in *Copland v. United Kingdom*, the court held that the protection afforded by Article 8 extends to forms of communication via the Internet.⁵¹²

In 2008, with the decision *K.U. v. Finland*, the European Court of Human Rights has defined the nature of the right to privacy and the manifestation of the confidentiality of communications. The court stressed that the right cannot be recognized as absolute but is subject to legal restrictions. Specifically, paragraph 2 of article 8 of the ECHR provides that the state may intervene in the exercise of the right, when its intervention is justified by a reason concerning the safeguarding of a democratic society and in particular national security, public security, the economic prosperity of the country, the protection of order and the prevention of criminal offenses, the protection of health or morals and the protection of the rights and freedom of others. Any restrictions imposed on the exercise of the right must be justified by these reasons and imposed by a formal law.⁵¹³

⁵⁰⁸ Global Partners Digital, "World map of encryption laws and policies"

<<https://www.gp-digital.org/world-map-of-encryption/>> accessed 20 February 2021.

⁵⁰⁹ Article 8 of the ECHR

<www.jus.uio.no/lm/coe.convention.on.human.rights.1950.and.protocols.to.1966.consolidated/8.html> accessed 20 February 2021.

⁵¹⁰ Article 7 of the Charter < https://fra.europa.eu/en/eu-charter/searchresults?filter_1=7 > accessed 20 February 2021.

⁵¹¹ *Halford v. The United Kingdom*, app. No 20605/92 (ECHR 25/07/1997).

⁵¹² *Copland V. United Kingdom* app. No 62617/00 (ECHR, 03/07/2007).

⁵¹³ *K.u V. Finland* app. No 2872/02 (ECHR, 02/12/2008).

Regarding the protection of confidentiality of communications from supranational sources of law, it is worth considering whether it is protected by GDPR, as transposed in the Greek legal order with Law 4624/2019. To determine if encrypted data falls within its regulatory scope,⁵¹⁴ its material scope and the effect of encryption on personal data should be examined.

The law 4624/2019 applies to all processing of personal data in the context of establishing a controller or a processor, when the processing takes place in Greece. Therefore, since the law 4624/2019 must be applied when 'personal data' is processed, it should, in turn, be examined what information is considered as personal data and the legal nature of the information covered by encryption keys, so as to ascertain whether it falls within its regulatory scope. A crucial element for information to be considered as personal data is the ability to be "identifiable" through the information of a natural person. According to Article 4 No. 1 S. GDPR, which has been transferred in the Greek legal order with the law 4624/2019, defines that 'personal data' means any information relating to an identified or identifiable natural person, directly or indirectly. As a result, the process that a potential data controller must do to match the natural person to the data is crucial for defining data as personal. Another factor when examining whether encrypted data is regulated by the said law is whether they are anonymised or pseudonymised. Anonymised data are excluded from the material scope of the GDPR, according to Article 4 paragraph 5 and thus from the material scope of the law 4624/2019, while pseudonymised data, since they reduce the chances of identification of the subject, they are not excluded. A distinction between encrypted transport of data and encrypted storing of data is crucial too.

Taking into account all the criteria mentioned above, the advocate general of the ECJ⁵¹⁵ has concluded that the applicability of GDPR on encrypted data is not prohibited, therefore the applicability should be examined in each specific case, considering at the same time the use of future decryption technologies and the security of the key management.

Moreover, the protection of the confidentiality of communications as a fundamental right is mentioned in Article 19 of the Greek Constitution.⁵¹⁶ Specifically, it is stipulated that:

1. The secrecy of letters and the free response or communication in any other way is absolutely inviolable, while the law defines the guarantees under which the judicial authority is not bound by secrecy for reasons of national security or for the correction of particularly serious crimes.
2. The law stipulates the establishment, operation and responsibilities of an independent authority that ensures the secrecy of paragraph 1.

⁵¹⁴ Prof. Dr. Gerald Spindler, Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' JUPITEC < www.jipitec.eu/issues/jipitec-7-2-2016/4440?fbclid=IwAR1koaxlvDN8uDdrj3nelM90IXeAq5GhwIleghK3ZGFpjdrA70uVmDJaaA > accessed 28 February 2021.

⁵¹⁵ *ibid.*

⁵¹⁶ Article 19 of the Greek Constitution
<<https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-19/>> accessed 28 February 2021.

3. The use of evidence obtained in violation of this article and articles 9 and 9A is prohibited. Based on article 19 of the Constitution, both freedom of response and communication and the inviolability of its confidentiality are protected as individual rights.

The content of the right of responding freely and communicating, on the one hand, overlaps with the right to communicate in private conditions with the means and manner, at the time, with the content and interlocutor of their free choice, without the obstruction of third parties. The object of constitutional protection is not the message itself, given that this is protected by Article 14 of the Greek Constitution, guaranteeing freedom of expression and dissemination of opinion, but the secrecy of the message.

The meaning of confidential, on the other hand, lies in the absolute secrecy or confidentiality from any third party, other than the recipient of the communication.⁵¹⁷ The concept of confidentiality primarily includes the content of the communication, in whatever way it is conducted. According to the decision 1091/2015 of the Council of the State, the protection of the confidentiality of letters and free response and communication is fully guaranteed, thus establishing an obligation to the state to take measures to ensure the confidentiality of communication among individuals as well.

The protection of confidentiality of communication, which is enshrined in Article 19 of the Greek Constitution, is specified, and complemented by Law 2225/1994, regulating procedural issues regarding the occasions and the manners in which confidentiality can be removed.

Specifically, Article 3 states that, in cases where Article 19 (1) of the Greek Constitution requires the removal of confidentiality for reasons of national security, the competent to request such removal of confidentiality is only a judicial or other political, military or public law enforcement authority which holds the responsibility of protecting national security. The application for such lift of protection must be submitted to the Appellate Prosecutor.

In addition, Article 4 of Greek Law 2224/1994 lists the crimes for which the removal of confidentiality is permissible⁵¹⁸ These are the crimes that are considered according to the penal code as insults to the democratic regime (Articles 134, 135 par. 1,2, 135A, 137A of the Greek Penal Code), the international situation of the country (Article 138 of the Greek Penal Code), the international peace of the country (Article 140 of the Greek Penal Code), defense capacity (Articles 143, 144 of the Greek Penal Code), insults against state secrets (Articles 146, 148 of the Greek Penal Code), crimes against state institutions (Article 157 (1) of the Greek Penal Code), crimes related to the currency (Articles 207, 208 paragraph 1 of the Greek Penal Code), commonly dangerous crimes (Articles 64 par. b, c, 265 par. 3, 270, 272, 275 of the Greek Penal Code), crimes against transport (Article 291 par. 1, par. b, c of the Greek Penal Code), crimes against human life (Article 299 of the Greek Penal Code), crimes against personal freedom (Articles 322, 324 par. 2, 3, 37-4 of the Greek Penal Code) crimes against property (Article 380 of the Greek Penal Code and Article 385 of the Greek Penal Code). Removal of confidentiality

⁵¹⁷ Tsolias Grigorios, *Special Penal Laws*, Sakkoulas Publications, 2013.

⁵¹⁸ Greek Law 2224/1994.

can also be granted for certain crimes included in the Greek Military Penal Code (Articles 26, 27, 28, 29, 31, 32, 33, 34, 35, 39, 40, 41, 63, 64, 76, 93 and 97 of the Greek Military Penal Code).

Moving on to more specialized cases, the lift of protection of confidentiality of communications is provided in the cases of article 15 par. 1 of Greek Law 2168/1993, concerning weapons, ammunition, explosives, explosive devices and other provisions⁵¹⁹ articles 5, 6, 7 and 8 of Greek Law 1729/1987, regarding Combating the spread of drugs, protection of young people and other provisions,⁵²⁰ as well as articles 89, 90 and 93 of Greek Law 1165/1968. The decision for removal of confidentiality is ordered by the Board of Appeals or the competent Misdemeanor Courts.

Moreover, the penal code also provides for a protective framework of the conceptual good of confidentiality of communications. In particular, Article 370 of the Penal Code establishes the breach of confidentiality of telephone communication and oral conversation as a criminal act.⁵²¹ According to it, anyone who unlawfully traps or otherwise interferes with a device, connection or network of fixed or mobile telephony services or with a system of hardware or software used to provide such services, for the purpose of informing or imprinting material on a carrier the content of a telephone conversation between third parties or details of the location and movement of such communication, shall be punishable by imprisonment. The act of the previous paragraph is respectively punishable when the perpetrator imprints on a material body the content of his telephone communication with another without the explicit consent of the latter.

The constitutionally guaranteed right to the confidentiality of communications and the obligations arising from it, including the legislation governing it, extends to relations between individuals. Presidential Decree 47/2005 regarding the procedures, as well as the technical and organizational guarantees for the removal of the confidentiality of information and its guarantee, establishes an explicit obligation to decrypt information.⁵²² Specifically, in relation to network providers, electronic communications services and their end users, providers using encryption, compression or encryption methods, when performing an obligation arising from the removal of confidentiality, are bound to deliver or transmit the requested data in decrypted form.

It should be noted that specifically the encryption and decryption of private messages remains largely unregulated in the Greek legal order.

8.3. Greek case law on decrypting private messages

In general, the Greek courts were on multiple occasions required to judge upon the legitimacy of lifting the protection of private communications in the context of civil and criminal proceedings, without, however, having to deal with the decryption of private messages per se. It is widely accepted by Greek jurisprudence that the protection of communications does not involve only paper-based communications such as letters, but also communications exchanged in a digital

⁵¹⁹ Greek Law 2168/1993.

⁵²⁰ Greek Law 1729/1987.

⁵²¹ Article 370 of the Greek Penal Code.

⁵²² Greek Presidential Decree 47/2005.

environment.⁵²³ Most commonly, the dilemma between protecting privacy and safeguarding the legal order has emerged in cases when an individual's reputation was harmed online, as well as in cases of combating child pornography.

Such an example is Decision 613/2016 of the First-Instance Judicial Council of Athens where the decryption of files stored in the cloud was required to establish the defendant's possession of pornographic material involving children. In this case, the Court ruled that such decryption should take place, according to the provisions of Article 4 par. 4 and 5 of the Greek Law 2225/1994. Noting that most cloud servers recognise the need to cooperate with the authorities in case a crime has been committed, the Court underlined that since the decryption would take place in the context of a specific and not widespread investigation involving one individual, the server would have to comply with providing the information requested by the authorities.⁵²⁴

In numerous occasions, the authorities have upheld that in order for the communications to be rendered accessible to the law enforcement bodies, the conditions stipulated in the law must be met, notably the competent Court must issue the relevant order, after having verified that solving the case or uncovering the defendant's address would be impossible or near to impossible, without lifting the protection framework, thus upholding the principle of proportionality.⁵²⁵ Of course, if such communication material is received without the legal conditions being upheld, it cannot be taken into consideration during the criminal proceedings and must be entirely disregarded, otherwise the proceedings shall be nullified.⁵²⁶

On that note, message exchanges on social media cannot be brought before a court by third parties not participating in the conversation at hand, unless there are no other effective means of proving their claims, always upholding the principle of proportionality. The situation is different regarding the parties to the conversation, who can submit communications between them in judicial proceedings involving them.⁵²⁷ Besides, the court file involving messages data is not considered as falling within the scope of "storing data in a file", which is not allowed without the party's consent.⁵²⁸

In spite of the Council of the State's opinion that the communication must be protected in its totality, including information identifying it,⁵²⁹ disclosing external information of the communication, such as the IP address and the holder's identity has been judicially excluded from the protection framework, as it was deemed not to fall within the scope of personal data.⁵³⁰

⁵²³ Greek Court of Cassation Decision 1/2017.

⁵²⁴ Ioannis Igglezakakis, "Lifting the communication protection when the data stored on the cloud are the subject of a criminal investigation", (Lawspot, 24 March 2017)

<https://www.lawspot.gr/nomika-nea/arsi-aporritoy-otan-antikeimeno-ereynas-apoteloy-n-dedomena-poy-einai-apo-thikeymena-se?fbclid=IwAR3A7tifpikPYAZEyIPEN_ryLZgonKH23TN-11vTudKnVIa7f7alCLYhZuE> accessed 21 February 2021.

⁵²⁵ Legal Opinion of the Prosecutor of the Greek Court of Cassation (Areios Pagos) 2/2017.

⁵²⁶ Greek Court of Cassation Decision 287/2018.

⁵²⁷ Single Member Court of First Instance of Heraklion Decision 8/2019.

⁵²⁸ Ioannis Igglezakakis, "Intervention to a personal data file (opinion)" (2013) PoinDik 10/2013.

<http://www.cybercc.gr/m/filer_public/2014/06/30/igglezakhs_dedomena_prosopikou_xaraktira.pdf> accessed 21 February 2021.

⁵²⁹ Greek Council of the State Decision 1593/2016.

⁵³⁰ Legal Opinion of the Prosecutor of the Greek Court of Cassation 12/2009.

As such, said information shall be provided by phone and web services hosts without meeting the above-mentioned legal conditions, in order for the authorities to verify crimes taking place online.⁵³¹

Furthermore, phone services providers have been deemed responsible for not properly protecting the privacy of their users against hacking attacks, as they were expected to use effective encryption methods to protect the content of communications and hold proper records to ensure that any such attacks would not take place in the future.⁵³² Similarly, the Court of Cassation has judged that employers shall not maintain any emails sent by their employees' personal email addresses in their hardware.⁵³³

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

It is undebatable that technology and digital advancements have dynamically entered everyday life, drastically altering all its facets. Nonetheless, as the use of new technologies in all aspects of human life increases, so does its abuse at the expense of fundamental human rights. It is in that context that not only the case law of the European Court of Human Rights, but also the Greek legal order has already emphasized on multiple occasions the value of law as a counterweight to technological developments.

Such an example is the case *Shimovolos v. Russia*,⁵³⁴ where the Court highlighted that a domestic law permitting the collection and processing of personal data, such as the movement of an individual by train or air, in a “surveillance database”, must indicate with sufficient clarity the scope and manner of the collection of said personal data. The Court also held that the law must provide guarantees to the public against any breaches or abuses. Otherwise, there is a violation of Article 8, stipulating the right to respect for private life, and Article 5, regarding the right to liberty and security.

Furthermore, in the case *Lopez Ribalda and Others v. Spain*,⁵³⁵ where the court opined that there was no violation of Article 8, it was stated that a measure like video surveillance without prior notification, despite such a legal requirement, can be justified because of “a reasonable suspicion of serious misconduct and to the losses involved, taking account of the extent and the consequences of the measure”. Taking this into account, the Court concluded that the use as evidence of a video recorded under such circumstances in trial proceedings does not violate the right to a fair trial provided for in Article 6 paragraph 1.

In case *Ben Faiza v. France*,⁵³⁶ on the other hand, the authorities had installed a geolocation device on a suspect's vehicle, because of their involvement in criminal offences. Although the geolocation measures were implemented for the purpose of preventing criminal offences, the Court highlighted the fact that French law had not clearly set limitations to the authorities'

⁵³¹ Greek Court of Cassation Decision 1093/2018.

⁵³² Greek Council of State Decision 4309/2015.

⁵³³ Greek Court of Cassation Decision 1/2017.

⁵³⁴ *Shimovolos v. Russia*, App no. 30194/09 (ECHR, 21/06/2011).

⁵³⁵ *Lopez Ribalda and others v. Spain*, App no. 1874/13 and 8567/13, (ECHR, 17/10/2019).

⁵³⁶ *Ben Faiza v. France*, app no. 31446/12, (ECHR 08/02/2018).

margin of discretion. The limitations to the power of the authority that are provided by law constitute the minimum protection of the civilian offered by the rule of law.

In Greece, however, the digitization process is still at an early stage. According to the European Commission's Digital Economy and Society Index (DESI) 2020,⁵³⁷ Greece places in the 27th place out of the 28 EU Member States. Said ranking is calculated upon evaluating aspects of the digitalization such as connectivity, human capital, digital public services, and the integration of digital technology by business, as well as the use of the internet. In particular, it was found that although 85 percent of citizens are Internet users, it is only a few that conduct their daily transactions through it, since, indicatively, only 40 percent of Internet users in Greece use the Internet for e-banking, while only 51 percent of users benefit from online shopping, a percentage which is ostensibly below the EU average of 71%. At the same time Businesses have not adequately integrated into the new digital reality either, as only 12 percent of businesses use big data or cloud services. In the Digital public services dimension, the rank of Greece is below the average of the EU too. Consequently, the issues that have arisen due to digital advancements applications and received judicial resolution are more limited.

However, human rights concerns have already emerged. Indicatively, the focus will be centred around the effect of the use of technology during the pandemic regarding personal data, the application of face-scan at the Greek borders and the human rights issues have been raised respectively, including as far as the use of new technologies and the risk of discrimination are concerned. Lastly, the effect of block chain in economic freedom will be ascertained.

Covid-19 and data protection

Ever since the emergence of the COVID-19 pandemic, technology is being considered as a crucial tool to support the fight against the spread of the virus. Among the most remarkable practices that are applied lies the use of Internet of Things technologies in order for an international platform to be created, enabling the exchange of COVID-19 pandemic statistics and the deployment of Artificial Intelligence to achieve the diagnosis of COVID-19 suspected cases through the initial screening method.⁵³⁸ However, the application of many practices required an intensive process of civilians' personal data, such as in the cases of countries employing Contact Tracing Apps.⁵³⁹

Of course, such measures have not been implemented without raising important human rights related issues, with the right to privacy appearing to be most in jeopardy, presenting the dilemma of whether privacy should be sacrificed on the altar of public health protection or whether it is possible to balance the protection of citizens' health and privacy.⁵⁴⁰ Andrea Jelinek Chairwoman of the European Data Protection Board in the Statement on the processing of personal data in

⁵³⁷ European Commission, Digital economic and society Index 2020 Greece, (2020).

<<https://ec.europa.eu/digital-single-market/en/scoreboard/greece>> accessed 28 February 2021.

⁵³⁸ Ting, D.S.W., Carin, L., Dzau, V. et al. Digital technology and COVID-19. Nat Med 26, 459–461 [2020] <www.nature.com/articles/s41591-020-0824-5> accessed 28 February 2021.

⁵³⁹ Contact Tracing Apps, Council of Europe, (2020) <www.coe.int/en/web/data-protection/contact-tracing-apps> accessed 28 February 2021.

⁵⁴⁰ Spyros Tasis, 'Pandemic and Privacy', [2020], Constitutionalism, <www.constitutionalism.gr/2020-06-tassis-pandimia-idiotikotita/> accessed 28 February 2021.

the context of the COVID-19 outbreak stated that data protection rules (such as the General Data Protection Regulation) do not hinder taking intrusive measures in the fight against the coronavirus pandemic. Even so, the European Data Protection Board would like to underline that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects. Emergency is a legal condition which may legitimize restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period.⁵⁴¹ PACE's rapporteur on Artificial Intelligence in healthcare, Selin Sayek Böke, supports that there is no reason to be obliged to choose between health and privacy, as both can be achieved.⁵⁴² According to GDPR⁵⁴³ and relevant established case law, the right to privacy is not absolute.

In Greece most of the measures applied involve massive data processing, in a way that serious concerns about the right to privacy of Greek citizens emerge. One of such measures is air surveillance through drones. In a press conference held on 22 March 2020, the Minister of Citizen Protection invoked the need of compliance with the lockdown measures as the reason that dictated the need to use drones.⁵⁴⁴ On that note, UNICEF drafted a relevant report, concluding that the use of drones could be a viable solution in the fight against the pandemic, extending their use to other purposes, such as transportation and aerial spraying, as well. UNICEF also highlighted the need of adopting this measure in an appropriate regulatory framework, taking into consideration the potential and a sustainability plan. Countries such as Italy, France, Spain and the UK have also used drones for surveillance.⁵⁴⁵

Besides the feasibility assessment, the use of drones is a measure that allows the collection, processing, sharing and storage of civilian's data. The legal provisions that enable interferences like this must be examined in combination with citizens' right to privacy, data protection, freedom of expression and assembly. In Greece, Presidential Decree 98/2019 on the Organization and structure of Drone Service allows the use of drones. Before the provision of Presidential Decree 98/2019, drones couldn't be deployed in operations involving surveillance.⁵⁴⁶

⁵⁴¹ European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak, 2019
<https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_el> access 28 February 2021.

⁵⁴² Parliamentary Assembly, 'COVID-19: 'We are not forced to choose between health and privacy, we can have both' says PACE rapporteur'(2020) , <<https://pace.coe.int/en/news/7893/covid-19-we-are-not-forced-to-choose-between-health-and-privacy-we-can-have-both-says-pace-rapporteur>> accessed 28 February 2020.

⁵⁴³ Regulation of the European parliament and the Council 2016/679 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 L 119/1.

⁵⁴⁴ Greek General Secretariat for Citizens' Protection, Common Press Conference for the limitation of citizens' circulation in the Greek territory due to Covid-19, (2020),
<www.civilprotection.gr/el/koini-synenteyxi-typoy-gia-ton-periorismo-kykloforias-politon-se-oli-tin-epikrateia-logo-koronoioy> accessed 28 February 2021.

⁵⁴⁵ Unicef, How drones can be used to combat COVID-19, [2020]
<www.unicef.org/supply/documents/how-drones-can-be-used-combat-covid-19> accessed 28 February 2021.

⁵⁴⁶ Greek Presidential Decree 98/2019.

The European Union Agency for fundamental rights (FRA)⁵⁴⁷ and EDRI⁵⁴⁸ networks have already assessed the above-described legal framework on the use of drones in Greece, highlighting important issues. First, the cases in which drones can be used are not restrictively described in the law, leading to the Greek authorities' provision of a wide margin of discretion. This is further enhanced by the fact that no prior authorization is required. As EDRI mentions, given the permission of the use of drones indiscriminately, the state surveillance in public spaces is likely to increase and create a serious interference with human rights, such that could lead to the creation of an omnipresent state surveillance. In addition, although the use of drones and data storing fall within the scope of both European and national data protection legislation, the decree does not provide any reference to the legislation. At the same time, it has been noticed that there are no provisions on the potential abusive use of drones or possible data breaches.

The imposition of the lockdown also entailed a general prohibition on the movement of citizens, providing for derogations by obtaining a movement certificate. Citizens wishing to move for one of the exceptional reasons provided by law are obliged to either fill out the paper form or send an SMS in the number 13033. The message includes the individual's personal information, such as name, surname, home address and the reason of the movement, corresponding to a number system. Movements without a certificate of movement via SMS is fined accordingly.

The above measure is of particular legal interest to the extent that citizens share their personal data via SMS, with the above procedure constituting a collection and processing of personal data that falls within the regulatory scope of legislation concerning the protection of personal data.

The General Secretariat for Civil Protection, recognizing its legal position, as responsible for the processing of personal data, issued the Privacy Policy to comply with its obligations under Law 4624/2019 on Personal Data Protection Authority, measures implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to data processing. With the Privacy Policy, the General Secretariat for Civil Protection complies with the basic principles that should govern the protection of personal data. These are the Principles of legality, objectivity and transparency, the Principle of limitation of purpose, Principle of data minimization, Principle of limitation of the storage period.⁵⁴⁹

In compliance with these principles, the General Secretariat for Civil Protection emphasizes that the data collected are in fact absolutely necessary for the fulfilment of the purpose of public interest invoked, which is the protection of health and the avoidance of the spread of the virus. It is also clarified that the data are retained for a time starting from the dispatch to the receipt of the exit certificate received by the citizen, then either deleted or anonymised and kept only for

⁵⁴⁷ European Union Agency for Fundamental Rights, Coronavirus pandemic in the EU – Fundamental Rights Implications, [2020] <<https://fra.europa.eu/en/country-data/2020/coronavirus-covid-19-outbreak-eu-fundamental-rights-implications-april-2020>> accessed 28 February 2021.

⁵⁴⁸ EDRI, COVID-Tech: COVID-19 opens the way for the use of police drones in Greece [2020] <<https://edri.org/our-work/covid-tech-covid-19-opens-the-way-for-the-use-of-police-drones-in-greece/>> accessed 28 February 2021.

⁵⁴⁹ Article 5 of the GDPR <www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-5-genikos-kanonismos-gia-tin-prostasia-dedomenon-arhes> accessed 28 February 2021.

statistical purposes. Finally, it is ensured that data subjects can invoke the rights of which they are holders in accordance with the above-described legal framework.

The effort of the General Secretariat of Civil Protection to comply with the conditions of lawful processing of data, as set by the relevant legislation, is a guarantee to avoid abuse of this measure to the detriment of fundamental rights of citizens and in particular with the right to privacy.

However, the Greek organization Homo Digitalis is not in total agreement with the above. The main concerns focus on the transparency of the processing. First, the protection policy does not specify the executor of the processing. At the same time, it seems contradictory to report that the data is accessed by the cooperating providers within the service, while at the same time it is explicitly stated that the data is not transferred to third parties. It was also observed that the contact details of the data protection officer are not provided. To ensure the protection of citizens' rights and the legality of the processing of the data, Homo Digitalis shared its observations with the General Secretariat for Civil Protection.⁵⁵⁰ However, a response was never received, and no improvement was noted. This omission motivated the organization to request an opinion from the Greek Data Protection Authority, which has not been published until May 2021.⁵⁵¹

Furthermore, the National Register of Patients with Covid- 19 collects all data from patients having contracted the covid-19 virus.⁵⁵² The purpose of the measure is considered to be the immediate and effective recording of cases and the assessment of the epidemiological situation prevailing in the country.

The National Patient Registry was established with Article 29 of the Legislative Act of March 30, 2020⁵⁵³ 'Measures to deal with the COVID-19 coronavirus pandemic and other urgent provisions. According to Article 29, the purpose of the measure is the immediate and effective recording of cases, the assessment of the epidemiological situation prevailing in the country and the automation of the process of issuing referrals for the examination of the coronavirus COVID-19. At the same time, regarding the same measure, Joint Ministerial Decision 2650/2020⁵⁵⁴ has been issued, regulating more specific technical issues.

The collection of personal data through the National Patient Registry is a measure falling within the regulatory framework of the protection of personal data. Thus, the Ministry of Health is defined as the executor of the processing is the "Electronic Government of Social Security IDIKA SA". At the same time, the personal data collected are clarified, namely the patient's name, age, sex, underlying diseases, and state of health, with the latter falling within the scope of sensitive data. According to Article 3 of decision 2650/10.04.2020 of the Ministers of Health and Digital Governance, the data collected are to be kept indefinitely and they can be kept for an

⁵⁵⁰ Homo digitalis, Open Letter to for the Protection Policy of 13033, [2020] <www.homodigitalis.gr/posts/5357> accessed 28 February 2021.

⁵⁵¹ Homo digitalis, Reports for violations of the GDPR by 13033, [2020] < www.homodigitalis.gr/posts/8546> accessed 28 February 2021.

⁵⁵² Lawspot, 'National COVID-19 Patients Registry: Foundations and main operation elements' [2020] <www.lawspot.gr/nomika-nea/ethniko-mitroo-asthenon-apo-ton-koronoio-covid-19-systasi-kai-vasikes-parametroi> accessed 28 February 2021.

⁵⁵³ Greek Legislatively Act of 30.03.2020.

⁵⁵⁴ Greek Joint Ministerial Decision 2650/2020.

additional period of 20 years after the individual's death. As is obvious, this highly extended retention period raises several issues. Since, as was emphasised in the case *Digital Rights Ireland*,⁵⁵⁵ the retention period is a crucial aspect when estimating the proportionality of a measure, in this case such an indefinite retention period could be considered as disproportionate.

What is more, the Greek state has applied techniques of automated decision making. "COVID 19 Symptom Checker", for instance, a local initiative of the Regional Governor of Attica, is a platform that estimates the possibilities of getting infected by the virus. The individuals share personal information in the platform, such as age and gender, their social environment, and their current state of health.⁵⁵⁶ The platform automatically processes the data and categorizes individuals according to their likelihood of contracting the virus, while personalized advice about the virus is also provided. The platform is powered by DOCANDU, a virtual diagnostic app for many diseases, using artificial intelligence and Geographic Information Systems (GIS).

The measure of the Passenger Locator Form is also worth noting. Travellers that come to Greece from abroad must answer a questionnaire, providing biographical information and information about their country of residence and their previously visited countries. This information is processed, and travellers receive a specific barcode⁵⁵⁷. When they arrive in Greece, the barcode is scanned, and the outcome of the scanning determines whether travellers should be tested for Covid-19. Algorithm Watch doubts about the efficacy of the Passenger Locator Form, especially given that traveller's health condition is not among the data that is evaluated.⁵⁵⁸

Although the use of technology during the pandemic and the massive data collection carried out by the Greek state raise major concerns for the protection of the right to privacy, the pandemic has made digitisation one of the country's priorities. Initiatives were taken by the State in several aspects of life. Teleworking was supported by the development of a Virtual Private Network for teleworking of public services. Almost 10.000 employees have worked via this network during the pandemic. In distance learning, technology was proven a valuable tool too. The Ministry of Education⁵⁵⁹ launched an online platform, under the name *MathainoumeStoSpiti*, while also providing students with digital educational material and Interactive school books to facilitate distance learning.

The Ministry of Digital Governance has begun providing more than 500 e-services through the recently introduced governmental portal "gov.gr". This portal is to include all services that will be digitalized in the future. The #DigitalSolidarityGR platform is also worth mentioning,

⁵⁵⁵ Case C-293/12, *Digital Rights Ireland V Ireland Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform* (2014), Joined Cases C-293/12 and C-594/12.

⁵⁵⁶ Algorithm Watch, *ADM Systems in the COVID-19 Pandemic: A European Perspective. Country analysis Greece* [2020]

<<https://algorithmwatch.org/en/project/automating-society-2020-covid19/greece/>> accessed 28 February 2021.

⁵⁵⁷ Keep Talking Greece - Greek News in English, Blog, Wit & Drama, "Barcode decides which tourists will be tested at Greece's airports", [2020]

<www.keeptalkinggreece.com/2020/06/28/barcode-decides-which-tourists-will-be-tested-at-greeces-airports>. accessed 28 February 2021.

⁵⁵⁸ *ibid.*

⁵⁵⁹ Unesco, *National learning platforms and tools* [2020]

<<https://en.unesco.org/covid19/educationresponse/nationalresponses>> accessed 28 February 2021.

offering information to citizens and businesses, as well as a variety of e-health services.⁵⁶⁰ Trying to confront the risks that are triggered by the digitalization of the state, a new National Cyber Security Strategy has been developed for the years 2020-2025.

In conclusion, the Greek state, during the pandemic, has been constantly incorporating more and more technologic means of facilitating daily activities. One of the major consequences of this increased use of technological tools has undoubtedly been the conflict caused between the right to privacy and the application of technology to the benefit of public health on multiple levels and occasions.

Nevertheless, the State strives to strike a balance, complying with its obligations under the legislative framework for the protection of personal data. In this way citizens are enabled to react in the event of abuse, invoking the rights deriving from the legislation mentioned above. However, it should be judged in concreto to what extent the legal deficiencies identified, are able to affect the ability of individuals to rely on the guarantees provided to them by the law.

Finally, it should be noted that the Greek state has avoided the use of even more intrusive measures, such as the use of contact tracing apps.

The case with face-scan at the Greek borders

In recent years, there has been a tendency for States to invest in programs involving the processing of biometric data. On that note, the notion of biometric methods is described as the set of techniques of certifying the identity of natural persons through the analysis of their fixed characteristics. Biometric methods can be classified as following: a) techniques based on the analysis of physical or genetic characteristics (such as fingerprints, palm geometry, pupil analysis, facial features, DNA) and b) techniques based on the analysis of behaviour (such as signature, voice, type of typing). The data extracted based on these processes, constitute biometric data, i.e. information, with which the identity of a natural person can be determined.

Typically, the use of such processing systems can mainly serve areas such as law enforcement and public security, military, border control and migration, healthcare and subsidies, civil identity, population registration, voter registration and Commercial applications.⁵⁶¹

Among the most usual functions of biometric data, as described above, is that of facial recognition. Facial recognition is the “automatic processing of digital images which contain the faces of individuals for identification, authentication/verification or categorization of those individuals”.⁵⁶² In the past few years, facial recognition technologies have been boosted from developing data availability, computing power and the growth of complex machine learning algorithms.⁵⁶³

⁵⁶⁰ European Commission, Digital economic and society Index 2020 Greece [2020] <<https://ec.europa.eu/digital-single-market/en/scoreboard/greece>> accessed 28 February 2021.

⁵⁶¹ Thales, “Biometrics: definition, trends, use cases, laws and latest news” [2021] <www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics> accessed 28 February 2021.

⁵⁶² Article 29 Data Protection Working Party (2012), Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192, Brussels, 22 March 2012, 2.

⁵⁶³ European Union Agency for Human Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement [2019]

Facial recognition can fulfil different tasks, the most important of which is the verification or authentication, identification, and categorisation. Verification refers to the process of enabling the comparison of two biometrics templates that it is possible to belong to the same person. This kind of procedure is applied for instance to Automated Border Control (ABC). Identification is defined as the procedure, according to which a person's facial image is compared to others stored in a database for the system to find images that refer to the same person. This procedure is also known as Automated Facial Recognition (AFR). The facial images can usually be obtained through video cameras or the users' smartphones and then the images extracted are compared to those included in the database. This system is referred to as Live Facial Recognition Technology (LFRIT). This use of facial images is used mostly in borders or police stations. Categorization concerns the process of matching individuals to general characteristics, such as age, gender, origin, or even sexual orientation. Facial recognition has evolved in a way that can detect people's emotional states, in this way systems can presumably detect whether a person is lying, a technology already used in the framework of the integrated portable control system (iBorderCtrl) project.⁵⁶⁴

Greece has deployed this digital advancement, mostly to achieve a more efficient way to control migration flows and safeguard the country's borders. Specifically, Greece is part to the EURODAC regulation, which establishes an EU asylum fingerprint database, containing in its database the fingerprints of all asylum applicants from each Member State, as well as prints from persons apprehended in an irregular border crossing.⁵⁶⁵ Greece will also participate in the Europe-wide "Entry/Exit System (EES)" plan. A combined information system for recording data on the entry and exit movements of short-stay Third Country Nationals crossing the external borders of the EU will be established by EES, meant to be put in place in 2022.⁵⁶⁶

Of particular interest are the country's investments in facial recognition technology, in the context of the smart policing policy, as the Hellenic Police (ELAS) concluded a contract regarding the supply of Smart Policing Systems with the company INTRACOM TELECOM amounting to 4 million Euros. The devices, which look like smartphones, will be connected to approximately 20 databases attracting data both from Greek and international sources.⁵⁶⁷ The project that is financially supported by the European Union is to launch by summer 2021. Through this project, the Hellenic Police will be provided with face photo recognition software.⁵⁶⁸

<<https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-cont-ext-law>> accessed 28 February 2021.

⁵⁶⁴ *ibid.*

⁵⁶⁵ European Commission, 'Identification of applicants: The Eurodac Regulation'

< https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en > accessed 28 February 2021.

⁵⁶⁶ European Commission, 'Entry/Exit System (EES)'

<https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/ees_en> accessed 28 February 2021.

⁵⁶⁷ Ayang MacDonald, 'Greek police to introduce mobile biometrics during patrols', [2021] biometric update.com

<www.biometricupdate.com/202102/greek-police-to-introduce-mobile-biometrics-during-patrols> accessed 28 February 2021.

⁵⁶⁸ Homo digitalis, "The use of facial recognition technology by the police is about to take place in Greece", [2019]

Greece also forms part to the iBorderCtrl (Intelligent Portable Control System), a pilot project that will be held up on the Hungarian, Greek, and Latvian borders, expected to contribute to the acceleration and improvement of the efficacy of the border control for third-country nationals crossing the land borders of EU Member States. Software and hardware technologies ranging from portable readers and scanners related to biometric verification, automated deception detection, document authentication, and risk assessment will be included. The project is funded by the European Union's Horizon 2020 research and innovation program.⁵⁶⁹

Such constant monitoring by the authorities may bring obstacles to the free development of the personality, which in the Greek legal order, is constitutionally protected by Article 5. Keeping in mind the ECtHR's confirmation that a person's facial image constitutes one of the most important aspects of his/her personality, as it reveals the person's unique characteristics and distinguishes the person among other individuals, the right to the protection of one's facial image is therefore considered to be one of the essential components of personal development.

Another human rights concern resulting from facial recognition technologies, is the jeopardy of freedom of expression, that is protected by Article 14 paragraph 1 of the Greek constitution, Article 11 paragraph 1 of the Charter of fundamental rights and Article 10 of the ECHR.

Furthermore, it also interferes with the right to assemble and associate, which is protected in Article 11 of the Greek constitution, Article 11 of the ECHR, and Article 12 paragraph 1 of the Charter. The deployment of facial recognition technologies may lead individuals to change their behaviour in public spaces, in a way that they feel limited and discouraged to attend demonstrations because of the sense that they are constantly being watched.

While Greece is investing in such technologies, international human organizations and civil societies' reaction to such initiatives are far from positive, noting that they could turn into a means of widespread government surveillance.⁵⁷⁰ For instance, International Amnesty has launched a campaign named "Ban the scan". Through this campaign, International Amnesty emphasizes the risks that the use of police facial recognition involves, mentioning mostly that the deployment of these technologies may lead to racial policing. Taking account of said risk, International Amnesty asks for a prohibition of deployment, production, and sale of facial recognition technology for surveillance and policing uses.⁵⁷¹

Another notable movement is the #ReclaimYourFace campaign, which is now an official European Citizens' Initiative seeking to protect public spaces from intrusive technologies, such as cameras equipped with face recognition software. This campaign, coordinated by the European Digital Rights Institute (EDRI), has also involved several Greek organizations, such as

< www.homodigitalis.gr/posts/4662 > accessed 28 February 2021.

⁵⁶⁹ Eleftherios Chelioudakis, 'Clarifications sought on human rights impacts of iBorderCtrl' [2018]

< www.edri.org/our-work/greece-clarifications-sought-on-human-rights-impacts-of-iborderctrl/ > accessed 28 February 2021.

⁵⁷⁰ Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., West, S.M., Richardson, R., Schultz, J. and Schwartz, O., AI Now 2018 Report, AI Now Institute [2018]

< https://ainowinstitute.org/AI_Now_2018_Report.html > accessed 28 February 2021.

⁵⁷¹ International Amnesty, 'Ban dangerous facial recognition technology that amplifies racist policing' [2021]

< www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/ > accessed 28 February 2021.

the Hellenic Union for Human Rights, the Hellenic Union for the Protection of Personal Data and Privacy and the Reporters United.⁵⁷²

What is more, 44 organizations have drafted a report, demanding that the Member States stop all current practices and future ambitions for mass surveillance through the use of biometric data, while also providing for a general prohibition on the processing of biometric data and asking the EU to stop funding such programs.⁵⁷³ According to a survey, examining the collection of biometric data in 50 countries worldwide, ranking them from most invasive to the least invasive, conducted by Comparitech, a remote group of 30 researchers that provides information on current technological developments, Greece appears to be on the verge of being evaluated as an invasive country.⁵⁷⁴

While Article 9A of the Greek Constitution guarantees the protection of privacy and personal data, the constitutionally guaranteed protection that it receives is affected by practices such as facial recognition. Yet, Greece's score of 15/31 can easily be explained taking into consideration the current investments in this field.

Ioannis Kouvakas, Legal Officer at the EDRi and member of Privacy International (PI), also warns that the introduction of facial recognition is a radical and dystopian idea, threatening our freedoms and questioning modern societies. As it is a highly intrusive surveillance technique, it can provide authorities with new opportunities to undermine democracy under the cloak of defending it. Even if initiatives like those are a big step for the digitalization of Greece, the use of facial recognition mechanisms undoubtedly raises serious human rights concerns, risking being gradually considered by the average person as something expected and normal.⁵⁷⁵

Concerns are also raised regarding the prohibition of any discrimination, as stipulated by Article 4 of the Greek Constitution, taking into consideration the European Union Agency for Fundamental Human Rights (FRA) declaration that violations of the non-discrimination principle can occur in data-supported algorithmic decision making, such as facial recognition. As the European Union Agency for Fundamental Human Rights has explained, discrimination in data-supported algorithmic decision making can be attributed to several reasons. It can take place during the design, testing and implementation of algorithms used for facial recognition, since the quality of data used to develop algorithms and software hold a crucial position. For effectiveness and accuracy to be achieved, facial recognition software needs to be supplied with vast amounts of facial images, reflecting different groups of people for the sample to be considered properly representing the total of the population. For instance, it is common that facial images used to

⁵⁷² Lawspot, 'Reclaim Your Face: The European citizens' initiative for a future without public surveillance technologies' [2021] Lawspot, <www.lawspot.gr/nomika-nea/reclaim-your-face-i-cyropaiki-protovoylia-politon-gia-ena-mellon-horis-tehnologies> accessed 28 February 2021.

⁵⁷³ Edri, 'Ban biometric mass surveillance!' [2020] <<https://edri.org/our-work/blog-ban-biometric-mass-surveillance/>> accessed 28 February 2021.

⁵⁷⁴ Paul Bischoff, 'Biometric data: 96 countries ranked by how they're collecting it and what they're doing with it' [2021] <www.comparitech.com/blog/vpn-privacy/biometric-data-study/> accessed 28 February 2021.

⁵⁷⁵ Magdalini Skondra, 'Face recognition and personal data' [2020] Lawspot <www.lawspot.gr/nomika-blogs/magdalini-skondra/anagnorisi-prosopoy-face-recognition-kai-prosopika-dedomena> accessed 28 February 2021.

develop algorithms in the Western world represent mostly white men, side-lining women, and individuals of other ethnic backgrounds.

Digital technologies and discrimination

It has already been made evident that, in the current digital economy, data is being produced and processed at unprecedented rates, proving of utmost importance to the further evolution of technological advancements. And while until the COVID-19 crisis, organizations had approached the digital transformation in a fragmented or even uncoordinated manner,⁵⁷⁶ the post pandemic reality has placed Analytic tools and Artificial Intelligence (AI) systems in the spotlight of processing big data for innovation purposes, analysing data collected, unravelling patterns and correlating them accordingly.⁵⁷⁷

It is worth mentioning that, in spite of the common idea around AI systems, involving humanoid robots mimicking human intelligence to an almost perfect degree, current AI is actually a synonym to machine learning, also called “weak AI”, enabling the System to automatically learn from the environment and apply that learning to make better decisions, based on the data supplied.⁵⁷⁸

With the E.U. having launched the Digital Europe Programme and following the declaration on cooperation on Artificial Intelligence, Greece has had to incorporate and demonstrate progress in technological sectors that the country was up to this point lacking.⁵⁷⁹ The private sector was the first to adapt to such technological advancements, with companies active in a range of sectors from energy to online gambling and pharmaceuticals, integrating AI to their main operation schemes.⁵⁸⁰ At the same time, Greece has placed among the top seven countries in the Union’s program for tech-related research and development, Horizon 2020.⁵⁸¹

Especially for the sector of AI systems, as of 2019,⁵⁸² Greece has already begun planning on the relevant national strategy, consulting stakeholders and aiming to ensure their efficacy, as well as their accordance with human rights, such as privacy or equality.⁵⁸³ What is more, the Greek

⁵⁷⁶European Institute of Innovation and Technology, “Digital Transformation in Greece 2020-2021” <https://www.eitdigital.eu/fileadmin/files/2020/publications/EIT-Digital_DT_report_2020-2021.pdf> accessed 23 February 2021.

⁵⁷⁷ Sokratis Katsikas and Vasilios Zorkadis, “E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age” (8th International Conference, e-Democracy 2019, December 2019) <<https://www.springer.com/gp/book/9783030375447>> accessed 23 February 2021.

⁵⁷⁸ Jun Wu, “AI, Machine Learning, Deep Learning Explained Simply” (Towards Data Science, 1 July 2019) <<https://towardsdatascience.com/ai-machine-learning-deep-learning-explained-simply-7b553da5b960>> accessed 25 February 2021.

⁵⁷⁹ Greece 2020 – Factsheet on Digital Transformation <http://iobe.gr/EC_Conference2020/Factsheet_Digital%20Transformation_Greece%20July%202020.pdf> accessed 23 February 2021.

⁵⁸⁰ Chrysos Kavounides, Markos Giakoumelos and Evdokia Kaffe, “Harnessing the power of AI in Greece – Embarking on the path to value” (Boston Consulting Group) <<https://web-assets.bcg.com/93/be/5ac6b7ff4d698947da09681332db/harnessing-the-power-web-final.pdf>> accessed 23 February 2021.

⁵⁸¹ Christian Bodewig and Wolfgang Fengler, “Thriving with technology in Greece” (Brookings, 25 April 2019) <<https://www.brookings.edu/blog/future-development/2019/04/25/thriving-with-technology-in-greece/>> accessed 23 February 2021.

⁵⁸² Ministerial Decision 8056/2019, Establishment of a committee for the examination of repercussions due to the application of Artificial Intelligence in the judicial system.

⁵⁸³ European Commission, “Digital Economy and Society Index (DESI) 2020”.

government introduced legislation transforming the already existing National Bioethics Committee to include matters related to Ethics and Technology in general.⁵⁸⁴ It is worth mentioning that Greece has nine operational innovation centres and digital hubs, focusing, among others, on AI-related matters.

With the pandemic reigning in the everyday agendas, it is not surprising that the effect of big data is also present at the public health sector, where the possible conflicts of public good on one hand and the right to privacy on the other are more thoroughly explored.⁵⁸⁵ Nonetheless, AI systems seem to be incorporating more rapidly in law enforcement and policing practices, as already explained with the example of iBorderCtrl technology that uses AI to detect inconsistencies and lies in migrants' and refugees' stories, as a means to fight crime.⁵⁸⁶

In spite of all positive effects of taking advantage of AI technology to improve the standard of living, there are also various threats arising from their unmoderated use, especially for human rights, with one of the most prominent ones being the right to equality and non-discrimination. Said danger of discrimination appears in almost all applications of AI in everyday life, including even banking and financial services where biased AI decisions based on factors such as sex, ethnicity, among others, can affect an individual's entire financial stability and social potential.⁵⁸⁷

The above-described admission is even more apparent when collecting and matching data about persons involved in criminal activities, which can lead to the creation and proliferation of stereotypes that end up marginalising even further certain population groups, thus intensifying social gaps. Computational systems perform based on data used to train them and their function is limited to connecting data automatically, leading to an automated result that is usually viewed as an accurate depiction of reality and not solely a tendency.⁵⁸⁸

This 'black-box' function of AI is precisely the reason why the justice sector is significantly more hesitant in incorporating AI to judicial proceedings, voicing mostly equality and transparency fears.⁵⁸⁹

At the same time, it would be irrational to disregard the critical role of the Internet in contemporary society, promoting a wide range of human rights and, thus, rendering its access a

⁵⁸⁴ "Greece acquires a National Techno-ethic Committee and National Authority of Accessibility" (Lawspot, 5 January 2021)

<<https://www.lawspot.gr/nomika-nea/ethniki-epitropi-tehnoithikis-kai-ethniki-arhi-prosvasimotitas-apokta-i-ellada>> accessed 23 February 2021.

⁵⁸⁵ Hellenic National Bioethics Commission, "Opinion on Big Data in Health"

<http://www.bioethics.gr/images/pdf/GNOMES/OPINION_Big_Data_FINAL_EN.pdf> accessed 23 February 2021.

⁵⁸⁶ Steven Feldstein, "The Global Expansion of AI Surveillance" (Carnegie, 17 September 2019)

<<https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>> accessed 23 February 2021.

⁵⁸⁷ Giannis Stournaras, "AI and its role in Economy, Business Management-Organisation and the Financial Sector" (Bank of Greece News, 21 February 2020)

<<https://www.bankofgreece.gr/enimerosi/grafeio-typoy/anazhthsh-enhmerwsewn/enhmerwseis?announcement=6baf1721-c2a8-42c2-b4b1-6bb0368c3b52>> accessed 23 February 2021.

⁵⁸⁸ Rafaela Matsouka, "Modern Technology and Human Rights" (September 2019) Panteion University of Social and Political Studies.

⁵⁸⁹ Vasilis Karkatzounis, "AI in Justice: Impressive potential, realistic expectations" (Lawspot, 11 February 2020)

<https://www.lawspot.gr/nomika-blogs/vasilis_karkatzounis/tehniiti-noimosyni-sti-dikaiosyni-entyposiakes-prooptikes> accessed 23 February 2021.

separate crucial human right on its own.⁵⁹⁰ Taking into consideration the strong correlation among the Web and the increase in public participation to decision making processes, it was anticipated that more and more Greek decision making actors would turn to technology to disseminate their views, gain support and educate.⁵⁹¹

However, it is not only the educational part of the Internet that is currently being promoted by the Greek government. In spite of placing at the 27th position out of the 28 EU Member-States on the Digital Economy and Society Index, during the past year Greece has focused all efforts in upgrading their public sector services, transferring a multitude of governmental services in a unified digital platform.⁵⁹²

Furthermore, Greece is significantly slower than the rest of Europe when it comes to making fast broadband available to its citizens, as well as offering government services digitally. Although the digital transformation plan of the Greek government had been put in place since 2014,⁵⁹³ while the relevant law providing for the modernisation of public services has been in force since 2011,⁵⁹⁴ it was the global pandemic that contributed to drastically speeding up the process of digitising the public sector, with the creation of a governmental platform providing 614 different government services to citizens.

It is in this context that the second manifestation of technology and discrimination takes place, creating the so-called “digital divide”,⁵⁹⁵ even though over 50% of Greek citizens claim to possess basic digital knowledge and 78,5% of all households have Internet access.⁵⁹⁶ On one hand, the Greek Constitution states that all persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of’ privacy, personal data and secrecy of correspondence. On the other hand, it is noted that not all population groups have access to the Internet, or even proper education and the technical means to do so, resulting in such groups being excluded from

⁵⁹⁰ Jacopo Coccoli, “The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era” (1 July 2019) PHRG Volume 1, Issue 2

<http://phrg.padovauniversitypress.it/system/files/papers/2017_2_4.pdf> accessed 23 February 2021.

⁵⁹¹ Kalliopi Panagiotidi, “The use of Information and Communication Technology in the citizens’ society”

(September 2016) Panepistimio Peloponnisou

<<https://amitos.library.uop.gr/xmlui/bitstream/handle/123456789/2920/2042016%20%ce%a0%ce%91%ce%9d%ce%91%ce%93%ce%99%ce%a9%ce%a4%ce%99%ce%94%ce%97%20%ce%a0%ce%91%ce%9b%ce%99%ce%9f%ce%a0%ce%97.pdf?sequence=1&isAllowed=y>> accessed 23 February 2021.

⁵⁹² ‘Greece begins digital odyssey as coronavirus crisis sparks innovation’ (Euronews, 6 April 2020)

<<https://www.euronews.com/2020/04/06/greece-begins-digital-odyssey-as-coronavirus-crisis-sparks-innovation>> accessed 23 February 2021.

⁵⁹³ European Commission, “Digital Government Factsheet 2019” (2019)

<https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Greece_2019.pdf> accessed 23 February 2021.

⁵⁹⁴ Law 3979/2011, Government Gazette 138/A/16.06.2011.

⁵⁹⁵ Georgia Paschalidou, “Digital gap and inequalities in the use of new technologies” (2011) University of Macedonia <<https://dspace.lib.uom.gr/bitstream/2159/14899/6/PaschalidouGeorgiaMsc2011.pdf>> accessed 23 February 2021.

⁵⁹⁶ OECD Data, “Greece” <<https://data.oecd.org/greece.htm#profile-innovationandtechnology>> accessed 23 February 2021.

democratic procedures defining their future, with this being only one of the facets of digital exclusion.

Most notably, it is the elderly, the economically disadvantaged minorities and those of a lower educational attainment,⁵⁹⁷ especially if living in rural areas, as well as the vision impaired people whose right to equal participation in a democracy are affected, since the Greek state does not seem to have adequately and sufficiently provided for these groups of citizens to be able to enjoy the benefits of electronic systems. Yet, there are efforts to improve the situation through the establishment of the Digital Academy, as well as Law 4591/2019 aiming to secure the active and equal access to websites and applications of the public sector authorities.

Blockchain and financial freedom

The notion of financial freedom in modern societies, as significantly altered during the past two centuries, is considered by many as the cornerstone of numerous other freedoms and rights. Freedom of expression, the freedom to unhindered develop one's personality are some of the freedoms where financial freedom plays a significant role.

As protected by Article 5 par. 1 of the Greek Constitution, every citizen has the right to freely develop their personality and participate in the social, financial and political life of the country, while not violating the rights of others, the Constitution and the accepted principles of morality. Given the general wording of the article, the forms of financial freedom cannot be described a priori, but only based on the forms already existing. As such, financial freedom has historically taken the following general forms:

1. Contractual freedom, in the sense of freedom to choose the parties and the terms of transacting with others and signing binding documents and agreement, while also taking advantage of one's assets, as confirmed by the Supreme Court of Greece's Decision 26/2003.
2. Business freedom, usually correlated with the freedom of competition
3. Professional freedom, in the sense of choosing the type, place and time of exercising a certain profession, when fulfilling the relevant criteria, which is also viewed as an indispensable element of the freedom to develop one's personality, according to the Greek Council of State's Decision 3665/2005.

In the financial sector, Financial Technology (FinTech), cryptocurrencies, and Smart Contracts have been a reality for some time. Nonetheless, it is only during the past six years that they have begun expanding and affecting society's current economic structures, with more and more states slowly recognising them in their legal orders. It was not until April of 2018 that E.U. Member-States and Norway moved forward with the creation of the European Blockchain Services Infrastructure, meant to support harmonised delivery of cross-border digital public

⁵⁹⁷ Aspasia Treulaki, "Dimensions of the Digital Gap in Greece" National Centre of Social Studies <https://www.ekke.gr/publication_files/diastasis-tou-psifiakou-chasmatos-stin-ellada> accessed 24 February 2021.

services, while also implementing security and privacy standards, and the EU Blockchain Observatory and Forum, investing in blockchain-related projects.⁵⁹⁸

Blockchain technology is viewed by the main actors on a European level as the defining technology of the future, expected to be integrated in all public and financial services and regarded as a means to further promote the protection of personal data, enhancing users' trust in their systems, while also boosting entrepreneurial activity. Since, in practice, Blockchain is a registry where data and information are interconnected by encrypted blocks, creating a chain of reliable information,⁵⁹⁹ it makes sense that such advancements be incorporated in Governance, offering the opportunity to public administration bodies to increase transparency and efficiency, simplifying bureaucratic procedures, and promoting automation.⁶⁰⁰

Revolutionising FinTech, providing the instruments of operation to cryptocurrencies and introducing the possibility of Smart Contracts, Blockchain lies at the centre of all modern financial innovation.⁶⁰¹ It is, thus, evident that such technology can crucially contribute to the ultimate exploitation of the Digital Single Market.

Greece is among the signatory parties to the above EU initiatives. The country's progress and development on the above sectors is taking place in more slow paced compared to the rest of the Union. Along with the country's 5.000 people user base and scarce Media coverage, no state-sponsored initiatives, it is normal that Greece is not a key-actor in the European Blockchain scenery.⁶⁰²

It wasn't until recently that one of the first companies in Greece to adapt to a FinTech environment, Viva, introduced a digital wallet, which can be used by users to store money and transfer it to other private actors or businesses based on the other party's respective wallet, their phone number, their Greek Tax Identification Number or a special barcode.⁶⁰³ This enhances the fact that most companies in the Greek FinTech ecosystem are concentrated on payment services,

⁵⁹⁸European Commission, "European countries join Blockchain Partnership" (10 April 2018) <<https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership>> accessed 24 February 2021.

⁵⁹⁹ Kostas Mavraganis, "Survey: Greece's and Cyprus' position in the world of blockchain and bitcoins" (Huffington Post, 9 December 2019) <https://www.huffingtonpost.gr/entry/ereena-e-these-tes-elladas-kai-tes-keproe-ston-kosmo-toe-blockchain-kai-to-n-bitcoins-gr_5fcfd50dc5b63a1534555f5b> accessed 24 February 2021.

⁶⁰⁰Georgios Panou, "Blockchain Opportunities for public administration and e-Governance" (Medium, 23 May 2019) <<https://medium.com/hellenic-blockchain-hub-el/blockchain-opportunities-for-public-administration-and-e-governance-9th-mobile-world-conference-e92c1bbc82f>> accessed 24 February 2021.

⁶⁰¹Fernandez-Vazquez S, Rosillo R, De La Fuente D, Priore P, "Blockchain in FinTech: A Mapping Study" (2019) Sustainability 11(22):6366 <<https://doi.org/10.3390/su11226366>> accessed 24 February 2021.

⁶⁰²The European Union Blockchain Observatory & Forum, "EU Blockchain Ecosystem Developments" (Huffington Post) <<https://big.assets.huffingtonpost.com/athena/files/2020/12/08/5fcfd780c5b6787f2a9b6ce4.pdf>> accessed 24 February 2021.

⁶⁰³ Eirini Kardara, "Legal approach of cryptocurrencies and Blockchain" (2020) University of Patras <<http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/8237/LOG%20-%20%CE%9A%CE%91%CE%A1%CE%94%CE%91%CE%A1%CE%91%20%CE%95%CE%99%CE%A1%CE%97%CE%9D%CE%97.pdf?sequence=1&isAllowed=y>> accessed 24 February 2021.

in spite of its potential for financial growth, with predictions placing the increase of GDP between 1% and 3,9%.⁶⁰⁴

Particularly as far as cryptocurrencies are concerned, the interest in Greece was mainly expressed in 2015, when banking restrictions were placed, leading multiple businesses to explore alternatives.⁶⁰⁵ Nonetheless, Greece has not up to this point passed any relevant legislation, while in terms of taxation, cryptocurrencies are taxed as capital gains on income, calculated upon the difference between the purchase value minus the liquidation value.⁶⁰⁶ Though Greek Law 4261/2014 has adapted EU Directive 2009/110 regarding electronic money, cryptocurrencies diverge from the definition of electronic money as provided in the Directive, as the monetary amounts are not expressed in a specific state's currency unit, but on a virtual unit, such as Bitcoin.⁶⁰⁷

Yet, in 2018 the first cryptocurrency of Greek origin, ParkGene, entered the market, aiming to alter the car parking system,⁶⁰⁸ with more start-up companies and the Hellenic Blockchain Hub initiative following. At the same time, the Hellenic Capital Market Commission, and the Bank of Greece, with the FinTech Innovation Hub Initiative, are combining efforts to understand and eventually provide a regulatory framework for the relevant assets.

With effective governance institutions being associated with a greater likelihood of a less restrictive regulatory stance on cryptocurrency, according to researchers, taking into consideration bureaucratic quality, a calculated governance indicator index, democratic institutions, and financial freedom, it seems obvious that more steps need to be made towards that result. Besides, it would be impossible for a State aiming to protect the financial freedom of its citizens to exclude them from globally widespread practices and technologies that directly fall within the scope of freely exercising financial activity and profiting from them.

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?

From the aforementioned analysis of the protection of human rights in the Greek legal order it becomes clear the developments taking place at international and, more importantly, at EU level have significantly shaped the protection of personal information in Greece and have acted as a catalyst for the introduction of new laws or for the amendment of existing ones. The regulatory

⁶⁰⁴ “The sector of Fintech and its importance for Greece” (Capital, 17 September 2018) <<https://www.capital.gr/oikonomia/3316484/o-klados-fintech-kai-i-simasia-tou-gia-tin-ellada>> accessed 24 February 2021.

⁶⁰⁵ P. Dimitrakos, “Cryptocurrency: an emerging tool of financial freedom” The American College of Greece. <https://www.acg.edu/ckeditor_assets/attachments/2063/kriptonomismata.pdf> accessed 24 February 2021.

⁶⁰⁶ Konstantinos Mpotsis, “Bitcoin and taxation of cryptocurrency » (FinHub, 9 February 2021) <<https://finhub.gr/bitcoin-kai-forologia-sta-kriptonomismata/>> accessed 24 February 2021.

⁶⁰⁷ Case C-264/14, Skatteverket v David Hedqvist [2015] ECJ <<http://curia.europa.eu/juris/liste.jsf?num=C-264/14>> accessed 24 February 2021.

⁶⁰⁸ Vaggelis Mandravelis, “The first Greek cryptocurrency circulated the market” (Kathimerini, 18 January 2018) <<https://www.kathimerini.gr/economy/local/943892/kykloforise-stin-agora-to-proto-elliniko-kryptonomisma/>> accessed 24 February 2021.

experience of technology, and more specifically of personal data and privacy, has highlighted the shortcomings of traditional 'command and control' approaches, revealed the difficulty of finding a precise regulatory target and given rise to the use of new types of legal instruments apart from classic state law (e.g., self-regulation, soft law). More importantly, perhaps, it has underlined the need for cooperation and the limits of nation states as the main actors with regulatory power, due to the international aspect of the digital world (e.g., in enforcement). Data-intensive technologies, such as artificial intelligence applications, contribute to creating a digital environment in which enterprises are increasingly able to track, analyze, predict, and even manipulate people's behavior to an unprecedented degree. These technological developments carry very significant risks for human dignity, autonomy and privacy and the exercise of human rights in general. It is sure that the legislation will defend the rights of the weak and will apply effective safeguards in the future. As a result, and taking into account that the regulatory issues related to new technologies are only expected to increase and become even more complicated and even more controversial in the coming years, the cooperation at EU -and even international-level appears to be a crucial element for the development of a successful, stable and efficient regulatory approach.

Table of legislation

Provision in Greek Language	Corresponding Translation in English
Σύνταγμα της Ελλάδας Άρθρο 4: Οι Έλληνες είναι ίσοι ενώπιον του νόμου. Οι Έλληνες και οι Ελληνίδες έχουν ίσα δικαιώματα και υποχρεώσεις. Άρθρο 5 παρ 2: Όλοι όσοι βρίσκονται στην Ελληνική Επικρατία απολαμβάνουν την απόλυτη προστασία της ζωής, της τιμής και της ελευθερίας τους, χωρίς διάκριση εθνικότητας, φυλής, γλώσσας και θρησκευτικών ή πολιτικών πεποιθήσεων. Εξαιρέσεις επιτρέπονται στις περιπτώσεις που προβλέπει το διεθνές δίκαιο. Άρθρο 9Α Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει. Άρθρο 94: 1. Στο Συμβούλιο της Επικρατείας και τα τακτικά διοικητικά δικαστήρια υπάγονται οι διοικητικές διαφορές, όπως νόμος ορίζει, με την επιφύλαξη των αρμοδιοτήτων του Ελεγκτικού Συνεδρίου. 2. Στα πολιτικά δικαστήρια υπάγονται οι ιδιωτικές διαφορές, καθώς και υποθέσεις εκούσιας δικαιοδοσίας, όπως νόμος ορίζει. Άρθρο 95: Στην αρμοδιότητα του Συμβουλίου της Επικρατείας ανήκουν ιδίως: α) Η μετά από αίτηση ακύρωση των εκτελεστών πράξεων των διοικητικών αρχών για υπέρβαση εξουσίας ή για παράβαση νόμου. Άρθρο 116: Δεν αποτελεί διάκριση λόγω φύλου η λήψη θετικών μέτρων για την προώθηση της ισότητας μεταξύ ανδρών και γυναικών. Το Κράτος μεριμνά για την άρση των ανισοτήτων που	Greek Constitution Article 4: ‘All Greeks are equal before the law’. ‘Greek men and women have equal rights and equal obligations’). Article 5(2): ‘All persons living within the Greek territory shall enjoy full protection of their life, honour and liberty irrespective of nationality, race or language and of religious or political belief’). Article 9A All persons have the right to be protected from the collection, processing, and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law. Article 94: 1. Administrative disputes, as provided by law, are subject to the Council of State and the regular administrative courts, without prejudice to the responsibilities of the Court of Auditors. 2. Private disputes, as well as cases of voluntary jurisdiction, as provided by law, are subject to civil courts. Article 95: The competence of the Council of State includes in particular: a) The annulment upon request of the executive acts of the administrative authorities for exceeding power or for violation of law. Article 116: It does not constitute gender discrimination to take positive steps to promote equality between men and women. The State takes care to remove the inequalities that exist in practice, especially to the detriment of women.

υφίστανται στην πράξη, ιδίως σε βάρος των γυναικών.	
Νόμος 4624 Τεύχος Α' 137/29.08.2019 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις. Άρθρο 29 παρ. 4 Κατά παρέκκλιση των οριζόμενων στα άρθρα 18 παράγραφος 1 εδάφια α', β' και δ' και στα άρθρα 20 και 21 του ΓΚΠΔ, τα δικαιώματα του υποκειμένου των δεδομένων περιορίζονται, εφόσον η άσκησή τους είναι πιθανό να καταστήσει αδύνατη ή να παρακωλύσει σοβαρά την εκπλήρωση των σκοπών της παραγράφου 1 και εφόσον οι περιορισμοί αυτοί κρίνονται απαραίτητοι για την επίτευξη των σκοπών αυτών. Άρθρο 30 παρ. 2 Κατά παρέκκλιση των οριζόμενων στα άρθρα 15, 16, 18 και 21 του ΓΚΠΔ, τα δικαιώματα του υποκειμένου των δεδομένων προσωπικού χαρακτήρα περιορίζονται, εφόσον η άσκησή τους είναι πιθανό να καταστήσει αδύνατη ή να παρακωλύσει σοβαρά την εκπλήρωση των σκοπών της παραγράφου 1 και εφόσον οι περιορισμοί αυτοί κρίνονται απαραίτητοι για την εκπλήρωσή τους. Για τον ίδιο λόγο δεν εφαρμόζεται και το προβλεπόμενο στο άρθρο 15 του ΓΚΠΔ δικαίωμα πρόσβασης του υποκειμένου, όταν τα δεδομένα προσωπικού χαρακτήρα είναι απαραίτητα για επιστημονικούς σκοπούς και η παροχή πληροφοριών απαιτεί δυσανάλογη προσπάθεια. Άρθρο 33 παρ. 5 Η υποχρέωση γνωστοποίησης σύμφωνα με το άρθρο 34 του ΓΚΠΔ, εκτός από την αναφερόμενη στην παράγραφο 3 του άρθρου 34 του ΓΚΠΔ εξαίρεση, δεν ισχύει στον βαθμό που μέσω της	Law 4624 Series A/Issue 137/29.08.2019 Hellenic Data Protection Authority (HDP), measures for implementing 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 transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions. Article 29 para. 4 By way of derogation from subparagraphs (a), (b) and (d) of Article 18(1), and from Articles 20 and 21 of the GDPR, the rights of the data subject shall be restricted where their exercise is likely to render impossible or seriously impair the achievement of the objectives referred to in paragraph 1 and where such limitations are deemed to be necessary for the achievement of such objectives. Article 30 para. 2 By way of derogation from the provisions of Articles 15, 16, 18 and 21 of the GDPR, the rights of the data subject shall be limited where their exercise is likely to render impossible or seriously impair the achievement of the objectives referred to in paragraph 1 and where such limitations are deemed to be necessary for their achievement. For the same reason, the data subject's right of access provided for in Article 15 of the GDPR shall not apply where personal data are necessary for scientific purposes and the provision of information would entail a disproportionate effort. Article 33 para. 5 The obligation to notify under Article 34 of the GDPR, with the exception of the exemption referred to in Article 34(3) of the GDPR, shall not apply to the extent that the obligation to notify would entail the disclosure of information which, according to the law or by reason of its nature, in particular due to overriding legitimate interests of

γνωστοποίησης θα αποκαλύπτονταν πληροφορίες, οι οποίες σύμφωνα με διάταξη νόμου ή λόγω της φύσης τους, ιδίως λόγω των υπέρτερων έννομων συμφερόντων τρίτου, πρέπει να παραμείνουν απόρρητες. Κατά παρέκκλιση από το προηγούμενο εδάφιο το υποκείμενο των δεδομένων προσωπικού χαρακτήρα πρέπει σύμφωνα με το άρθρο 34 του ΓΚΠΔ να ενημερώνεται, όταν τα συμφέροντά του, λαμβάνοντας ιδίως υπόψη τις επαπειλούμενες ζημιές, υπερτερούν του συμφέροντος διατήρησης του απορρήτου. Άρθρο 19: (Απόρρητο επιστολών, ανταπόκρισης & επικοινωνίας) 1. Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.	third parties, should remain confidential. By way of derogation from the previous subparagraph, the data subject must be informed, in accordance with Article 34 of the GDPR, where his or her interests, considering imminent damage, override the interest relating to maintaining confidentiality. Article 19 (Confidentiality of letters, responses & communications) 1. Secrecy of letters and all other forms of free correspondence or communication shall be inviolable. The guaranties under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating especially serious crimes, shall be specified by law.
Αστικός Κώδικας ΠΔ 456/1984 Άρθρο 57 Δικαίωμα στην προσωπικότητα Όποιος προσβάλλεται παράνομα στην προσωπικότητά του έχει δικαίωμα να απαιτήσει να αρθεί η προσβολή και να μην επαναληφθεί στο μέλλον. Αν η προσβολή αναφέρεται στην προσωπικότητα προσώπου που έχει πεθάνει το δικαίωμα αυτό έχουν ο σύζυγος, οι κατιόντες, οι ανιόντες, οι αδελφοί και οι κληρονόμοι του από διαθήκη. Αξίωση αποζημίωσης σύμφωνα με τις διατάξεις για τις αδικιοπραξίες δεν αποκλείεται. Άρθρο 914 Αστικού Κώδικα Έννοια Αδικοπραξίας Όποιος ζημιώσει άλλον παράνομα και υπαίτια έχει υποχρέωση να τον αποζημιώσει. Άρθρο 932 Αστικού Κώδικα Ικανοποίηση της ηθικής βλάβης Σε περίπτωση αδικιοπραξίας, ανεξάρτητα από την αποζημίωση για την περιουσιακή ζημία, το δικαστήριο μπορεί να επιδικάσει εύλογη κατά την	Civil Code 456/1984 Article 57 Personality Right When someone's personality right is violated without legal cause, they have the right to demand the violation to be stopped and not to be repeated it in the future. If the violation concerns the personality of a dead individual, their family has this right. Right to compensation according to the provisions of delict is not excluded. Article 914 of Civil Code 456/1984 Definition of Delict When someone has provoked damage to someone else illegally and by fault, they have the obligation to compensation. Article 932 of Civil Code 456/1984 Reimbursement of moral damage In case of delict, except from the compensation for material damages, the court can impose financial reimbursement of moral damage, especially for those whose health, honor or

κρίση του χρηματική ικανοποίηση λόγω ηθικής βλάβης. Αυτό ισχύει ιδίως για εκείνον που έπαθε προσβολή της υγείας, της τιμής ή της αγνείας του ή στερήθηκε την ελευθερία του. Σε περίπτωση θανάτωσης προσώπου η χρηματική αυτή ικανοποίηση μπορεί να επιδικαστεί στην οικογένεια του θύματος λόγω ψυχικής οδύνης. Άρθρο 105 - Εισαγωγικός Νόμος του Αστικού Κώδικα Για παράνομες πράξεις ή παραλείψεις των οργάνων του δημοσίου κατά την άσκηση της δημόσιας εξουσίας που τους έχει ανατεθεί, το δημόσιο ενέχεται σε αποζημίωση, εκτός αν η πράξη ή η παραλείψη έγινε κατά παράβαση διάταξης που υπάρχει για χάρη του γενικού συμφέροντος. Μαζί με το δημόσιο ευθύνεται εις ολόκληρον και το υπαίτιο πρόσωπο, με την επιφύλαξη των ειδικών διατάξεων για την ευθύνη των υπουργών. Άρθρο 106 - Εισαγωγικός Νόμος του Αστικού Κώδικα(2783/1941) Οι διατάξεις των δύο προηγούμενων άρθρων εφαρμόζονται και για την ευθύνη των δήμων, των κοινοτήτων ή των άλλων νομικών προσώπων δημοσίου δικαίου από πράξεις ή παραλείψεις των οργάνων που βρίσκονται στην υπηρεσία τους.	freedom was violated. In case of death, the family of the victim can be compensated. Article 105-Introductory Law of Civil Code For illegal actions or neglects of public sector bodies when they act at their capacity, the State, and the person responsible have the obligation to compensation, unless the illegal action or neglect took place for the general good (Joint and several liability) Article 106-Introductory Law of Civil Code (2783/1941) The previous provisions apply for the responsibility of municipalities, communities or other public legal persons for actions or neglects of their bodies.
Κώδικας Διοικητικής Διαδικασίας 2690/1999 Άρθρο 11 §1 Η βεβαίωση του γνησίου της υπογραφής του ενδιαφερομένου γίνεται, από οποιαδήποτε διοικητική αρχή ή από τα Κ.Ε.Π., βάσει του δελτίου ταυτότητας ή των αντίστοιχων εγγράφων που προβλέπονται στο άρθρο 3.	Administrative Procedure Code 2690/1999 Article 11 §1 The authenticity of the signature is verified by an administrative authority, based on the documents described on article 3.
Νόμος 4624/2019 Άρθρο 6 Ορισμός του υπεύθυνου προστασίας δεδομένων σε δημόσιους φορείς 1. Οι δημόσιοι φορείς ορίζουν υπεύθυνο προστασίας δεδομένων (εφεξής: ΥΠΔ). 2. Μπορεί να ορίζεται ένας μόνο ΥΠΔ για περισσότερους δημόσιους φορείς, λαμβάνοντας υπόψη την οργανωτική δομή και το μέγεθός τους.	Law 4624/2019 Article 6 Designation of the data protection officer in public 1. Public bodies shall designate a data protection officer (hereinafter: the DPO). 2. A single DPO may be appointed for several public bodies, considering their organisational structure and size.

3. Ο ΥΠΔ επιλέγεται βάσει επαγγελματικών προσόντων και, ιδίως βάσει των εξειδικευμένων γνώσεων του στο δίκαιο της προστασίας δεδομένων προσωπικού χαρακτήρα και των πρακτικών περί προστασίας δεδομένων προσωπικού χαρακτήρα, καθώς και βάσει των ικανοτήτων του να εκπληρώσει τα καθήκοντα του άρθρου 8. 4. Ο ΥΠΔ μπορεί να είναι υπάλληλος του δημόσιου φορέα με οποιαδήποτε σχέση εργασίας ή να εκπληρώνει τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών. 5. Ο δημόσιος φορέας δημοσιοποιεί τα στοιχεία επικοινωνίας του ΥΠΔ και τα ανακοινώνει στην Αρχή, εκτός και εάν αυτό δεν επιτρέπεται για λόγους εθνικής ασφάλειας ή λόγω τήρησης του καθήκοντος εχεμύθειας (εμπιστευτικότητας), που προβλέπεται από τον νόμο. Άρθρο 7 - Θέση του ΥΠΔ σε δημόσιους φορείς 1. Ο δημόσιος φορέας διασφαλίζει ότι ο ΥΠΔ μετέχει δεόντως και έγκαιρα σε όλα τα ζητήματα σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. 2. Ο δημόσιος φορέας υποστηρίζει τον ΥΠΔ κατά την εκτέλεση των καθηκόντων που αναφέρονται στο άρθρο 8, παρέχοντάς του τους απαραίτητους πόρους για την εκτέλεση των καθηκόντων αυτών και την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, επεξεργασίας, και για τη διατήρηση των ειδικών γνώσεων του. 3. Ο δημόσιος φορέας διασφαλίζει ότι ο ΥΠΔ δεν λαμβάνει εντολές κατά την άσκηση των καθηκόντων του, αναφέρεται απευθείας στο ανώτατο ιεραρχικά προϊστάμενο όργανο του δημόσιου φορέα, δεν απολύεται ούτε υφίσταται κυρώσεις από τον υπεύθυνο επεξεργασίας επειδή επιτέλεσε τα καθήκοντά του. 4. Η καταγγελία της σύμβασης εργασίας του ΥΠΔ ή η ανάκληση της ανάθεσης των καθηκόντων του, στην περίπτωση που αυτός είναι και υπάλληλος του δημόσιου φορέα, επιτρέπεται μόνον για σπουδαίο λόγο. Μετά τη λήξη της σύμβασης εργασίας του ως ΥΠΔ, δεν μπορεί να απολυθεί για ένα (1) έτος,	3. The DPO shall be selected based on professional qualities and expert knowledge of data protection law and practices, and the ability to fulfil the tasks referred to in Article 8. 4. The DPO may be an employee of the public body in any capacity or fulfil his or her tasks based on a service contract. 5. The public body shall publish the contact details of the DPO and communicate them to the Authority, unless this is not permitted for reasons of national security or for the purposes of maintaining confidentiality, as provided for by law. Article 7 Position of the DPO in public bodies 1. The public body shall ensure that the DPO is involved, properly and in a timely manner, in all issues relating to the protection of personal data. 2. The public body shall support the DPO in performing the tasks referred to in Article 8 by providing resources necessary to carry out those tasks, ensuring access to personal data, to processing operations, and to maintain his or her expert knowledge. 3. The public body shall ensure that the DPO does not receive any instructions regarding the exercise of his or her tasks, reports directly to the highest management level of the public body, and is not dismissed or penalised by the controller for performing his or her tasks. 4. Termination of the employment contract of the DPO, or revocation of the duties assigned to him or her, where the DPO is also an employee of the public body, shall only be allowed for good reason. After the expiry of his or her employment contract as a DPO, he or she shall not be dismissed for one (1) year, unless the public body has good reason to terminate his or her contract. 5. The data subjects may consult the DPO on any matter relating to the processing of personal data and the exercise of their rights under the GDPR, this Law and any other legislation on the protection of personal data. The DPO shall be bound by secrecy or confidentiality concerning the identity of data subjects and the circumstances in which conclusions can be drawn as to the data subject, unless the identity of the data subject is

εκτός εάν ο δημόσιος φορέας έχει σπουδαίο λόγο να προβεί στην καταγγελία της σύμβασής του.

5. Τα υποκείμενα των δεδομένων μπορούν να συμβουλευονται τον ΥΠΔ για κάθε θέμα σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την άσκηση των δικαιωμάτων τους βάσει του ΓΚΠΔ, του παρόντος και άλλης νομοθεσίας για την προστασία των δεδομένων προσωπικού χαρακτήρα. Ο ΥΠΔ είναι υποχρεωμένος να διατηρεί εμπιστευτικότητα ως προς την ταυτότητα των υποκειμένων των δεδομένων και σχετικά με τις περιστάσεις που επιτρέπουν την εξαγωγή συμπερασμάτων ως προς το υποκείμενο των δεδομένων, εκτός αν η ταυτότητα του υποκειμένου αποκαλύπτεται από αυτό.

6. Εάν ο ΥΠΔ λάβει γνώση δεδομένων Προσωπικού Χαρακτήρα κατά την άσκηση του έργου του, για τα οποία ο επικεφαλής του δημόσιου φορέα έχει το δικαίωμα να αρνηθεί να καταθέσει ως μάρτυρας για επαγγελματικούς λόγους, το δικαίωμα αυτό ισχύει και για τον ΥΠΔ και τους βοηθούς του.

Άρθρο 8 - Νόμος 4624/2019 - Καθήκοντα του ΥΠΔ σε δημόσιους φορείς

1. Επιπλέον των καθηκόντων του σύμφωνα με τον ΓΚΠΔ, ο ΥΠΔ έχει τουλάχιστον τα ακόλουθα καθήκοντα:

α) να ενημερώνει και συμβουλεύει τον δημόσιο φορέα και τους εργαζομένους που διενεργούν την επεξεργασία σχετικά με τις υποχρεώσεις τους σύμφωνα με τις διατάξεις του παρόντος και κάθε άλλη νομοθεσία για την προστασία δεδομένων προσωπικού χαρακτήρα·

β) να παρακολουθεί την τήρηση των διατάξεων του παρόντος και κάθε άλλης νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα, και των πολιτικών του δημόσιου φορέα σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της λογοδοσίας, καθώς και των σχετικών ελέγχων·

γ) να παρέχει συμβουλές όσον αφορά την εκτίμηση αντικτύπου για την προστασία των δεδομένων

disclosed by the subject itself. 6. If the DPO, in performing his or her tasks, becomes aware of personal data for which the head of the public body has the right to refuse to give evidence as a witness for professional reasons, that right shall also apply to the DPO and his or her assistants.

Article 8 Tasks of the DPO in public bodies

1. In addition to his or her tasks under the GDPR, the DPO shall have at least the following tasks:

(a) to inform and advise the public body and the employees, who carry out the processing, of their obligations under the provisions of this Law and any other legislation on the protection of personal data.

(b) to monitor compliance with the provisions of this Law and any other legislation on the protection of personal data, and with the personal data protection policies of the public body, including accountability and the related audits.

(c) to provide advice as regards the data protection impact assessment and monitor its implementation pursuant to Article 65.

(d) to cooperate with the Authority.

(e) to act as the contact point with the Authority on issues relating to processing, including the prior consultation referred to in Article 67, and to consult the Authority, where appropriate, about any other matter.

2. The tasks of the DPO, who may be designated by judicial and prosecutorial authorities, shall not concern the processing operations carried out by judicial and prosecutorial authorities acting in their judicial capacity.

3. The DPO may fulfil other tasks and duties. The controller or processor shall ensure that the exercise of any such tasks and duties does not result in a conflict of interests. 4. The DPO shall, in the performance of his or her tasks, have due regard to the risk associated with processing, the nature, scope, context and purposes of processing.

προσωπικού χαρακτήρα και παρακολουθεί την εφαρμογή της σύμφωνα με το άρθρο 65· δ) να συνεργάζεται με την Αρχή· ε) να ενεργεί ως σημείο επαφής με την Αρχή σε θέματα που αφορούν την επεξεργασία, συμπεριλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 67, και τη συμβουλευεται, κατά περίπτωση, σχετικά με οποιοδήποτε άλλο θέμα. 2. Τα καθήκοντα του ΥΠΔ ο οποίος τυχόν ορίζεται από δικαστικές και εισαγγελικές αρχές δεν αφορούν τις πράξεις επεξεργασίας που διενεργούνται από τις δικαστικές και εισαγγελικές αρχές στο πλαίσιο της δικαστικής λειτουργίας και των δικαστικών τους καθηκόντων. 3. Ο ΥΠΔ μπορεί να εκτελεί και άλλα καθήκοντα. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διασφαλίζουν ότι η άσκηση των καθηκόντων αυτών δεν οδηγεί σε σύγκρουση συμφερόντων. 4. Ο ΥΠΔ κατά την εκτέλεση των καθηκόντων του λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με την επεξεργασία, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.	Article 38 Penal sanctions 1. Anyone who, without legal grounds: (a) interferes in any way with a data filing system and in so doing is made aware of such data; (b) copies, removes, alters, harms, collects, registers, organises, structures, stores, adapts, modifies, recovers, seeks information, correlates, combines, restricts, erases, destroys, shall be punished with imprisonment of up to one (1) year, unless the act is punishable with a more severe penalty under another provision. 2. Anyone who uses, transmits, disseminates, discloses by transmission, makes available, announces or makes accessible to unauthorised persons personal data acquired pursuant to indent (a) of paragraph 1, or allows unauthorised persons to become aware of such data, shall be punished with imprisonment, unless the act is punishable with a more severe penalty under another provision. 3. If the act referred to in paragraph 2 relates to special categories of personal data referred to in Article 9(1) of the GDPR or data relating to criminal convictions and offences or relevant security measures referred to in Article 10 of the GDPR, the offender shall be punished with imprisonment of at least one (1) year and a fine of up to one hundred thousand euros (EUR 100,000), unless the act is punishable with a more severe penalty under another provision. 4. The person who has committed the acts referred to in the previous paragraphs shall be punished with incarceration of up to ten (10) years, if he or she intended to secure for himself or herself or others an unjust profit, or cause financial loss to another person, or cause damage to another person, and the total profit or total loss exceeds the amount of one hundred and twenty thousand euros (EUR 120,000). 5. If the acts referred to in paragraphs 1 to 3 have resulted in a risk to the free functioning of democracy or national security, they shall be
Άρθρο 38 Ποινικές κυρώσεις 1. Όποιος, χωρίς δικαίωμα: α) επεμβαίνει με οποιονδήποτε τρόπο σε σύστημα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα, και με την πράξη του αυτή λαμβάνει γνώση των δεδομένων αυτών· β) τα αντιγράφει, αφαιρεί, αλλοιώνει, βλάπτει, συλλέγει, καταχωρεί, οργανώνει, διαρθρώνει, αποθηκεύει, προσαρμόζει, μεταβάλλει, ανακτά, αναζητεί πληροφορίες, συσχετίζει, συνδυάζει, περιορίζει, διαγράφει, καταστρέφει, τιμωρείται με φυλάκιση μέχρι ενός (1) έτους, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη. 2. Όποιος χρησιμοποιεί, μεταδίδει, διαδίδει, κοινολογεί με διαβίβαση, διαθέτει, ανακοινώνει ή καθιστά προσιτά σε μη δικαιούμενα πρόσωπα δεδομένα προσωπικού χαρακτήρα, τα οποία απέκτησε σύμφωνα με την περίπτωση α' της	

παραγράφου 1 ή επιτρέπει σε μη δικαιούμενα πρόσωπα να λάβουν γνώση των δεδομένων αυτών, τιμωρείται με φυλάκιση, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη.

3. Εάν η πράξη της παραγράφου 2 αφορά ειδικών κατηγοριών δεδομένα προσωπικού χαρακτήρα του άρθρου 9 παράγραφος 1 του ΓΚΠΔ ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα ή τα σχετικά με αυτά μέτρα ασφαλείας του άρθρου 10 του ΓΚΠΔ, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή έως εκατό χιλιάδες (100.000) ευρώ, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη.

4. Με κάθειρξη μέχρι δέκα (10) ετών τιμωρείται ο υπαίτιος των πράξεων των προηγούμενων παραγράφων, εάν είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία σε άλλον ή να βλάψει άλλον και το συνολικό όφελος ή η συνολική ζημία υπερβαίνει το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ.

5. Εάν από τις πράξεις των παραγράφων 1 έως και 3 προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή έως τριακόσιες χιλιάδες (300.000) ευρώ.

6. Τα κακούργηματα που προβλέπονται στο παρόν άρθρο υπάγονται στην αρμοδιότητα του Τριμελούς Εφετείου Κακούργημάτων.

Άρθρο 39

Διοικητικές κυρώσεις

1. Με την επιφύλαξη των διορθωτικών εξουσιών της Αρχής σύμφωνα με το άρθρο 58 παράγραφος 2 του ΓΚΠΔ, η Αρχή με ειδικά αιτιολογημένη απόφασή της και ύστερα από προηγούμενη κλήση για παροχή εξηγήσεων των ενδιαφερομένων μπορεί να επιβάλει στους φορείς του δημόσιου τομέα, όπως αυτός οριοθετείται στην περίπτωση α' της παραγράφου 1 του άρθρου 14 του ν. 4270/2014 (Α' 143), εξαιρουμένων των δημοσίων επιχειρήσεων και των οργανισμών του Κεφαλαίου Α' του ν. 3429/2005 (Α' 314), υπό την ιδιότητά τους ως

punishable with imprisonment and a fine of up to three hundred thousand euros (EUR 300,000). 6. The felonies provided for in this Article shall fall within the jurisdiction of the three-member court of appeal for felonies.

Article 39

Administrative sanctions

1. Without prejudice to the Authority's corrective powers in accordance with Article 58(2) of the GDPR, the Authority may, in a specific reasoned decision and following a previous notice summoning the interested parties to provide explanations, impose to bodies of the public sector, as this is defined in indent (a) of Article 14(1) of Law 4270/2014 (Government Gazette Α' 143), with the exception of public undertakings and bodies referred to in Chapter Α of Law 3429/2005 (Government Gazette Α' 314), in their capacity as data controllers, for infringements relating to: (a) indent (a) of Article 83(4) of the GDPR, with the exception of Articles 8, 27, 29, 42, 43 of the GDPR, (b) Article 83(5) and (6) of the GDPR, with the exception of Articles 17, 20, 47, 90 and 91 of the GDPR, (c) Articles 5, 6, 7, 22, 24, 26, 27 (with the exception of paragraph 7 thereof), Articles 28 to 31, and indent (a) of Article 32(1), Articles 33 to 35 of this Law, an administrative fine of up to ten million euros (EUR 10,000,000).

2. When deciding whether to impose an administrative fine and determining its amount, in each individual case due regard shall be given to the following: (a) the nature, gravity and duration of the infringement taking into account the scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them, (b) any action taken by the body of the public sector to mitigate the damage suffered by data subjects, (c) any relevant previous infringements by the body of the public sector, (d) the categories of personal data affected by the infringement, (e) the manner in which the infringement became known to the Authority, in

υπεύθυνων επεξεργασίας δεδομένων προσωπικού χαρακτήρα, για τις παραβάσεις:

α) της περίπτωσης α) της παραγράφου 4 του άρθρου 83 του ΓΚΠΔ, εκτός των άρθρων 8, 27, 29, 42, 43 του ΓΚΠΔ, β) των παραγράφων 5 και 6 του άρθρου 83 του ΓΚΠΔ, εκτός των άρθρων 17, 20, 47, 90 και 91 του ΓΚΠΔ, γ) των άρθρων 5, 6, 7, 22, 24, 26, 27 (πλην της παραγράφου 7 αυτού), 28 έως και 31, και των άρθρων 32 παράγραφος 1 περίπτωση α', 33 έως και 35 του παρόντος, διοικητικό πρόστιμο έως δέκα εκατομμύρια (10.000.000) ευρώ.

2. Κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου, καθώς και για τον καθορισμό του ύψους αυτού, για κάθε εξατομικευμένη περίπτωση λαμβάνονται υπόψη τα ακόλουθα:

α) η φύση, η βαρύτητα, η διάρκεια της παράβασης, η έκταση ή ο σκοπός της σχετικής επεξεργασίας, καθώς και ο αριθμός των υποκειμένων των δεδομένων προσωπικού χαρακτήρα που έθιξε η παράβαση και το μέγεθος της ζημίας που αυτά υπέστησαν,

β) οποιεσδήποτε ενέργειες στις οποίες προέβη ο φορέας του δημόσιου τομέα, για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων προσωπικού χαρακτήρα,

γ) τυχόν σχετικές προηγούμενες παραβάσεις του φορέα του δημόσιου τομέα,

δ) οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που θίγει η παράβαση,

ε) ο τρόπος με τον οποίο η Αρχή πληροφόρηθηκε την παράβαση, ειδικότερα αν και κατά πόσο ο φορέας του δημόσιου τομέα κοινοποίησε την παράβαση και

στ) εάν έχουν ήδη διαταχθεί σε βάρος του φορέα του δημόσιου τομέα, για την ίδια παράβαση, τα μέτρα που αναφέρονται στο άρθρο 58 παράγραφος 2 του ΓΚΠΔ, ο βαθμός συμμόρφωσής του με αυτά.

3. Σε περίπτωση που ο φορέας του δημόσιου τομέα για τις ίδιες ή για συνδεδεμένες πράξεις επεξεργασίας, παραβιάζει περισσότερες διατάξεις του ΓΚΠΔ ή του παρόντος, το συνολικό ύψος του

particular whether, and if so to what extent, the body of the public sector notified the infringement and (f) where measures referred to in Article 58(2) of the GDPR have previously been ordered against the body of the public sector, with regard to the same infringement, the degree of compliance with those measures.

3. If a body of the public sector, for the same or linked processing operations, infringes several provisions of the GDPR or of this Law, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

διοικητικού προστίμου δεν υπερβαίνει το ποσό που ορίζεται για τη βαρύτερη παράβαση.	
Προεδρικό Διάταγμα 18/1989 Άρθρο 17 παρ 1. Τα ένδικα μέσα ενώπιον του Συμβουλίου ασκούνται δια καταθέσεως δικογράφου.	Presidential Decree 18/1989 Article 17 paragraph 1: Redress before the Council of State shall be brought by lodging an application
Ελληνικός Ποινικός κώδικας Άρθρο 370 1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους. 2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.3. Οι πράξεις που προβλέπονται στο άρθρο αυτό διώκονται με έγκληση.	Greek Penal Code Article 370 1. Whoever improperly copies, prints, uses, discloses to a third party or in any case violates computer data or programs, which constitute state, scientific or professional secrets or secrets of a public or private company, shall be punished by imprisonment of at least three months. Confidential are also those those whose rightful owner, out of justified interest, treats them as secret, especially when he has taken measures to prevent third parties from obtaining their knowledge. 2. If the perpetrator is in the service of the data holder, as well as if the secrecy is of economic importance, imprisonment of at least one year is imposed.3. The acts provided for in this article are prosecuted on appeal.
Νόμος 2225/1994 Άρθρο 3 Άρση του απορρήτου για λόγους εθνικής ασφάλειας 1.Αίτηση για άρση του απορρήτου μπορεί να υποβάλλει μόνο δικαστική ή άλλη πολιτική, στρατιωτική ή αστυνομική δημόσια αρχή στην αρμοδιότητα της οποίας υπάγεται το θέμα εθνικής ασφάλειας που επιβάλλει την άρση. 2.Η αίτηση υποβάλλεται προς τον Εισαγγελέα Εφετών του τόπου της αιτούσας αρχής ή του τόπου, όπου πρόκειται να επιβληθεί η άρση. Ο Εισαγγελέας Εφετών αποφασίζει μέσα σε είκοσι τέσσερις (24) ώρες για την άρση ή όχι του απορρήτου με διάταξή του στην οποία περιέχονται τα αναφερόμενα στην παρ. 1 του άρθρου 5	Law 2225/1994 Article 3 Removal of confidentiality for reasons of national security 1. An application for a waiver of confidentiality may be made only by a judicial or other political, military or police public authority which has jurisdiction over the national security issue requiring the waiver. 2. The application shall be submitted to the Appellate Prosecutor of the place of the requesting authority or of the place where the removal is to be imposed. The Appellate Prosecutor decides within twenty-four (24) hours on the removal or not of the confidentiality by an

στοιχεία. Αν κατά την κρίση του, μετά από εισήγηση της αιτούσας αρχής, ειδικές περιστάσεις εθνικής ασφάλειας επιβάλουν την παράλειψη ή τη συνοπτική παράθεση ορισμένων από τα στοιχεία αυτά, γίνεται ειδική μνεία στη διάταξη. Άρθρο 4 Άρση του απορρήτου για διακρίβωση εγκλημάτων 1. Η άρση του απορρήτου είναι επιτρεπτή για τη διακρίβωση των κακουργημάτων που προβλέπονται από: α) τα άρθρα 134, 135 παρ. 1, 2, 135Α, 137Α, 137Β, 138, 139, 140, 143, 144, 146, 148 παρ. 2, 150, 151, 157 παρ. 1, 168, παρ. 1, 207, 208 παρ. 1, 264 παρ. β, γ, 265 παρ. 3, 270, 272, 275 παρ. β, 291 παρ. 1, εδ. β, γ', 299, 322, 324 παρ. 2, 3, 37-4, 380, 385 του Ποινικού Κώδικα, β) τα άρθρα 26, 27, 28, 29, 31, 32, 33, 34, 35, 39, 40, 41, 63, 64, 76, 93 και 97 του Στρατιωτικού Ποινικού Κώδικα, γ) το άρθρο 15 παρ. 1 του ν. 2168/1993, δ) τα άρθρα 5, 6, 7 και 8 του ν. 1729/1987. ε) τα άρθρα 89, 90 και 93 του ν. 1165/1968. Επίσης, επιτρέπεται η άρση του απορρήτου για τη διακρίβωση των προπαρασκευαστικών πράξεων για το έγκλημα της παραχάραξης νομίσματος κατά το άρθρο 211 του Ποινικού Κώδικα. 2. Η άρση στις περιπτώσεις αυτές είναι επιτρεπτή μόνο αν αιτιολογημένα το αρμόδιο δικαστικό συμβούλιο διαπιστώσει ότι η διερεύνηση της υπόθεσης ή η εξακρίβωση του τόπου διαμονής του κατηγορουμένου είναι αδύνατη ή ουσιαστικά δυσχερής χωρίς αυτήν. 3. Η άρση στρέφεται μόνο κατά συγκεκριμένου προσώπου ή προσώπων που έχουν σχέση με την υπόθεση που ερευνάται ή για τα οποία, βάσει συγκεκριμένων περιστατικών, προκύπτει ότι λαμβάνουν ή μεταφέρουν συγκεκριμένα μηνύματα που αφορούν ή προέρχονται από τον κατηγορούμενο ή χρησιμοποιούνται ως σύνδεσμοί του.	order which contains the elements referred to in par. 1 of article 5. If, in its discretion, following a request by the requesting authority, special circumstances of national security require the omission or summary of some of these elements, special reference shall be made to the provision. Article 4 Removal of confidentiality for crime detection 1. The removal of secrecy is permissible for the verification of the crimes provided by: a) Articles 134, 135 par. 1, 2, 135A, 137A, 137B, 138, 139, 140, 143, 144, 146, 148 par. 2, 150, 151, 157 par. 1, 168, par. , 207, 208 par. 1, 264 par. B, c, 265 par. 3, 270, 272, 275 par. B, 291 par. 1, ed. b, c ', 299, 322, 324 par. 2, 3, 37-4, 380, 385 of the Penal Code, b) Articles 26, 27, 28, 29, 31, 32, 33, 34, 35, 39, 40, 41, 63, 64, 76, 93 and 97 of the Military Penal Code. c) article 15 par. 1 of law 2168/1993, d) Articles 5, 6, 7 and 8 of Law 1729/1987. e) articles 89, 90 and 93 of law 1165/1968. It is also allowed to remove the secrecy for the verification of the preparatory acts for the crime of currency counterfeiting according to article 211 of the Penal Code. 2. Removal in such cases is permissible only if the competent judicial council finds that the investigation of the case or the verification of the place of residence of the accused is impossible or substantially difficult without it. 3. The removal is directed only against a specific person or persons related to the case under investigation or for which, based on specific facts, it appears that they receive or convey specific messages concerning or coming from the accused or used as his links. 4. The removal of confidentiality in the cases of this article is imposed by an order of the Board of Appeals or Misdemeanor Courts in the

4. Η άρση του απορρήτου στις περιπτώσεις του παρόντος άρθρου επιβάλλεται με διάταξη του Συμβουλίου Εφετών ή Πλημμελειοδικών στην καθ' ύλην και κατά τόπο αρμοδιότητα του οποίου υπάγεται η διακρίβωση του συγκεκριμένου εγκλήματος με το οποίο σχετίζεται η άρση. 5. Την αίτηση για την άρση υποβάλλει στο Συμβούλιο ο καθ' ύλην και κατά τόπο αρμόδιος εισαγγελέας, ο οποίος εποπτεύει ή ενεργεί προανάκριση ή προκαταρκτική εξέταση και ο ανακριτής, ο οποίος ενεργεί τακτική ανάκριση για τα πιο πάνω εγκλήματα. Το Συμβούλιο αποφασίζει μέσα σε είκοσι τέσσερις (24) ώρες για την άρση ή όχι του απορρήτου, με διάταξή του, στην οποία περιέχονται τα κατά την παρ. 2 του άρθρου 5 στοιχεία.	substantive and local jurisdiction which is responsible for the verification of the specific crime with which the removal is related. 5. The request for removal shall be submitted to the Council by the competent and locally competent prosecutor, who supervises or conducts a preliminary investigation or preliminary examination, and the investigator, who conducts a regular investigation for the above crimes. The Council decides within twenty-four (24) hours on the removal or not of the secrecy, by its order, which contains
Νόμος 2168/1993 Άρθρο 15 Διαχειριμένες περιπτώσεις 1. Όποιος εισάγει, κατέχει, κατασκευάζει, μετασκευάζει, συναρμολογεί, εμπορεύεται, παραδίδει, προμηθεύει ή μεταφέρει πολεμικά τυφέκια, αυτόματα, πολυβόλα, πιστόλια, περίστροφα, χειροβομβίδες, πυρομαχικά, εκρηκτικές ύλες, εκρηκτικούς μηχανισμούς και λοιπά είδη πολεμικού υλικού, με σκοπό τη διάθεσή τους σε τρίτους για διάπραξη κακουργήματος ή με σκοπό τον παράνομο εφοδιασμό ομάδων, οργανώσεων, σωμάτων ή ενώσεων προσώπων, τιμωρείται με κάθειρξη, αν η πράξη δεν τιμωρείται βαρύτερα από άλλη διάταξη. Με την ίδια ποινή τιμωρείται και όποιος, για τον ίδιο σκοπό, λαμβάνει, αποκρύπτει ή με οποιονδήποτε τρόπο δέχεται τα ανωτέρω αντικείμενα. Με την ίδια, επίσης, ποινή τιμωρούνται και τα μέλη διοικητικού συμβουλίου ή διοικούσας επιτροπής ή οι υπεύθυνοι ή αρχηγοί των κατά την προηγούμενη περίπτωση ομάδων, οργανώσεων, σωμάτων και ενώσεων, αν γνωρίζουν ότι κάποιο από τα μέλη τους έχει παράνομα εφοδιαστεί ή κατέχει τα ανωτέρω αντικείμενα, καθώς και τους σκοπούς που επιδιώκει και δεν το καταγγέλλουν στις αρμόδιες αρχές.	Law 2168/1993 Article 15 Distinguished cases 1. Whoever imports, possesses, manufactures, remodels, assembles, markets, delivers, supplies or transports war rifles, submachine guns, pistols, pistols, grenades, ammunition, explosives, explosive devices and other types of ammunition; to third parties for committing a crime or for the purpose of illegally supplying groups, organizations, unions or associations of persons, shall be punished by imprisonment, unless the act is punished more severely by another provision. Whoever, for the same purpose, receives, conceals or in any way accepts the above objects is punished with the same punishment. The members of the board of directors or the steering committee or the leaders or the leaders of the groups, organizations, unions and associations in the previous case are also punished with the same punishment, if they know that one of their members has been illegally supplied or possesses the above objects. , as well as the purposes it seeks and do not report it to the competent authorities.

Προεδρικό διάταγμα 47/2005 Άρθρο 8 εδάφιο 1 Υποχρεώσεις των παροχών υπηρεσιών και δικτύων. 1. Οι πάροχοι υπηρεσιών και δικτύων επικοινωνίας υποχρεούνται να ανταποκρίνονται αμέσως σε κάθε αίτημα για άρση του απορρήτου της επικοινωνίας που τους κοινοποιείται από τις αρμόδιες αρχές σύμφωνα με τα προβλεπόμενα στο παρόν.	Presidential Decree 47/2005 Article 8, paragraph 1 Obligations of services and networks. 1. The providers of services and communication networks shall be obliged to respond immediately to any request for the removal of the confidentiality of the communication notified to them by the competent authorities in accordance with the provisions hereof.
Νόμος 1729/1987 Άρθρο 5 Βασικά εγκλήματα 1. Με κάθειρξη τουλάχιστο δέκα (10) ετών και με χρηματική ποινή εκατό χίλιες (100.000) μέχρι εκατό εκατομμύρια (100.000.000) δραχμές τιμωρείται όποιος; α) Εισάγει στην επικρατεί.* ή εξάγει από αυτή ή διαμετακομίζει ναρκωτικά. β) Πωλεί, αγοράζει ή διαθέτει σε τρίτους με οποιονδήποτε τρόπο ναρκωτικά ή μεσολαβεί στις πράξεις αυτές, αποθηκεύει ή παρακαταθέτει. γ) Εισάγει ναρκωτικά ή διευκολύνει την εισαγωγή τους σε στρατόπεδα, αστυνομικά κρατητήρια, σωφρονιστικά καταστήματα, καταστήματα ανηλίκων κάθε κατηγορίας ή τόπους ομαδικής εργασίας ή διαβίωσης ή σε νοσηλευτικά ιδρύματα ή αναρρωτήρια. δ) Αναμινύει με οποιονδήποτε τρόπο ναρκωτικά σε τρόφιμα, ποτά ή άλλα είδη προορισμένα ή πρόσφορα να εισαχθούν στον ανθρώπινο οργανισμό. ε) Παρασκευάζει είδη του μονοπωλίου ναρκωτικών ή οποιαδήποτε ναρκωτική ουσία ή κατέχει για το σκοπό αυτόν τις αναγκαίες πρώτες ύλες, όργανα ή σιεύη. στ) Καλλιεργεί ή συγκομίζει οποιαδήποτε ποικιλία ινδικής κάνναβης, υπνοφόρου μήκωνος, ERYTHROXYLCM COCA και λοιπών φυτών από τα οποία παράγονται ναρκωτικές ουσίες. ζ) Κατέχει ή μεταφέρει ναρκωτικά με οποιονδήποτε τρόπο ή μέσο είτε στο έδαφος της επικράτειας είτε	Law 1729/1987 Article 5 Basic crimes 1. Whoever is punished with imprisonment of at least ten (10) years and with a fine of one hundred thousand (100,000) to one hundred million (100,000,000) a) It imports into the prevailing. * or exports from it or transports drugs. b) Sells, buys, or distributes to third parties' drugs in any way or mediates in these transactions, stores, or deposits. c) Introduces drugs or facilitates their introduction in camps, police detention centers, penitentiaries, juvenile shops of any category or places of group work or living or in hospitals or convents. d) Mixes in any way drugs in food, drink or other items intended or suitable to be introduced into the human body. e) Manufactures articles of the drug monopoly or any narcotic substance or possesses for this purpose the necessary raw materials, instruments, or utensils. f) Cultivates or harvests any variety of cannabis, sleeping mycosis, ERYTHROXYLCM COCA and other plants from which drugs are produced. g) Possesses or transports drugs in any way or means either on the territory of the territory or sailing or crossing the coastal zone or flying in the Greek airspace.

παραπλέοντας ή διασχίζοντας την αιγιαλίτιδα ζώνη είτε ιπτάμενος στον ελληνικό ενάεριο χώρο. η) Αποστέλλει ή παραλαμβάνει εν γνώσει του δέματα, δείγματα χωρίς αξία ή επιστολές που περιέχουν οποιοδήποτε ναρκωτικό ή δίνει εντολή σε άλλον για όμοια αποστολή ή παραλαβή. Διαθέτει σε άλλους οποιοδήποτε χώρο για χρήση ναρκωτικών ή διευθύνει κατάστημα στο οποίο γίνεται κατά σύστημα χρήση ναρκωτικών ή αποτελεί μέλος του προσωπικού τέτοιου καταστήματος και γνωρίζει τη χρήση αυτή. Ι) Συντελεί με οποιονδήποτε τρόπο στη διάδοση της χρήσης των ναρκωτικών. ια) Νοθεύει ή πωλεί νοθευμένα είδη του μονοπωλίου ναρκωτικών. ιβ) Πλαστογραφεί, νοθεύει ή χρησιμοποιεί πλάστη η νοθευμένη ιατρική συνταγή χορήγησης ναρκωτικών ουσιών με, σκοπό τη διακίνησή τους.	h) Sends or receives knowingly. parcels, worthless samples, or letters containing any drug or ordering another to receive a similar consignment. Has any other place for drug use or runs a store in which drugs are used systematically or is a member of the staff of such a store and knows • this use. I) Contributes in any way to the spread of drug use. k) Falsifies or sells falsified items of the drug monopoly. l) The falsified prescription for the administration of drugs for the purpose of their trafficking is falsified, falsified, or used as a forgery.
Πράξη Νομοθετικού Περιεχομένου της 30.03.2020 Άρθρο 29 1. Με απόφαση του Υπουργού Υγείας συστήνεται και λειτουργεί Εθνικό Μητρώο Ασθενών από τον κορωνοϊό COVID-19. Η σύσταση και λειτουργία του ανωτέρω Μητρώου αποσκοπεί στην προάσπιση της υγείας του πληθυσμού ενόψει της μεγάλης επίπτωσης του νοσήματος στον γενικό πληθυσμό, της ανάγκης καταγραφής επιδημιολογικών δεδομένων, φαρμακοεπαγρύπνησης και άσκησης εποπτείας στους φορείς υγειονομικής φροντίδας του ιδιωτικού τομέα. Ειδικότεροι σκοποί λειτουργίας του Εθνικού Μητρώου Ασθενών από τον κορωνοϊό COVID-19 είναι: α) η άμεση και ταχεία καταγραφή των κρουσμάτων του κορωνοϊού COVID-19 στα νοσοκομεία αναφοράς, στα ειδικά κέντρα υγείας της χώρας και σε κάθε φορέα παροχής υπηρεσιών υγείας με δυνατότητα επέκτασης της χρήσης του, β) η άμεση καταγραφή και ιατρική παρακολούθηση της εξέλιξης των κρουσμάτων που εντοπίζονται ή και παρακολουθούνται από τις Κινητές Ομάδες Υγείας (Κ.Ο.Μ.Υ.) Ειδικού Σκοπού, γ) η αυτοματοποίηση της διαδικασίας έκδοσης παραπεμπτικών για την εξέταση του κορωνοϊού	Legislative Content Act of 30.03.2020 Article 29 1. By decision of the Minister of Health, a National Register of Patients with COVID-19 coronavirus is established and operates. The establishment and operation of the above Register aims to protect the health of the population in view of the large impact of the disease on the general population, the need to record epidemiological data, pharmacovigilance and exercise supervision in private health care providers. Specific purposes of operation of the National Registry of patients with coronavirus COVID-19 are: a) the immediate and rapid recording of cases of COVID-19 coronavirus in the reference hospitals, in the special health centers of the country and in each health service provider with the possibility of expanding its use, b) the immediate recording and medical monitoring of the development of the cases identified or monitored by the Special Purpose Mobile Health Teams (KOMY), c) the automation of the process of issuing referrals for the examination of COVID-19 coronavirus and d) the

COVID-19 και δ) η διαμόρφωση επαρκών επιδημιολογικών δεδομένων για την, επί τη βάσει των καταγραφών αυτών, αποστολή των δειγμάτων από τον Εθνικό Οργανισμό Δημόσιας Υγείας (Ε.Ο.Δ.Υ.) προς τα διαπιστευμένα εθνικά και άλλα εργαστήρια. Η σύσταση και η λειτουργία του Μητρώου διενεργούνται σύμφωνα με τα διεθνή επιστημονικά πρότυπα και ιδίως την ενωσιακή νομοθεσία και τις ειδικές εθνικές ρυθμίσεις, καθώς και τις σχετικές οδηγίες και συστάσεις του Παγκόσμιου Οργανισμού Υγείας και του Ευρωπαϊκού Κέντρου Ελέγχου Νοσημάτων (ECDC). Τα δεδομένα που καταγράφονται στο αρχείο είναι το ονοματεπώνυμο του ασθενούς, η ηλικία, το φύλο, τα υποκείμενα νοσήματα και η κατάσταση της υγείας του.	formation of sufficient epidemiological data for the Based on these records, sending the samples by the National Organization of Public Health (EODY) to the accredited national and other laboratories. The establishment and operation of the Register shall be carried out in accordance with international scientific standards, in particular EU law and specific national regulations, as well as the relevant guidelines and recommendations of the World Health Organization and the European Centers for Disease Control (ECDC). The data recorded in the file are the patient's name, age, sex, underlying diseases, and state of health.

Bibliography

English Titles

Legislation

European Convention on Human Rights

Treaty on the Functioning of the European Union

Treaty on the European Union

Charter of Fundamental Rights of the European Union

Convention for the protection of Human Rights and Dignity of the Human Being about the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (64/1997).

Convention for the Protection of Individuals about Automatic Processing of Personal Data (108/1981).

European Ethical Charter on the use of artificial intelligence in judicial systems adopted by the Council of Europe.

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 European Council 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.

Directive (EU) 2016/681 of the European Parliament and European Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

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, e-Privacy Directive).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals about the processing of personal data and on the free movement of such data.

Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation

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)

Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services.

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).

Directive 2014/54/EU of the European Parliament and of the Council of 16 April 2014 on measures facilitating the exercise of rights conferred on workers in the context of freedom of movement for workers Text with EEA relevance.

EU Commission, 'White Paper on Artificial Intelligence: Public consultation towards a European approach for excellence and trust' (2020).

Unboxing Artificial Intelligence: 10 steps to protect Human Rights- Recommendation of the Commissioner for human rights

Reports

Guidelines on safeguarding privacy in the media, Council of Europe (2019).

Guidelines on Artificial Intelligence and Data Protection, Council of Europe (2019).

European Commission, 'Enter the Data Economy: EU Policies for a thriving data ecosystem' EPSC Strategic Note Issue 21 (11 January 2017).

Draft Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) Committee on Legal Affairs Rapporteur: Mady Delvaux.

European Commission, European Group on Ethics in Science and New Technologies, 'Statement on Artificial Intelligence, Robotics and 'Autonomous Systems' (2018).

Internet Organised Crime Threat Assessment (IOCTA) Report 2018, Europol

Periodicals

Philipp Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law, (2018)', 55 Common Market Law Review 1143-1186.

Digital Resources

Collinsdictionary.com. 2021. Digital technology definition and meaning | Collins English Dictionary. [online] <<https://www.collinsdictionary.com/dictionary/english/digital-technology>>.

Gartner. 2021. Definition of Advanced Technology - Gartner Information Technology Glossary. [online] <<https://www.gartner.com/en/information-technology/glossary/advanced-technology>>.

<https://www.e-ir.info/>. 2018. Defining Post-truth: Structures, Agents, and Styles. [online] <<https://www.e-ir.info/2018/10/22/defining-post-truth-structures-agents-and-styles/>>.

Hinchliffe R., ‘Greece's major banks cancel 15,000 cards after travel website breach - FinTech Futures’ [2020] FinTech Futures.
<<https://www.fintechfutures.com/2020/01/greeces-major-banks-cancel-15000-cards-after-travel-website-breach/>>.

Greek City Times, ‘Greek Government Websites Hacked’ [2020] Greek City Times.
<<https://greekcitytimes.com/2020/01/18/greek-government-websites-hacked/>>.

Boslaugh, S., n.d. ‘Anthropocentrism | philosophy’, Encyclopedia Britannica.<
<https://www.britannica.com/topic/anthropocentrism>>.

Javier Espinoza & Sam Fleming, ‘Europe urged to use industrial data trove to steal march on rivals’ Financial Times (Brussels, 14 January 2020) <
<https://www.ft.com/content/8187a268-3494-11ea-a6d3-9a26f8c3cba4>>.

How can I demonstrate that my organisation is compliant with the GDPR? European Commission,
<https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/how-can-i-demonstrate-my-organisation-compliant-gdpr_en>.

Europe 2020 “Innovation Europe”.
<http://ec.europa.eu/research/innovation-union/index_en.cfm?pg=home>.

IERC: Internet of Things Research. Available online:
www.internet-of-things-research.eu/about_ierc.htm

EU Connected Communities.
<https://ec.europa.eu/digital-single-market/events/cf/connected-communities-experience-sharing/item_display.cfm?id=15644>.

Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment
<<https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>>.

Views of the EU insurance industry on artificial intelligence,
<<https://www.insuranceeurope.eu/sites/default/files/attachments/Views%20of%20EU%20insurance%20industry%20on%20AI.pdf>>.

Partnership for AI, Tenets <<https://www.partnershiponai.org/tenets/>>.

Hellenic Federation of Enterprises,<
<https://www.sev.org.gr/grafeio-typou/arthrografia-synentefxeis-se-mme/ta-anoichta-dedomena-einai-to-petrelaio-tou-21ou-aiona-arthro-tou-aki-skertsou-genikou-diefthynti-sev-stin-kathimerini-14-10-2018/?>>.

Case law

Facebook Ireland and Others (C-645/19)

Google v CNIL (C-507/17 Google v CNIL EU:C:2019:772)

Fashion ID (C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV)

Nowak (C-434/16, Peter Nowak v Data Protection Commissioner)

C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C: 2014:317.

Reklos and Davourlis v. Greece, No. 1234/05, 15 January 2009 ECOHR.

ECJ, C-414/16, Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V. [2018], ECLI:EU:C:2018:257.

ECJ, C-202/18 and C-238/18, Ilmārs Rimšēvičs and European Central Bank v Republic of Latvia [2019], ECLI:EU:C:2019:139.

Greek Titles

Legislation

Greek Constitution

Greek Civil Code

Greek Criminal Code

Code of Criminal Procedure

Code of Administrative Procedure

Code of Civil Procedure

Law 4637/2019

Law 4443/2016

Law 4097/2012

Law 4624/2019

Law 3917/2011

Law 3471/2006

Law 2619/1998

Law 2472/1997

Law 2225/1994

Law 2068/1992

Law 1178/1981

Law 53/1974

Law 1059/1971

Law 3896/2010

Law 4604/2019

Law 3769/2009

Law 3304/2005

Law 3094/2003

Law 2667/1998

Law 2605/1998

Law 2706/1999

Presidential Decree 18/1989

Presidential Decree 98/2017

Ministerial Decision no 8056 (Government Paper 431, 14.02.2019)

Reports

Guidelines for teleworking (15/04/2020), Hellenic Data Protection Authority.

5/2020 Guidelines for the processing of personal data in the context of COVID-19 (18/03/2020), Hellenic Data Protection Authority.

Opinion 1/2020 of the Hellenic Data Protection Authority.

Opinion 9/2020 Hellenic Data Protection Authority

Opinion20/2020 Hellenic Data Protection Authority

The new General Regulation for Data Protection (GDPR), Application and challenges for business in the age of digitization, Hellenic Federation of Enterprises (SEV) (2018).

Ασπασία Τρευλάκη, “Διαστάσεις του Ψηφιακού Χάσματος στην Ελλάδα” Εθνικό Κέντρο Κοινωνικών Ερευνών.

Books

Λαζαράκος Γ., “Το δικαίωμα προστασίας του ατόμου από την αθέμιτη επεξεργασία προσωπικών δεδομένων” σε Σπύρος Βλαχόπουλος (επιμέλεια), Θεμελιώδη δικαιώματα (1η έκδοση, Νομική Βιβλιοθήκη 2016).

Τσόλιας, Ειδικοί Ποινικοί Νόμοι,(ΠΝ Σάκουλας 2013).

Ιωάννης Δαλακούρας, “ Η προστασία των απορρήτων, κατά τα άρθρα 370B – 370E Ποινικού Κώδικα, Ουσιαστική και Δικονομική προσέγγιση” (2020)

<https://dspace.lib.uom.gr/bitstream/2159/24455/1/DalakourasIoannisMsc2020.pdf>

Ραφαέλα Ματσούκα, “Σύγχρονη Τεχνολογία και Ανθρώπινα Δικαιώματα” (Σεπτέμβριος 2019)

Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών.

Καλλιόπη Παναγιωτίδη, “Η χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών στην κοινωνία πολιτών” [Σεπτέμβριος 2016] Πανεπιστήμιο Πελοποννήσου.

Πασχαλίδου Γεωργία, “Ψηφιακό Χάσμα και Ανισότητες στη χρήση νέων τεχνολογιών” [2011] Πανεπιστήμιο Μακεδονίας.

Καρδαρά Ειρήνη, “Νομική προσέγγιση των κρυπτονομισμάτων και του Blockchain” (2020)

Πανεπιστήμιο Πατρών.

Periodicals

Spiliotopoulou, S. (2014), 'Austerity measures in Greece and human rights: judgments of international bodies, EU Law and examples of Greek jurisprudence', Review of social security law 2014.

Digital Resources

Ιωάννης Ιγγλεζάκης, "Άρση απορρήτου όταν αντικείμενο έρευνας αποτελούν δεδομένα που είναι αποθηκευμένα σε cloud (υπολογιστικό νέφος)", (Lawspot, 24 March 2017)

<https://www.lawspot.gr/nomika-nea/arsi-aporritoy-otan-antikeimeno-ereynas-apoteloy-n-dedomena-poy-einai-apothikeymena-se?fbclid=IwAR3A7tufpikPYAZEylPEN_ryLZgonKH23TN-11vTudKnVIa7f7alCLYhZuF>.

Σπύρος Τάσης, 'Πανδημία και Ιδιωτικότητα', [2020], Constitutionalism, <www.constitutionalism.gr/2020-06-tassis-pandimia-idiotikotita/>.

Γενική Γραμματεία Πολιτικής Προστασίας, Κοινή Συνέντευξη Τύπου για τον περιορισμό κυκλοφορίας πολιτών σε όλη την επικράτεια λόγω κορονοϊού, (2020), <www.civilprotection.gr/el/koini-syntentyxi-typoy-gia-ton-periorismo-kykloforias-politon-se-oli-tin-epikrateia-logo-koronoioy>.

Homo digitalis, Ανοιχτή Επιστολή για την Πολιτική Προστασίας του 13033, [2020] <www.homodigitalis.gr/posts/5357>.

Homo digitalis, Καταγγελίες για παράβαση του GDPR από το 13033, [2020] <www.homodigitalis.gr/posts/8546>.

Lawspot, 'Εθνικό Μητρώο Ασθενών από τον κορωνοϊό COVID-19: Σύσταση και βασικές παράμετροι λειτουργίας' [2020] <www.lawspot.gr/nomika-nea/ethniko-mitroo-asthenon-apo-ton-koronoio-covid-19-systasi-kai-vasikes-parametroi>.

Homo digitalis, 'Προ των πυλών η χρήση τεχνολογίας αναγνώρισης προσώπου από την αστυνομία στην Ελλάδα' [2019] <www.homodigitalis.gr/posts/4662>

Lawspot, 'Reclaim Your Face: Η ευρωπαϊκή πρωτοβουλία πολιτών για ένα μέλλον χωρίς τεχνολογίες δημόσιας παρακολούθησης' [2021]

Lawspot.gr <www.lawspot.gr/nomika-nea/reclaim-your-face-i-eyropaiki-protovoylia-politon-gia-ena-mellon-horis-tehnologies>.

Μαγδαληνή Σκόνδρα, 'Αναγνώριση προσώπου (Face recognition) και προσωπικά δεδομένα' [2020] Lawspot.gr

<www.lawspot.gr/nomika-blogs/magdalini-skondra/anagnorisi-prosopoy-face-recognition-kai-prosopika-dedomena>.

"Εθνική Επιτροπή Τεχνηθικής και Εθνική Αρχή Προσβασιμότητας αποκτά η Ελλάδα" (Lawspot, 5 January 2021) <<https://www.lawspot.gr/nomika-nea/ethniki-epitropi-tehnoithikis-kai-ethniki-arhi-prosvasimotitas-apokta-i-ellada>>.

Γιάννης Στουρνάρας, “Η Τεχνητή Νοημοσύνη και ο ρόλος της στην Οικονομία, τη Διοίκηση-Οργάνωση Επιχειρήσεων και το Χρηματοπιστωτικό Τομέα” (Τράπεζα της Ελλάδος, Νέα, 21 Φεβρουαρίου 2020)

<<https://www.bankofgreece.gr/enimerosi/grafeio-typoy/anazhthsh-enhmerwsewn/enhmerwseis?announcement=6baf1721-c2a8-42c2-b4b1-6bb0368c3b52>>.

Βασίλης Καρκατζούνης, “Τεχνητή Νοημοσύνη στη Δικαιοσύνη: Εντυπωσιακές προοπτικές, ρεαλιστικές προσδοκίες” (Lawspot, 11 February 2020)

<https://www.lawspot.gr/nomika-blogs/vasilis_karkatzounis/tehniti-noimosyni-sti-dikaiosyni-e-ntyposiakes-prooptikes>.

Κώστας Μαυραγάνης, “Έρευνα: Η θέση της Ελλάδας και της Κύπρου στον κόσμο του blockchain και των bitcoins” (Huffington Post, 9 Δεκεμβρίου 2019)

<https://www.huffingtonpost.gr/entry/ereena-e-these-tes-elladas-kai-tes-keproe-ston-kosmo-to-e-blockchain-kai-ton-bitcoins_gr_5fcfd50dc5b63a1534555f5b>

Γεώργιος Πάνου, “Ευκαιρίες Blockchain για την δημόσια διοίκηση και την ηλεκτρονική διακυβέρνηση” (Medium, 23 Μαΐου 2019)

<<https://medium.com/hellenic-blockchain-hub-el/blockchain-opportunities-for-public-administration-and-e-governance-9th-mobile-world-conference-ef92c1bbc82f>>

Π. Δημητράκος, “Κρυπτονόμισμα : Ένα αναδυόμενο εργαλείο οικονομικής ελευθερίας” Αμερικανικό Κολλέγιο Ελλάδος

<<https://finhub.gr/bitcoin-kai-forologia-sta-kryptonomismata/>>.

Κωνσταντίνος Μπότσης, “Bitcoin και φορολογία στα κρυπτονομίσματα” (FinHub, 9 Φεβρουαρίου 2021) <<https://finhub.gr/bitcoin-kai-forologia-sta-kryptonomismata/>>.

Βαγγέλης Μανδραβέλης, “Κυκλοφόρησε στην αγορά το πρώτο ελληνικό κρυπτονόμισμα” (Καθημερινή, 18 Ιανουαρίου 2018)

<<https://www.kathimerini.gr/economy/local/943892/kykloforise-stin-agora-to-proto-elliniko-kryptonomisma/>>.

Case law

Decision 1/2017 Areios Pagos Supreme Civil and Criminal Court of Greece.

Decision 653/2013 Areios Pagos Supreme Civil and Criminal Court of Greece.

Decision 26/2019 Hellenic Data Protection Authority.

Decisions 82/2016, 83/2016, 84/2016 Hellenic Data Protection Authority.

Decision 66/2018 Hellenic Data Protection Authority.

Απόφαση 1/2017 του Αρείου Πάγου.

Γνωμοδότηση του Εισαγγελέα του Αρείου Πάγου υπ'αριθμ. 2/2017.

Απόφαση 287/2018 του Αρείου Πάγου.

Απόφαση 8/2019 του Μονομελούς Πρωτοδικείου Ηρακλείου.

Απόφαση 1593/2016 του Συμβουλίου της Επικρατείας.

Γνωμοδότηση του Εισαγγελέα του Αρείου Πάγου υπ'αριθμ. 12/2009.

Απόφαση 1093/2018 του Αρείου Πάγου.

Απόφαση 4309/2015 του Συμβουλίου της Επικρατείας.

ELSA THE NETHERLANDS

Contributors

National Coordinator

Uejanaua T'jhumino

National Academic Coordinator

Maria Jose Recalde-Vela

National Researchers

Tom Hartmann

Jari van den Berg

Natália Racková

Brianna Muir

(Hanh Ha) Nguyen Nguyen

Georgia Lynch

Anas A. Qazi

Mitko Tatarov

Jagoda Frost

Max Schaetzel

Younna Osama Mohamed Ahmed Hassanein

National Linguistic Editors

Andrea Rodrigues

Emma Bowar

Parthabi Kanungo

Lara Siminovski

National Technical Editors

Elke van der Heijden

Stefana Feciuc

Pawel Tarnowski

National Academic Supervisor

Maria Jose Recalde-Vela

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

1.1 Introduction

The Netherlands views itself as a leading force in the development of Advanced Digital Technologies (ADT), with its capital Amsterdam set to become one of Europe's leading tech-hubs by 2030.⁶⁰⁹ Whilst the government has gone to great lengths to fast-track legislation to facilitate hosting companies with an information technology emphasis,⁶¹⁰ it has struggled to adopt a national framework which would provide for human rights impact assessments (HRIA).⁶¹¹ The classical rights referred to in the Dutch Constitution have served to protect privacy and freedom of expression rights in the early 21st century, but face difficulty being applied to current technological developments, as they rely on an expansive interpretation of the aforementioned law.⁶¹²

The Netherlands has, to a certain extent, resolved this issue by adopting international and European treaties into the monist Dutch legal system.⁶¹³ By ratifying and adopting (mainly European) laws pertaining to effective human rights protection in many fields of ADT, such as the General Data Protection Regulation (GDPR),⁶¹⁴ the European Charter of Human Rights (ECHR)⁶¹⁵ and the International Covenant on Civil and Political Rights (ICCPR),⁶¹⁶ it has reduced the burden of legislating on the topic.

1.2 National legal framework of human rights and access to human rights impact assessments

1.2.1 The national legal framework

The Dutch Constitution 'grondwet' (Gw) protects the fundamental rights of individuals in relation to digital technologies in articles 7 (freedom of expression), 10 (right to respect for privacy) and 13 (the right to privacy of correspondence).⁶¹⁷ What is noteworthy about these articles is that, with the exception of Article 7, they can only be applied to digital technologies by

⁶⁰⁹ T. Zanni and A. Holt 'KPMG Technology innovation hubs', <<https://info.kpmg.us/content/dam/info/en/innovation-enterprise-solutions/pdf/2019/technology-innovation-hubs-2019.pdf>> accessed 10 February 2021.

⁶¹⁰ M. Hildebrandt, R.E. Leenes, M. Lokin, *Technologie en wetgeving in Cyberspace* (RegelMaat 2012), 61-75.

⁶¹¹ *ibid.*

⁶¹² B.J. Koops, 'Criteria for Normative Technology – The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values', in: R. Brownsword & K. Yeung (red.), *Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes*, (Hart Publishing 2008) 157-174.

⁶¹³ R. Foqué & A.C. 't Hart, *Instrumentaliteit en rechtsbescherming*, (Gouda Quint/ Kluwer Rechtswetenschappen 2011).

⁶¹⁴ Regulation 2016/679 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.

⁶¹⁵ Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) as Amended by Protocol No. 11. *Council of Europe Treaty Series 155*, Council of Europe, 1988 (ECHR).

⁶¹⁶ United Nations, International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

⁶¹⁷ 2008 Constitution of the Kingdom of the Netherlands (*Grondwet voor het Koninkrijk der Nederlanden* (Gw))

analogy. This has to do with the outdated wording of the aforementioned articles, as is showcased by the example of Article 13 sub 2 Gw:

'The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament.'

The lack of mention of other electronic correspondence or information poses a risk to the application of such laws in practice, as it has often been argued that the use of such provisions strays ever further away from the intention of the lawmakers, and thereby the constitutional protection provided.⁶¹⁸

Furthermore, the aforementioned laws are not absolute: they are relative to restrictions given by 'wetten in formele zin' or laws adopted by an act of parliament.⁶¹⁹ This gives the government greater leeway in the interpretation and implementation of said constitutional rights. Such freedom has both positive and negative implications, as the government has adopted numerous laws on the Internet of things (IoT) as well as big data.⁶²⁰ With regard to discrimination based on data, the 'Algemene Wet Gelijke Behandeling' (AWGB) has provided a more contemporary approach to discrimination on the basis of the use of digital technology.⁶²¹ With regard to privacy, the 'Algemene Verordening Gegevensbescherming' (AVG) and its implementing regulation dubbed the 'Uitvoeringswet Algemene Verordening Gegevensbescherming' (UAVG),⁶²² have offered a digitally minded approach to Article 10 Gw, and the rights protected therein. By adopting a broad interpretation, laws surrounding electronic communications, such as the "Telecommunicatiewet," have established a basic set of rights regarding the respect of privacy rights by internet and data providers, as well as telecommunication companies on a more general level. These rules relate to the scrambling and unscrambling of data, as well as access to wiretapping in (for example) criminal investigations.⁶²³

At the same time, legislation providing for a circumvention or restriction of constitutional rights, is based mostly upon criminal activity. Dutch criminal law allows for infringements of digital privacy rights when an individual or company is suspected of having breached the law.⁶²⁴ This may be as part of an ongoing investigation, a suspicion of links to criminal organisations, or a very early suspicion of terrorist activities. The latter of these reasons has allowed the Intelligence Agencies of the Netherlands to expand their digital investigative abilities, including the use of a widespread wiretapping campaign not seen in most other countries.⁶²⁵ This controversial competence is, amongst others, laid down in the 'Wet op de inlichtingen en veiligheidsdiensten' and has come under great scrutiny by the public in recent years.⁶²⁶

⁶¹⁸ Bunschoten, *Tekst en Commentaar Grondwet* (Kluwer 2015), 6-11.

⁶¹⁹ C. Kortmann, *Constitutioneel recht*, (Kluwer 2016).

⁶²⁰ *Kamerstukken II* 2010/11, 32 417, 14-25.

⁶²¹ Vegter, *T&C arbeidsrecht* (Kluwer 2016), 896.

⁶²² GDPR.

⁶²³ Telecommunicatiewet, 19 October 1998, as amended 21 December 2020 (Tw).

⁶²⁴ Wetboek van Strafvordering, 15 January 1921, as amended 01 January 2021 (Sv).

⁶²⁵ *Kamerstukken II* 2005/06, 30 300 VI, nr. 32, 6.

⁶²⁶ As seen by the public referendum held on 21 March 2018, <<https://www.kiesraad.nl/actueel/nieuws/2018/03/29/uitslag-referendum-over-wiv-meerderheid-tegen>>.

1.2.2 Access to national human rights impact assessments

The Netherlands, in its assessment of a human rights violation, makes a distinction between a potential breach by two different types of parties: the government on one side and private enterprises or individuals on the other. This distinction is pivotal, as access to an autonomous and unbiased institution to test these breaches varies accordingly. Companies with a sizable workforce are expected to have an internal mechanism within which an employee is able to bring forward a potential violation of human rights.⁶²⁷ This task is often given to a human resources department or an external union tasked with the wellbeing of the employers of said company; however, if none of those safeguards exist, access to the more general institutions is mandatory.⁶²⁸ These general institutions are the same which launch inquiries of potential human rights violations within the Netherlands.

The relevant institutions for the investigation of human rights violations in regard to ADT are the *College voor de Rechten van de Mens*, the *Nationale Ombudsman* and the *Autoriteit Persoonsgegevens*. These independent institutions have varying rules on admissibility and jurisdiction with regard to ADT based human rights complaints. The *College voor de Rechten van de Mens* is considered to have the broadest jurisdiction, with the ability to investigate complaints on technology related discrimination cases in education, sports, leisure, consumerism, and many other situations.⁶²⁹ The *Nationale Ombudsman* meanwhile investigates complaints brought in relation to government actions and policies, as well as laws which may infringe on human rights. Most cases brought before the Ombudsman relate to discrimination based on the use of AI by local or national authorities, although certain instances of free speech infringements are also accepted by this institution.⁶³⁰ The most specialised cases of human rights infringements in relation to ADTs are dealt with by the *Autoriteit Persoonsgegevens*. It oversees the use of personal data by both private enterprises as well as public institutions and handles all human rights cases with references to privacy infringements by ADTs or the misuse of personal data. It also assesses the seriousness of data leaks or instances of hacking and the subsequent loss of privacy rights.⁶³¹

Note that all these institutions are not based on judicial authority; they are all organs that present a report which can then be used in the national courts as evidence (most notably in civil or administrative courts). This is important, as it demonstrates the fact that the Netherlands uses HRIAs not as a stand-alone enforcement procedure.⁶³² It also does not see human rights violations as the purview of a specific national court who further executes the reports published by the aforementioned institutions.⁶³³

⁶²⁷ H. Sakkers, 'DECENTRALISATIES' EN MENSENRECHTEN IN NEDERLAND *Lokale praktijken in een nationale én internationale context* (NJCM-Bull 2017), 3.

⁶²⁸ E. van den Berg, 'Acting Normal and doing good: the Dutch and human rights', in: I. Lintel, A. Buyse & B. Ley McGonigle (red.), *Defending Human Rights: Tools for Social Justice* (Cambridge Intersentia 2012).

⁶²⁹ 'Instellingen en taken van het College Voor de Rechten Van de Mens' <https://mensenrechten.nl/nl/digitalisering>, accessed 29 January 2021.

⁶³⁰ Wet op de Nationale Ombudsman, 4 februari 1981, as amended on 1 January 2020 (WNO).

⁶³¹ Uitvoeringswet Algemene Verordening Gegevensbescherming, 25 May 2018 (UAVG).

⁶³² Sakkers (n 627).

⁶³³ With the exception of the *Hoge Raad* which is the constitutional court of the Netherlands. Procedures to this court can however only be brought by referral of a more generalised court.

1.3 International legal framework of human rights and access to human rights impact assessments

1.3.1 The International legal framework

Internationally, the Netherlands is party to multiple treaties on human rights in relation to digital advancements and the problems they pose. Most noteworthy amongst these are the rights derived from the treaties of the European Union, to which the Netherlands is a 'Member State'. As mentioned in the introduction, the monist system of the Netherlands allows it to introduce international law into its own legal system without the need of transposition or additional implementation measures, besides those given by the EU itself.⁶³⁴ With respect to human rights, this means that the Charter of Fundamental Rights of the European Union is applicable within the legal system of the Netherlands. Most noteworthy of these rights are Article 8 (protection of personal data), Article 10 (freedom of thought, conscience, and religion), and Article 11 (Freedom of expression and information).⁶³⁵ The CJEU has given special emphasis to data privacy, and, in its case *Google Spain*, clearly defined the importance of the applicability of such a right and what value should be given to it in light of the Charter.⁶³⁶

Furthermore, the Netherlands is a member of the Council of Europe, and the European Convention of Human Rights (ECHR). It has ratified the ECHR, meaning articles 8 (Right to respect for private and family life), 9 (Freedom of thought, conscience, and religion) and 10 (freedom of expression) are of equal application. It should be added that the ECtHR provides the only dedicated judicial review, with regard to human rights, of any treaty to which the Netherlands is a party.⁶³⁷ This constitutes a right for any person to bring an ADT related complaint to the ECtHR without prejudice. It is therefore the most effective protection and enforcement for an individual of their human rights violations, in relation to modern technology.⁶³⁸ National courts of the Netherlands need to inspect human rights violations in light of an underlying claim that is brought forward in either a civil, administrative or criminal court, which may then assess it as a subsidiary aspect to the main case.⁶³⁹ Conversely, the ECtHR accepts claims solely based on human rights violations, creating an individualised mechanism for the review of human rights related infringements.

The International Covenant on Civil and Political Rights (ICCPR) is the last of the treaties significant to ADT related human rights. The Covenant covers many human rights which are also present in the ECHR and the EU Charter, with the most notable being articles 17 (right to privacy), 18 (freedom of thought) and 19 (freedom of expression).⁶⁴⁰ What must also be noted is that, while the Netherlands has signed many of the protocols adhering to the ICCPR, it has not actually ratified them.⁶⁴¹ This is due to the fact that the Netherlands considers the ECHR to be

⁶³⁴ R. Foqué & A.C. 't Hart (n 613).

⁶³⁵ European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02

⁶³⁶ Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317.

⁶³⁷ Council of Europe (n 615).

⁶³⁸ E. van den Berg (n 628).

⁶³⁹ C. Kortmann (n 619).

⁶⁴⁰ ICCPR (n 616).

⁶⁴¹ H. Reiding, *The Netherlands and the Development of International Human Rights Instruments* (Kaaten 1996).

more effective in terms of implementation of its rights. It also sees the enforcement mechanisms of the ECHR as a more successful guarantee than the options offered by the ICCPR.⁶⁴² This means that (in practice) the Netherlands gives secondary importance to the meaning and interpretation of the rights laid down in the ICCPR, when compared to the ECHR or the EU Charter.⁶⁴³

1.3.2 Access to international human rights impact assessments

Almost all of the aforementioned charters offer judicial review to assess potential violations of human rights. The only exception to this rule is the ICCPR which, instead of a judicial mechanism, has the United Nations Human Rights Committee (UNHRC). The UNHRC assesses cases brought before it by member states. This institution is considered to be a semi-judicial one rather than a fully-fledged court. The UNHRC's activity within the Netherlands is limited to recommendations, which may be used as evidence in national court cases, but do not constitute a given right or enforceable ruling in themselves.⁶⁴⁴ This remains at the discretion of the national courts. This severe lack of enforcement causes most cases within the Netherlands to be handled by the ECtHR (instead of the UNHRC), whose decisions do have binding force within the country, since the ECHR has been ratified by the Netherlands.⁶⁴⁵

The ECtHR thereby also forms the most prominent instance of HRIA. The court has the possibility to assess cases from all of its member states including the Netherlands, and forms an autonomous assessment mechanism, separate from the national judicial institutions. Notably (and in contrast to the UNHRC) access by private individuals to the ECtHR is relatively easy, given the central position the ECHR has given the court.⁶⁴⁶ Rulings of the ECtHR are binding within the Netherlands and often include a revision of a national judgement, if the case has been ruled in favour of the applicant.⁶⁴⁷ This makes it the most effective institution to assess HRIAs.

The EU Charter offers a rather peculiar form of HRIA. Article 51 of the Charter states that the rights conferred within the EU Charter are only able to be called upon in relation to acts of the institutions of the EU, or Member States when they are 'implementing Union Law'. This creates a rather restrictive form of access, as the evaluation of whether an infringement of a human right has occurred is fully dependent on whether or not an applicant is able to argue that it occurred during the implementation of Union Law by a Member State, according to the CJEU's admissibility criterion.⁶⁴⁸ In addition, when it comes to advanced technology related human rights infringements, the CJEU prefers to have the appointed institution of the national state (such as the *Autoriteit Persoonsgegevens*) establish whether or not a case has fulfilled the criterion of

⁶⁴² Ministry of Foreign Affairs (the Netherlands), 1986, 366; Appendices to the reports of the Second Chamber, 1982-1983, 17 600, chapter V, no. 2, 51; Appendices to the reports of the Second Chamber, 1997-1998, 25 600, chapter V, no. 2.

⁶⁴³ *ibid.*

⁶⁴⁴ H. Reiding (n 614).

⁶⁴⁵ *ibid.*

⁶⁴⁶ ECHR, art 32.

⁶⁴⁷ *Hoge Raad* 12 april 2002, ECLI:NL:PHR:2002:AD9119.

⁶⁴⁸ Piątek, W. *The right to an effective remedy in European law: significance, content and interaction*, China-EU Law Journal 6, 163–174 (2019).

a state implementing Union law.⁶⁴⁹ This means that, whilst the final assessment is done by the CJEU, the initial consideration of a case is by a national authority.

1.4 Risks to the human rights standards by ADT

Currently, the risks to human rights are considered to be two-dimensional: the Netherlands is considered to be amongst the easiest countries to perform surveillance of individuals based on a criminal investigation,⁶⁵⁰ but at the same time, companies and private institutions are bound to very strict guidelines set out in the AVG.

Within the European cooperation of law enforcement authorities, it is permitted to wiretap conversations or collect electronic data on the basis of a criminal investigation, even if said investigation is not taking place within the Netherlands or the Netherlands has no relevant interest.⁶⁵¹ Merely the indication of an ongoing investigation within a Member State of the EU satisfies the criterion to use these powers.⁶⁵² This greatly increases the risk of infringements of human rights, particularly the right to privacy. In response to the growing threat of terrorism, the government introduced the 'Wet op Inlichtingen en Veiligheidsdiensten' in 2017, which expanded the authority of the national surveillance and security agencies. Most notable (and controversial) is the authorities' ability to 'sweep surveillance' the communication of entire neighbourhoods or towns on the 'credible suspicion' of a potential terroristic threat.⁶⁵³ It also makes it quite difficult for individuals to determine when their human rights have been infringed, as the surveillance agencies are not obliged to inform the person who is (wrongfully) being surveilled.⁶⁵⁴ Upon a request of information to the agencies, most information is redacted and therefore difficult to use in potential court cases as the basis for a human rights infringement.⁶⁵⁵

In contrast to public institutions, private enterprises and individuals have seen a great swell in the responsibility and care required for the handling of data due to the AVG. Whilst this has greatly reduced the number of human rights related cases, instances of so called 'data-leaks' are still a regularity, and incidences of individuals hacking companies for data have been grounds for many human rights related cases in the Netherlands.⁶⁵⁶ The ever-looming threat of data leaks from a corporation is the paramount issue which private enterprises face today.

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

2.1. Introduction

⁶⁴⁹ Sakkers (n 627).

⁶⁵⁰ *Kamerstukken II*, 2008/09, 30 517, nr.11-13.

⁶⁵¹ see articles 5.1.4 and further Sv.

⁶⁵² *ibid.*

⁶⁵³ see articles 18 and 19 Wet op de inlichtingen- en veiligheidsdiensten 2017 (WIV).

⁶⁵⁴ Arts 137 and further WIV.

⁶⁵⁵ *ibid.*

⁶⁵⁶ 27.000 data leaks were reported in 2019, which constitutes a 28% increase from 2018. See 'Jaarrapportage Meldplicht Datalekken':

<<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2019>>. Accessed 18 February 2021.

The protection of personal information is one of the major challenges in the contemporary age of digital technology.⁶⁵⁷ With a significant escalation in the transnational flow of personal data,⁶⁵⁸ the ‘crucial raw materials’ of the global economy,⁶⁵⁹ effective control over the processing of personal information of individuals has been considerably limited.⁶⁶⁰ As such, the need for an adequate response in the form of an obligated level of protection of personal data is of the utmost importance. The right to protection of personal data is, within the legal framework of the European Union, a fundamental right.⁶⁶¹ Furthermore, the ‘European scope’ of the right to protection of personal data has been elaborated on within the case law of the European Court of Human Rights and the Court of Justice of the European Union.⁶⁶²

The principle aim of this section is to examine the protection of personal information within the legal system of the Netherlands. Firstly, the notion of personal data in the national legislation of the Netherlands, as well as in the legal framework of the European Union, will be addressed. Secondly, an analysis of the compatibility of the national legislation of the Netherlands with the law of the European Union, with regard to the protection of personal information, will be provided. The influence of external instruments on data protection in the Netherlands will subsequently be considered.

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

In the legislative framework of the Netherlands, Article 10 of the Dutch Constitution is, with respect to the right to privacy, of paramount importance. Not only is the comprehensive right to privacy acknowledged per se, Article 10 also necessitates that legislation on data protection be laid down by an Act of Parliament.

The scope of personal data is defined in Regulation (EU) 2016/679, hereinafter referred to as the ‘General Data Protection Regulation’ or ‘GDPR’, which is a legal framework with influence over the national legislation of the Netherlands. Taking a broad view of personal information, the General Data Protection Regulation defines personal data as ‘any information relating to an identified or identifiable natural person (‘data subject’).⁶⁶³ An equivalent definition is provided within the international framework of the Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data (1981),⁶⁶⁴ which is legally binding on the Netherlands.⁶⁶⁵ With regard to the concept of identifiable data subject, the GDPR stipulates that in the ascertainment of whether a natural person is identifiable or not, consideration should be given to ‘all the means reasonably likely to be used, such as singling out, either by the controller

⁶⁵⁷ European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Publications Office of the European Union 2018), 975.

⁶⁵⁸ GDPR, recital 5.

⁶⁵⁹ Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) 1.

⁶⁶⁰ Mariusz Krzysztofek, *Post-Reform Personal Data Protection in the European Union: General Data Protection Regulation* (Wolters Kluwer 2017), 24.

⁶⁶¹ GDPR, art 1(2).

⁶⁶² Krzysztofek (n 660), 5.

⁶⁶³ GDPR, art 4(1).

⁶⁶⁴ Council of Europe Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108, art 2 (a).

⁶⁶⁵ Constitution of the Kingdom of the Netherlands, arts 93-94.

or by another person to identify the natural person directly or indirectly'.⁶⁶⁶ Additionally, the GDPR identifies the categories of personal data which are notably sensitive, such as racial or ethnic origin, political, religious or philosophical beliefs, or sexual orientation,⁶⁶⁷ and further defines personal data that relates to criminal convictions and offences.⁶⁶⁸

Correspondingly, the policy-neutral domestic implementation of Regulation (EU) 2016/679 in the Netherlands - the General Data Protection Regulation Implementation Act (2018) (Uitvoeringswet AVG) - provides a definition of the personal data related to an individual's criminal history.⁶⁶⁹

2.3. 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).

An issue of concern, with respect to the protection of personal information in the Netherlands, is the compatibility of the legislative framework of the Netherlands with European Union law. Even though the General Data Protection Regulation is a legal instrument that is directly applicable in the Netherlands,⁶⁷⁰ further domestic legislation clarifying the GDPR's position in the Netherlands was laid down. The Dutch General Data Protection Implementation Act consists of national rules defining the status of the supervisory authority for data protection and the discretionary powers provided for in the General Data Protection Regulation.⁶⁷¹

As such, it is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), the supervisory authority established in accordance with the GDPR⁶⁷² and the General Data Protection Regulation Implementation Act,⁶⁷³ that primarily administers and monitors the application of the GDPR in the Netherlands.⁶⁷⁴ In particular, the Authority is responsible for the assessment of compliance with the GDPR.⁶⁷⁵ Therefore, upon a breach of the law, the Authority is competent to act in accordance with its enforcement powers,⁶⁷⁶ and, for instance, impose an administrative fine, as per Article 83(1) of the GDPR.⁶⁷⁷ Apart from the competence of the Dutch Data Protection Authority to impose administrative fines, the supervisory Authority is allotted additional powers, pursuant to Article 58(6) of the GDPR, as enunciated by the General Data Protection Regulation Implementation Act. Accordingly, the Authority is competent to not only impose an administrative enforcement order (last onder bestuursdwang), but also an order subject to a penalty (last onder dwangsom).⁶⁷⁸

⁶⁶⁶ GDPR, recital 26.

⁶⁶⁷ *ibid* art 9(1).

⁶⁶⁸ *ibid* art 10.

⁶⁶⁹ UAVG (n 631) art 1.

⁶⁷⁰ Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326, art 288.

⁶⁷¹ Data Protection Laws of the World (The Netherlands)

<<https://www.dlapiperdataprotection.com/index.html?t=law&c=NL>> accessed 30 January 2021.

⁶⁷² GDPR, art 51.

⁶⁷³ UAVG (n 631) art 6.

⁶⁷⁴ GDPR, art 57(1)(a).

⁶⁷⁵ *ibid* art 55; UAVG (n 631) art 15(1).

⁶⁷⁶ GDPR, art 58(2).

⁶⁷⁷ *ibid* art 58(2)(i).

⁶⁷⁸ UAVG (n 631) art 16.

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

Membership of the Netherlands in both the European Union⁶⁷⁹ and the Council of Europe⁶⁸⁰ is reflected in the substantial influence of not only the Court of Justice of the European Union but also the European Court of Human Rights, as well as the legal framework of the European Union.

With respect to external influence on data protection in the Netherlands, it is not only the right to privacy, acknowledged in Article 10 of the Dutch Constitution, that is subject to interpretation in light of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. Despite the fact that the wording of the latter provision implies an application restricted to the relationship between individuals and public bodies, the Dutch Supreme Court has recognised the direct horizontal effect of Article 8 of the Convention.⁶⁸¹ As such, an individual in a legal dispute against another individual is able to rely on the fundamental right to protection of natural persons as regards the processing of personal data pursuant to Article 8 of the Convention. Simultaneously, pursuant to the European Court of Human Rights, the protection of personal data falls within the scope of Article 8 of the Convention, on the strength of the fact that the protection of personal information is ‘of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life’.⁶⁸² On that premise, the safeguarding of personal information is addressed as a ‘subset’ of the right to privacy.⁶⁸³ In a similar manner, the right to the protection of personal data is not only acknowledged in the primary law of the European Union:⁶⁸⁴ pursuant to the secondary law of the Union - particularly the General Data Protection Regulation - the Dutch Data Protection Authority, the powers of which substantially influence data protection in the Netherlands,⁶⁸⁵ was established.⁶⁸⁶

Furthermore, data protection in the Netherlands is influenced by the relevant international legal framework. For example, the Universal Declaration of Human Rights (1948), ‘a common standard of achievements for all peoples and all nations,’⁶⁸⁷ although not legally binding, reflects a myriad of principles and rights (such as the right to privacy)⁶⁸⁸ that have been integrated into national constitutional provisions and other domestic laws. Additionally, the right to privacy is acknowledged in Article 17 of the International Covenant on Civil and Political Rights (1996), to which the Netherlands is a Contracting Party.⁶⁸⁹

⁶⁷⁹ European Union, Countries

<https://europa.eu/european-union/about-eu/countries_en> accessed 30 January 2021.

⁶⁸⁰ The Council of Europe in Brief, Member States

<<https://www.coe.int/en/web/about-us/our-member-states>> accessed 30 January 2021.

⁶⁸¹ Supreme Court of the Netherlands ECLI: NL: HR: 1876: AG5500

<<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:1987:AG5500>> accessed 14 February 2021.

⁶⁸² *S and Marper v the United Kingdom* App nos 3056/04 and 30566/04 (ECtHR, 4 December 2008) para 103.

⁶⁸³ Maja Brkan and Evangelia Psychogiopoulou (eds), *Courts, Privacy and Data Protection in the Digital Environment* (Edward Elgar Publishing 2017) 33.

⁶⁸⁴ Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326 art 16(1).

⁶⁸⁵ GDPR, arts 57-58; UAVG (n 631) arts 14-21(a).

⁶⁸⁶ GDPR, art 51.

⁶⁸⁷ Universal Declaration of Human Rights (adopted 10 December 1948) UNGA res 217 A(III) (UDHR).

⁶⁸⁸ *ibid* art 12.

⁶⁸⁹ United Nations Treaty Collection, Status of Treaties (International Covenant on Civil and Political Rights)

2.5. Conclusion

With respect to the protection of personal information in the Netherlands, the recognition of the right to privacy, as well as the obligation to lay down statutory provisions on data protection by Acts of Parliament, is defined in Article 10 of the Dutch Constitution. The definition of personal data is further specified in the General Data Protection Regulation,⁶⁹⁰ an EU legislative instrument that affects the national legislation and is directly applicable⁶⁹¹ in the Netherlands. The General Data Protection Regulation, in a similar manner, not only clarifies the notion of an identifiable data subject⁶⁹² but also lays down the special categories of data.⁶⁹³ Within the Dutch legislative framework, the General Data Protection Implementation Act (the domestic implementation of GDPR) defines personal data with respect to the matters of criminal law.⁶⁹⁴ In terms of the compatibility of the legislative framework of the Netherlands with European Union law, it is the Dutch Data Protection Authority that supervises the application of the General Data Protection Regulation.⁶⁹⁵ In addition, the Authority is responsible for the assessment of compliance with that law⁶⁹⁶ and, as such, utilises a myriad of enforcement powers.⁶⁹⁷ In conclusion, the Netherlands, a Member State of the European Union⁶⁹⁸ and of the Council of Europe,⁶⁹⁹ is subject to the influence of the Court of Justice of the European Union, the European Court of Human Rights, and the legal framework of the European Union. In connection with the international legal framework, the International Covenant on Civil and Political Rights and, in particular, the Universal Declaration of Human Rights have a substantial influence on the domestic constitutional provisions of the Netherlands.

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?

As technology continues to become a prominent part of our lives, the need for regulation regarding privacy rules becomes more important. Due to fast-paced technological advancements, more flexible forms of regulation, such as self-regulation and co-regulation by data controllers and processors, is necessary to create effective data protection regulation. As many controllers and processors are part of the private sector, it is necessary that self-regulation powers are given to them in order to monitor their compliance. This section seeks to address the extent of

<https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en> accessed 30 January 2021.

⁶⁹⁰ GDPR, art 4(1).

⁶⁹¹ Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326 art 288.

⁶⁹² GDPR, recital 26.

⁶⁹³ *ibid* arts 9(1), 10.

⁶⁹⁴ UAVG (n 631) art 1.

⁶⁹⁵ GDPR, art 57(1)(a).

⁶⁹⁶ *ibid* art 55; UAVG (n 631) art 15(1).

⁶⁹⁷ GDPR, art 58(2)(i).

⁶⁹⁸ European Union, Countries

<https://europa.eu/european-union/about-eu/countries_en> accessed 30 January 2021.

⁶⁹⁹ The Council of Europe in Brief, Member States

<<https://www.coe.int/en/web/about-us/our-member-states>> accessed 30 January 2021.

self-regulation by the private sector in the Netherlands and how the public and private sector cooperate in this regard.

3.1. Terminology

- The term **self-regulation** refers to 'the possibility for economic operators, the special partners, non-governmental organisations or associations to adopt common guidelines amongst themselves.'⁷⁰⁰ This form of regulation cannot replace laws and state power, and the relationship between the state and self-regulation should be identified.⁷⁰¹
- **Co-regulation** falls between self-regulation and public regulation on the same continuum. This form occurs when there is a basic legislative act that defines the framework and extent of co-regulation, but the parties are able to conclude voluntary agreements amongst themselves to attain the legislative objectives of the act.⁷⁰²
- A **data controller** as defined under Article 4(7) General Data Protection Regulation (GDPR) refers to the natural or legal person, public authority, agency, or other both which decides the 'why' and 'how' personal data is processed.⁷⁰³
- A **data processor** under Article 4(8) GDPR refers to those who process personal data on behalf of the controller, processors are usually an external third party. However, processors can also be part of a group undertaking where one group acts as the processor for another undertaking.⁷⁰⁴
- A **supervisory authority** in the context of the GDPR is an independent public authority that is responsible for monitoring the Regulation and particularly ensuring fundamental rights and freedoms of natural persons in relation to the processing of personal data within the Union.⁷⁰⁵
- A **code of conduct** is a document that reflects an organization's daily operations, values, company culture, and how employees are expected to act. It is often a powerful tool for self or co-regulation by companies.

3.2. Relevant National Legislation

The General Data Protection Regulation (Regulation (EU) 2016/679 ('GDPR'))⁷⁰⁶ and the 2018 Dutch Implementation Act (*Uitvoeringswet AVG*) are the main legislations regarding data

⁷⁰⁰European Commission, European Parliament & Council of Ministers, 'Inter-Institutional Agreement on Better Lawmaking' [2003] OJC 321/1

<<http://www.europarl.europa.eu/legislative-train/theme-union-of-democratic-change/file-interinstitutional-agreement-on-better-law-making>> accessed 8 February 2021.

⁷⁰¹ Irene Kamara, 'Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate' (2017) 8(1) EJLT <<https://ejlt.org/index.php/ejlt/article/view/545/723>> accessed 12 February 2021.

⁷⁰² European Commission, European Parliament & Council of Ministers (n 92).

⁷⁰³ Regulation 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 [2016] OJ L119/1 (GDPR) Arts 4(7); 29 Working Party, 'Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP 169, 16 February 2010), arts 7-17.

⁷⁰⁴ *ibid* arts 4(8), 24-31.

⁷⁰⁵ *ibid* art 51.

⁷⁰⁶ GDPR.

protection in the Netherlands. These legislative acts have replaced the previous EU Data Protection Directive (Directive 95/46/EC) and the Dutch Personal Protection Act (*Wet bescherming persoonsgegevens*). The Dutch Implementation Act includes exemptions and limitations as permitted by the GDPR. Examples of such deviations are the additional conditions relating to data concerning health as well as criminal convictions and offenses. In addition, there are additional exemptions for data subject's rights and obligations in certain cases.⁷⁰⁷

3.3. Data Protection Supervisory Authorities (DPA)

The main supervisory authority in the Netherlands is the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) hereinafter Dutch DPA. The tasks and powers of the Dutch DPA are described by the GDPR and supplemented by the Dutch Implementation Act. Furthermore, it is bound by the principles of proper administration and the procedural rules of the Dutch General Administrative Law Act (*Algemene wet bestuursrecht*).⁷⁰⁸ The tasks and powers can be divided into four sections: supervising, advising, informing, and international assignments.⁷⁰⁹ The most relevant powers for this section will be stated. Under the supervision task, the Dutch DPA undertakes investigations to assess and monitor compliance with the law pursuant to Articles 55 and 58(1)(e) of the GDPR, if a violation of the law is found, the enforcement powers conferred through Articles 58(2), 83 and 84 of the GDPR are used by the Dutch DPA. Under the Dutch Implementation Act, Individuals and organizations have the right to challenge the Dutch DPA's decisions before administrative courts. In addition to enforcement measures, it can also conduct prior consultations with controllers. This is especially required when a controller's data protection impact assessment (DPIA) suggests a high risk on data protection, the DPIA will be further discussed in a later section.⁷¹⁰ Under Article 40 of the GDPR, the Dutch DPA can assess codes of conduct and under Article 42(1) it can encourage the establishment of data protection certification mechanisms such as data protection seals and marks that demonstrate GDPR compliance by controllers and processors. As part of its advisory tasks as outlined in Article 36(4) of the GDPR, the Dutch DPA provides solicited and unsolicited advice to the legislative proposals and draft texts that deal to a large extent with the processing of personal data. While the Dutch DPA is the supervisory authority for data protection, other supervisory authorities such as the Authority for Consumers and Markets, the Dutch Central Bank, and the Telecom Agency, cooperate with the Dutch DPA on matters regarding data protection.⁷¹¹

3.4. Self-Regulation and Cooperation: Codes of Conduct, Privacy Impact Assessments (PIA) and Data Protection Officers (DPOs)

⁷⁰⁷Herald Jongen, Nienke Bernard and Emre Yildirim, 'The Privacy, Data Protection and Cybersecurity Law Review: Netherlands' in Alan Charles Raul and Sidley Austin LLP(ed), *The Privacy, Data Protection and Cybersecurity Law Review* (The Law Reviews 2020).

⁷⁰⁸Dutch General Administrative Law Act [1992] (*Algemene wet bestuursrecht*) (Awb).

⁷⁰⁹Autoriteit Persoonsgegevens, 'Tasks and Powers of the Dutch DPA' (*Autoriteit Persoonsgegevens*) <<https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/tasks-and-powers-dutch-dpa>> accessed 10 February 2021.

⁷¹⁰GDPR, art 36(1).

⁷¹¹Autoriteit Persoonsgegevens (n 709).

One of the tools of self-regulation under Chapter 4, Section 5 of the GDPR is the opportunity to establish codes of conduct pursuant to Article 40 of the GDPR.⁷¹² Under the provision, organisations are encouraged to draw up such codes ‘to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.’⁷¹³ The benefits are that they take into account the special features of the sector they regulate and can be tailored to the specific data processing that takes place in it. In addition, transnational codes can bridge harmonisation gaps between different Member States due to varying applications of the GDPR. The codes are voluntary accountability tools that could represent a high level of consistency of data protection through practical and cost-effective methods.⁷¹⁴ Organisations have to cooperate with the Dutch DPA in this regard as the codes of conduct need to be approved by the Dutch DPA which also monitors compliance with the code after approval.⁷¹⁵

Another instrument for cooperation is the establishment of Data Protection Officers (DPOs) under Article 37 of the GDPR. The article states that controllers and processors shall appoint a DPO in the cases where: the controller and processor are public authorities, the core activities, the core activities consist of processing operations by require regular and systematic monitoring of data subjects on a large scale, the core activities consist of processing sensitive personal data on a large scale. The tasks of a DPO are set out in Article 39 and include: informing and advising on GDPR compliance, monitoring compliance with the law and with the internal policies of the organisation as well as assigning responsibilities, raising awareness and training staff, to advise and monitor data protection impact assessments where requested and lastly to cooperate and act as point of contact with the supervisory authority. Organisations must register their DPO with the Dutch DPA. Due to the nature of their responsibility, a DPO needs to possess expert knowledge on data protection law and practice, be adequately resourced, independent and report to the supervisory authority (Dutch DPA). DPOs serve as a point between an organisation and the Dutch DPA. They monitor compliance within the organisation but still report to the Dutch DPA when needed.

The Privacy Impact Assessments (PIA) is the Dutch implementation of the Data Protection Impact Assessment under Article 35 of the GDPR, it is based on the GDPR, the Directive Data Protection Investigation and Prosecution and national legislation.⁷¹⁶ A PIA is mandatory in cases where regulations or policies related to the processing of personal data are being developed or when data processing is the consequence of a policy or regulation. In addition, it is mandatory when the intended processing of personal data is likely to result in a high risk to the freedoms of

⁷¹²GDPR, art 40.

⁷¹³ *ibid.*

⁷¹⁴ European Data Protection Board, 'Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.'

<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf> accessed 15 February 2021.

⁷¹⁵ GDPR, art 41.

⁷¹⁶ Rijksoverheid, 'Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)' (2017). For an English translation see:

<https://www.uu.nl/sites/default/files/model_data_protection_imact_assessment_pia_translated_from_dutch.pdf> accessed 15 February 2021.

data subjects.⁷¹⁷ If the processing entails high risk which the controller believes cannot be mitigated, the Dutch DPA is consulted. In 2019, the Dutch DPA received 13 prior consultation requests, with two resulting in positive advice.⁷¹⁸ The PIA provides an example of preliminary self-regulation by controllers with cooperation between the public and private sector when high risk processing is carried out.

3.5. Illustration of Codes of Conduct and DPOs: The Data Pro Code

The first code of conduct was approved by the Dutch DPA in August 2020. The code was the Dutch Pro Code developed by NLDigital, the industry trade association of the Dutch Digital Sector (ICT Sector).⁷¹⁹ It elaborates on the obligations of data processors under Article 28 of the Implementation Act by laying down concrete rules of conduct for processors, this code applies to processing operations in the Netherlands.⁷²⁰ The code is built on three principles: information obligations, review and monitoring, as well as operation and adjustment of Data Pro Code.

Information obligations show the obligation placed on a processor to ensure client awareness, the duty entails that a data processor should inform its clients about the security measures taken with regard to the product or service. To present this in a way that is comprehensible to the consumer, the Data Pro Statement was created. In this statement, the data processor should inform the consumer on the pseudonymisation and encryption of personal data, the ability to ensure integrity, confidentiality and availability of processing systems and services, and the ability in the event of an incident, to restore the availability of and access to personal data in a timely manner.⁷²¹

The second principle regarding review and monitoring shows an independent monitoring of the code of conduct developed by the private industry. It explains that the DPO for this code, the Data Pro Supervisor, is responsible for verifying compliance with the code, handling data breaches complaints with respect to it and assessing whether affiliated parties are qualified to apply the code.⁷²² Furthermore, the Data Pro Supervisor manages the Data Pro register and makes it public. They have administrative discretion to remove data processors from the public register of Data Pro.⁷²³ The Data Pro Supervisor is further required to cooperate with the Dutch DPA if needed.

The third principle regarding operation and adjustment of the Data Pro Code illustrates the flexibility that using self-regulation can provide in contrast to public regulation. The principle states that the Code is evaluated every two years, if changes are proposed, they will be sent for approval to the Dutch DPA. This principle is especially crucial as self-regulation through the GDPR codes of conduct are in their early phases, so openness to change is necessary as there is insufficient knowledge on what to expect.

⁷¹⁷ *ibid.*, 6.

⁷¹⁸ Jongen, Bernard and Yildirim (n 707).

⁷¹⁹ NLDigital is composed of 600 members including both small and medium sized enterprises and tech giants. Its code was drafted with the goal of improving compliance with the EU privacy regulations.

⁷²⁰ NLDigital, 'Meer weten over de Data Pro Code' (*NLDigital*, April 2019)

<<https://www.nldigital.nl/data-pro-code/>> accessed 15 February 2020; UAVG (n 631), art 28.

⁷²¹ *ibid.*

⁷²² *ibid.*

⁷²³ *ibid.*

The Data Pro Code shows the beginning of a possible shift in regulation forms for technology and shows how the Netherlands is opening up to the private sector to set standards for data processing while ensuring compliance with data protection rights standards through requiring approval of codes of conduct as well as monitoring and supervising the implementation of codes of conduct.

3.6. Conclusion

The regulation of data protection by the private sector can be identified as monitored self-regulation, a form of co-regulation. On the one hand, private bodies are allowed to establish their own data protection codes of conduct. On the other hand, they have to comply with GDPR standards, and their codes have to be approved and monitored by the Dutch DPA. Their compliance is further assessed by the independent Data Protection Officers. The recent nature of the very first approval of a code of conduct for data protection in the Netherlands shows that such self-regulation is still at its beginning phases and more developments can be expected in the near future. As the implementation continues to become more utilised, more self-regulation projects like the Data Pro project will come into being, thus strengthening and monitoring the self-regulatory nature of technology. This will make regulation of data protection more sector-specific and efficient while ensuring they are monitored to prevent abuses of power by tech giants. Self-regulation is a more flexible alternative however in order to protect the rights of Dutch citizens, there needs to be supervision and monitoring.

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 a recognised and clearly defined right in the Dutch legal system. This involves protection at the national level as well as through supranational laws with direct effect in Dutch courts. Firstly, the right to data privacy is guaranteed by Art. 10 of the Constitution of the Netherlands. Initially, this provision provided limited protection of privacy, in particular, securing merely the confidentiality of letters and the inviolability of the home. However, in 1983, an amendment was passed to encompass a broader area of 'privacy'. Presently, Section 1 of the article recognises everyone's right to privacy, which the Dutch government has determined to include: privacy in the home, privacy of letter exchanges and communication, as well as the right to not be overheard or spied on, the right to a careful processing of personal data, the right to personal life and that of physical integrity.⁷²⁴ The 1983 constitutional revision additionally introduced two new articles, establishing the obligation of the national government to ensure the protection of their citizens against any possible data abuses (section 2), as well as citizens' right to receive information regarding the recording and the usage of their personal data (section 3). The last section furthermore provides the right to correction of the personal data in question, for instance in cases of mistakes.

⁷²⁴ Kamerstukken II 1975/76, 13 872, No. 2 (1976), 40.

Although the right to data privacy is constitutionally protected, the most significant source of legislation concerning this right is the General Data Protection Regulation (GDPR), of 25 May 2018, whose primary objective is to safeguard the right to the protection of personal data for all natural persons.⁷²⁵ Before the adoption of the GDPR, the right to data privacy was protected by the Personal Data Protection Act, passed in 1999 as means of implementing Directive 95/46/EC of 23 November 1995 which pertained to the processing of personal data. Today, ‘personal data’, as confirmed by the Hague Court of Appeal, can be defined as any type of information, both objective and subjective (i.e., personal opinion), by means of which the data subject can be identified either by the data controller or any other person.⁷²⁶ As a regulation, the GDPR is directly applicable in the Netherlands, allowing all its citizens to rely on its provisions directly, as national law.⁷²⁷ The GDPR is supplemented by the Dutch Implementation Act (in Dutch: *Uitvoeringswet Algemene verordening gegevensbescherming*, or UAVG), passed on 16 May 2018, which implements the regulation to the extent it provides that its rules can be specified or limited by Dutch law. Although the GDPR and UAVG are not the sole sources of law protecting the right to data privacy, they are the most used and cited in Dutch courts in cases of violations of the rules on personal data.

Additionally to national legislation, international law too plays an important role in defining the right to data privacy. This is a result of the Dutch monist legal order, which allows international law to be immediately applicable and override national statutes in cases of conflict of laws, providing individuals with the possibility to rely on treaties ratified by the Dutch government in their national courts.⁷²⁸ There are two international treaties that are primarily used by the Dutch judiciary. In the first place is the European Convention on Human Rights (ECHR), which is binding upon all contracting parties.⁷²⁹ Of particular relevance is Art. 8, which stipulates, in para. 1, that ‘everyone has the right to respect for his private and family life, his home and his correspondence’ and in para. 2, prohibits ‘interference by a public authority with the exercise of this right’, unless this is done ‘in accordance with the law and is necessary in a democratic society’. The scope of the concept of ‘respect for private life’ has been challenged various times in Dutch courts. An example is provided by the C/09/550982/HA ZA 18-388 case of 5 February 2020, in which the Court of the Hague was asked to decide whether the use of the System Risk Indication (SyRI) by the public authorities to combat fraudulent activities violates Art. 8 ECHR. The court concluded that the government failed to ensure a ‘fair balance’ between the right to private life and the interests of society, as ‘SyRI legislation is insufficiently transparent and verifiable’. As a result, its application violates Art. 8(2) ECHR and is thus illegal.⁷³⁰

The second relevant source of supranational law, which may be used in Dutch courts is the Charter of Fundamental Rights of the European Union (CFR). The Charter has direct effect in

⁷²⁵ GDPR, art 1.

⁷²⁶ *C / 10/546981 / HA RK 18-263* [2019] The Hague Court of Appeal ECLI: NL: GHDHA: 2019: 2398 para 4.13

⁷²⁷ TFEU, para 288.

⁷²⁸ Constitution of the Kingdom of the Netherlands 2008, arts 93-94.

⁷²⁹ European Convention on Human Rights: European Convention for the Protection of Human Rights and Fundamental Freedoms, Sept. 3, 1953, ETS 5, 213 UNTS 221 art 1.

⁷³⁰ Case C/09/550982 *NJCM c.s./ De Staat der Nederlanden (SyRI)* ECLI:NL:RBDHA:2020:865 para 6.7.

all EU Member States, and may therefore be invoked in front of Dutch courts, insofar as the case involves an implementation of EU law.⁷³¹ Of particular importance are Art. 7, which recognises the right to respect for private and family life, and Art. 8, which secures the protection of personal data. These provisions were central to the C/13/634059/HA RK 17-233 case, in which the plaintiff brought charges against Google for refusing to remove his picture with the alleged contract killer, taken by a Dutch TV show in 2012. The Amsterdam Court of Appeal concluded that, despite his fundamental rights provided by Arts. 7 and 8 CFR have been violated in the current situation, an exemption is justified in order to preserve the interest of the public.⁷³²

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

According to the GDPR and the UAVG, all data subjects have the right to restrict and object to the data processing. There are three provisions in the GDPR which are of particular importance to the establishment of relevant rights: Art. 17 - the right to be forgotten; Art. 18 - the right to restriction of personal data processing; and Art. 21 - the right to object.

Art. 17 GDPR - the right to be forgotten - is frequently mentioned in Dutch case law, and the correct interpretation of this right has been an object of several legal disputes in the Netherlands. This concept was indirectly established in the *Google v. Spain* case, in which the CJEU confirmed that data subjects may request a search engine to remove public information, if this information is related to the data subject, provided that the interests of the general public are taken into consideration.⁷³³ However, the 'right to be forgotten' may not be granted to everyone. The courts must always consider both parties on a case-by-case basis, and decide whether the interests of one party outweigh that of the other - a principle that has been confirmed by the Arnhem-Leeuwarden Court of Appeal in 2019.⁷³⁴ Further, two types of exceptions can be established through Dutch case law. In the first place is the so-called 'right to remembrance', which, according to the Court of the Northern Netherlands, is the opposite of the 'right to be forgotten'.⁷³⁵ This principle allows for the rejection of a request to be removed from a search engine, in cases where the information may be needed to protect the public interest. However judges do not customarily invoke this rule, as the principle is generally applied when the case concerns criminal data. Therefore, requests by criminals are largely rejected. In fact, in the aforementioned judgement of the Court of the Northern Netherlands, it was concluded that the appellant, a former prisoner, is not fully rehabilitated, and as such, it is in the interest of the general public to have access to information regarding his offences.⁷³⁶ In the second place, Dutch courts must examine and determine whether erasure from the engine will lead to violations of the right to freedom of information. This was illustrated by the AMS 18/7146 case, in which the plaintiff relying, on Art. 17 GDPR, requested Google to remove his name from a list of

⁷³¹ TFEU, art 6(1).

⁷³² C / 13/634059 / HA RK 17-233 FB / DP/ Rechtbank Amsterdam ECLI:NL:RBAMS:2018:2979 paras 4.19-4.20.

⁷³³ Case C-131/12 *Google Spain SL* (n28) paras 81&99.

⁷³⁴ C. 200.256.387, Arnhem-Leeuwarden Court of Appeal, ECLI: NL: GHARL: 2019: 10345 para 4.2.

⁷³⁵ C/18/190912 / HA RK 19-19 Rechtbank Noord-Nederland ECLI:NL:RBNNE:2019:5169 para 5.6.

⁷³⁶ *ibid* paras 6-22-6.23

disciplinary suspended lawyers in the Netherlands Bar Association.⁷³⁷ The Court of Amsterdam, however, dismissed the case, arguing that certain information can be retained for a longer period of time if that is necessary for the exercise of the right to freedom of expression and information, as provided by Art. 17(c)(a).⁷³⁸

Art. 18 GDPR, which grants data subjects the right to restrict the processing of their data, consists of another crucial provision regarding the restriction and objection to the data processing. Art. 4(3) GDPR describes 'restriction of processing' as 'the marking of stored personal data' in order to limit its processing in the future. This moreover includes the right to suspend the processing, as defined in para. 2. Art. 18 provides further scenarios in which the data subject may request a restriction. In the first place, as provided for by para (a), are cases where the data in question is inaccurate or incorrect. In the second place, as provided for by para. (c), the data subject may request a suspension of the data processing if the processing was done illegally. Furthermore, para. (d) stipulates that the data subject may object if their interest outweighs that of the data controller. According to the UAVG, there are, however, certain exceptions to the rules postulated in this rule. Art. 44 GDPR entails that the right to restriction of processing of data may not be exercised in cases of 'scientific research or statistical purposes', while Art. 45 further provides an exception for archiving, and Art. 47 - in public registers.

In this respect, Art. 21 GDPR, which enshrines the right to object, is also an important provision. This Article stipulates that the data subject has the right to object to the processing of their personal data by the controller. Hence, if the data subject objects, the controller must cease the processing, unless there are prevailing circumstances which either override the interests of the data subject, or are related to the establishment, exercise or defence of legal claims. If the controller refuses to do so without reasonable justification, the data subject may bring the dispute before a court, as provided for by Art. 79 GDPR. The controller must therefore evaluate their own interests against those of the data subject, and if necessary, this balancing may be reviewed by a court.⁷³⁹

The GDPR, however, prohibits the collection and processing of certain types of data. This includes data concerning race, ethnicity, religion, political views, trade union membership, sexuality, health data and genetic and biometric data. This rule is reflected in Art. 22 UAVG, which also limits the collection and processing of similar types of information. Consequently, the data subject may refuse to provide such details. Accordingly, the Court of the Northern Netherlands concluded that the ABNA bank violated Art. 22 GDPR by means of requiring information regarding the medical issues of the plaintiff, which were to be used in order to conclude a debt settlement.⁷⁴⁰

It is nevertheless pertinent to mention that the right to object or restrict data processing is not an absolute right, and as such, it is subject to various limitations. Examples of exceptions to this

⁷³⁷ AMS 18/7146 *Rechtbank Amsterdam* ECLI:NL:RBAMS:2019:8329

⁷³⁸ *ibid* paras 6.1-6.5

⁷³⁹ G. J. Zwenne, in: T&C Privacy- en gegevensbeschermingsrecht, art. (21) [Algemene verordening gegevensbescherming], aant (1.1).

⁷⁴⁰ 162046 FT RK 18.474 & 162054 FT RK 18.476 *Rechtbank Noord-Nederland* ECLI:NL:RBNNE:2018:3788.

right may include: consent from the data subject; cases where the processing of the data 'is necessary to protect the vital interests of the data subject or another natural person'; cases where the data is essential in the process of adjudication, among others. [Those exemptions can be found in the GDPR (Art. 9(1) and Article 9(2)(a), (c)-(f)) and the UAVG (Art. 22-30)] Additionally, Art. 23 UAVG allows the Dutch Data Protection Authority to collect special categories of special data if it 'is necessary in order to satisfy an obligation under international law', given that the data is processed by either the National Ombudsman, or the ombuds committee, or in the event that the processing is required in cases related to criminal law.⁷⁴¹ Moreover, Art. 24 UAVG allows the processing of sensitive data for scientific and historical research, while Art. 25 UAVG allows for the processing of data concerning race and ethnic origins 'with the aim of eliminating or reducing actual disadvantages'. In both cases, however, the information must not be processed if the data subject has objected.⁷⁴²

According to Art. 26 UAVG, political beliefs also fall within the scope of such sensitive data, if such beliefs arise in view of a requirement that can be reasonably expected in connection with positions in administrative bodies and advisory boards. The same principle applies to religious and philosophical beliefs, if the data is processed by a non-religion or spiritual organisation, such as, but not limited to, the military, prisons and hospitals.⁷⁴³ Additionally, Art. 28 UAVG, which corresponds to Art. 9(4) GDPR, stipulates that exceptions can be made for genetic data in two separate situations. Firstly, this exception can be made in cases of a 'serious medical interest' (e.g. when medical treatment of others, related to the person in question, is required). Secondly, the processing of genetic data is nevertheless permitted when this information is necessary to a scientific study, provided that the data subject has consented to provide the information and will not be disproportionately harmed, and under the condition that the study serves a general interest. In addition, in an advancing digitised world, the use of biometric data is becoming increasingly vital, as its collection is crucial to the security sectors. Thus, Art. 29 UAVG provides certain exceptions for the prohibition of the collection of biometric data, when it is 'necessary for authentication or security purposes'. In this context, the necessity requirement is of particular importance - in 2019, for instance, the Court of Amsterdam concluded that a shop owner, who required his employees to use a finger scan authorisation system, violated both Art. 29 UAVG and Art. 9(2)(a) GDPR.⁷⁴⁴ This conclusion was reached on the basis of the finding that the implementation of the said authorisation system was not necessary, nor proportionate. Moreover, the workers did not consent to the usage of their biometric data, and as such, denying the data controller the right to process it.⁷⁴⁵ Lastly, it is necessary to mention Art. 30 UAVG, according to which exceptions may be made in reference to health data. Institutions, which may collect this type of data include administrative bodies, pension funds, as well as employers, schools probation institutions, healthcare institutions and insurance companies, if they must assess the risk of contracting with the data subject, or execute an insurance agreement. Here, it must be

⁷⁴¹ Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) (2018) Art 23.

⁷⁴² *ibid* art.25(b)(3).

⁷⁴³ *ibid* art. 27.

⁷⁴⁴ 7728204 CV VERZ 19-9686 Rechtbank Amsterdam ECLI:NL:RBAMS:2019:6005

⁷⁴⁵ *ibid* paras 21-24.

underlined, that all data controllers must keep this processed data confidential, as per Art. 30(4) UAVG.

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?

Each controller has the obligation to notify the Data Protection Authority (DPA) in a timely manner in cases of data protection breaches. ‘Data breach’ can be generally defined as any loss of control over personal data of data subjects.⁷⁴⁶ The process regarding the notification of the DPA and the exceptions to this procedure are regulated by the GDPR and the UAVG. Art. 33 GDPR provides that in cases of data protection breaches, the DPA shall be informed ‘without undue delay’ within 72 hours after the data processor has become aware of the situation. The Article 29 Working Party has determined that a controller becomes ‘aware’ of the situation, once they gain sufficient information and proof that a breach has occurred.⁷⁴⁷ During the 72-hour period, the controller may assess the seriousness and the impact of the incident, and subsequently decide whether the notification will pose a risk to individuals. It is important to note that it is possible to dispatch the notification after the required time frame if such a delay is reasonable.⁷⁴⁸ In such cases the controller must provide an explanation for the delay, and the DPA must be nevertheless informed of all unfolding developments.⁷⁴⁹ In 2018, for instance, the DPA imposed a joint 600,000 EUR administrative fine on Uber B.V. and Uber Technologies for failing to inform the Authority and the data subjects about the data breach within the 72-hour period. Further, according to Art. 33(2) GDPR, the processor must first inform the controller ‘without undue delay’. Unlike the controller, however, the processor does not have the duty to conduct a risk assessment. They might, on the other hand, conduct an investigation if back-ups of data which has been destroyed or lost by the controller is available.⁷⁵⁰

Art. 33(3) GDPR describes the content of the notification which is to be sent to the DPA. It shall, first of all, provide information regarding the nature of the breach, and if possible, the number and the category of the people affected, as well as the number of data records involved and the potential consequences of the breach. Further, contracts of data protection officers must be additionally mentioned, if such posts have been appointed. Lastly, the controller is obliged to propose measures - technical or organisation - to alleviate the negative consequences of the data breach, as such a privacy infraction may have a severe negative impact on the persons concerned. Therefore, if the data controller determines that the data subject is at high risk, the latter must be informed ‘without undue delay’, according to Art. 34 GDPR. This ‘high risk’ requirement is essential in such situations, as the threshold for informing a data subject is higher than that of the supervisory authority.⁷⁵¹ In general, individuals may be at high risk in situations involving sensitive data - special categories of data, financial and identification data, citizen service

⁷⁴⁶ GDPR, recital 85.

⁷⁴⁷ Working Party, ‘Guidelines On Personal Data Breach Notification Under Regulation 2016/679’ (2018), Art 29, 39.

⁷⁴⁸ GDPR, recital 86.

⁷⁴⁹ *ibid* art 33(4).

⁷⁵⁰ Working Party (n 747).

⁷⁵¹ *ibid*, 20.

numbers, copies of documents of identification, among others - and if the breach may result in a stigmatisation, discrimination or health and financial problems.⁷⁵² Moreover, the content of the notification remains the same as that of the notification sent to the DPA and the data subjects must be informed directly.

There are four general exceptions to the aforementioned obligations laid down in Art. 34(3) GDPR and Art. 42 UAVG. Firstly, it is not necessary to inform the data subjects if the controller has taken sufficient technical and organisational protection measures, which have been applied to the data in question. This includes, for instance, the encryption of the breached data. Secondly, it is not necessary to inform the data subjects if the controller has taken decisive measures to ensure that a high risk to the data subjects will not materialise.⁷⁵³ This includes, for example, the remote deletion of data stored in an electronic device.⁷⁵⁴ Thirdly, it is not necessary to inform the data subjects if the effort to notify them will amount to a disproportionate burden on the part of the controller. This occurs when the affected person cannot be reached individually, and therefore a public announcement would be required.⁷⁵⁵

The UAVG provides three additional circumstances in which the data subject may not be notified about the data breach. Art. 41 stipulates that the controller is exempted from the obligation towards the data subject if an attempt to notify (i) may affect national security, national defence, or public safety; (ii) involves the 'prevention, investigation, detection and prosecution of criminal offence'; (iii) is necessary to protect the public interest of the Netherlands the European Union, or the national judiciary system and its independence; (iv) is necessary to ensure the data subject or the rights and freedoms of others, etc. In this context, it is crucial to highlight that, as the right to process, the requirement for necessity and proportionality must be met. In order to reach this standard, multiple factors must be taken into account: the objectives of the processing, the category of the data concerned and the inclusion of any possible safeguards to ensure that data will not be misused. The controller must further consider any possible risks that may arise from their own freedom to process data. Therefore, a balance between the rights of the data subjects, provided for by the GDPR and the UAVG on the one hand, and the public interest together with the interests of the controller, on the other, shall be achieved.

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

5.1. The Right to Data Protection

Given the sensitive nature of personal data, the right to protection of data is accorded the status of being a fundamental right as envisioned by Art. 8 of the European Convention on Human Rights.⁷⁵⁶ As recognised under Recital 1 of Regulation 2016/679, more commonly known as the General Data Protection Regulation (GDPR),⁷⁵⁷ both Art. 8(1) of the Charter of Fundamental

⁷⁵² G. J. Zwenne (n 739) art. 34 annt 1.1.

⁷⁵³ GDPR, art. 34(3)(b).

⁷⁵⁴ G. J. Zwenne (n 739) art. 34 aant 3.3.a.

⁷⁵⁵ *ibid*, aant 3.3.c.

⁷⁵⁶ ECHR, art 8.

⁷⁵⁷ GDPR.

Rights of the European Union⁷⁵⁸ (CFR) and Art. 16(1) of the Treaty on the Functioning of the European Union⁷⁵⁹ (TFEU) stipulate the fundamental right to the protection of natural persons in relation to the processing of personal data. Looking at the national level, Art. 10 of the Dutch Constitution also provides for the right to privacy. Owing to the fact that the Netherlands is both a Member State of the EU and a member of the Council of Europe, its legal framework shows a heavy influence of the jurisprudence of both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR), as well as legislation adopted by the EU.

As established by Art. 288 TFEU, EU regulations are binding in their entirety and are directly applicable in the national legal orders of Member States;⁷⁶⁰ thus they confer rights and obligations not only on EU institutions and Member States, but also on EU citizens. Therefore, the GDPR is directly applicable in the Netherlands. However, due to the fact that it has, in some areas, left room for national implementing measures by the Member States, the Netherlands has subsequently adopted the GDPR Implementation Act (UAVG),⁷⁶¹ which has been in force since 1 January 2020.

Furthermore, the CFR also stipulates the right to an effective remedy as a fundamental right,⁷⁶² as does the ECHR.⁷⁶³ Given the fundamental nature of the right to data protection that is at stake, it is thus of paramount importance that the victim(s) of a data protection breach can have swift and effective recourse to justice.⁷⁶⁴ The GDPR recognises this: Arts. 77-79 affirm the right to lodge a complaint and the right to an effective judicial remedy.

5.2. The Requirement for a Supervisory Authority

The GDPR also entails the requirement for each Member State to provide for a supervisory authority, the *raison d'être* of which is to supervise and monitor the application of the GDPR and therefore protect the fundamental rights and freedoms of natural persons that stem from the processing of personal data.⁷⁶⁵ Pursuant to this provision, the Netherlands has established, through the UAVG, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, AP).⁷⁶⁶ Section 14 of the UAVG forms the legal basis that grants the AP the competence to exercise supervisory powers within the ambit of the GDPR. Thus, the AP forms the independent body responsible for the supervision of personal data processing for the Netherlands. Article 36(1) UAVG also confers upon the AP the right to mediate as a form of dispute resolution in cases of data protection disputes brought by data subjects.⁷⁶⁷ Due to being an administrative body, the AP also falls under the scope of the General Administrative Law Act (in Dutch: *Algemene wet*

⁷⁵⁸ Charter, art 8(1).

⁷⁵⁹ TFEU, art 16(1).

⁷⁶⁰ *ibid* art 288.

⁷⁶¹ UAVG (n 631)

⁷⁶² Charter, art 47.

⁷⁶³ ECHR, art 13.

⁷⁶⁴ GDPR, Recital 85.

⁷⁶⁵ *ibid* art 51(1).

⁷⁶⁶ UAVG (n 631), art 6.

⁷⁶⁷ *ibid* art 36(1).

bestuursrecht (Awb))⁷⁶⁸ in the exercise of its powers and is bound by principles of good administration. Ultimately, it is thus both the Awb and the UAVG that concern themselves with the competences of the AP at the national level.

Another salient feature of the GDPR is the introduction of a supranational organisation to further revolutionise and bolster the EU's data protection enforcement mechanism: the European Data Protection Board (EDPB).⁷⁶⁹ In addition to monitoring the GDPR's implementation throughout the EU and promoting its consistent application,⁷⁷⁰ the EDPB is further entrusted with the power to issue opinions carrying significant authoritative weight — a joint reading of Art. 64(2) and Art. 65(1)(c) GDPR reveals that the EDPB may even adopt binding decisions on any matter that is of general application or produces effects in more than one Member State.⁷⁷¹ Nonetheless, while the EDPB may have a role to play in enforcement of European data protection laws, the GDPR leaves considerable room for implementation to the national legislature, courts, and the national supervisory authority. As such, the Autoriteit Persoonsgegevens remains the main guardian of the General Data Protection Regulation within the Netherlands.

5.3. The Autoriteit Persoonsgegevens & Data Protection Breaches

A breach in the protection of personal data is defined in Art. 4(12) GDPR as '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'.⁷⁷² This means that the scope of a data protection breach is rather wide. Consequently, having regard to Art. 47 CFR, should a data subject believe their right to data protection under the GDPR to have been infringed, they must retain the right to an effective remedy.

The GDPR does not envision a process whereby a data subject may immediately seek recourse with the courts in one's Member State. There do, however, exist several possibilities for data subjects to take action themselves, should they believe themselves to be victim to a data protection breach in the processing of their personal data. Art. 77 GDPR gives any data subject who considers there to be a breach of their personal data the right to lodge a complaint with a supervisory authority.⁷⁷³ While it does not set out any requirements or restrictions as to the form of a complaint, each supervisory authority must take measures to facilitate the submission of complaints to ensure compliance with this Article.⁷⁷⁴ Accordingly, the Autoriteit Persoonsgegevens has made a complaints form available on its website.⁷⁷⁵ It is noteworthy that

⁷⁶⁸ Dutch General Administrative Law Act [1992] (*Algemene wet bestuursrecht*) (Awb).

⁷⁶⁹ GDPR, art 68.

⁷⁷⁰ *ibid*, recital 139.

⁷⁷¹ Dominique Hagenauw and Hielke Hijmans 'The New EU Data Protection Regime' (*Fédération Internationale Pour Le Droit Européen XXIX Congress*, The Hague, 2020) 4
<<https://static1.squarespace.com/static/5574a2fae4b0083487121509/t/5dc42af7d261b94f33bd18df/1573137144670/NL+FIDE+report+Topic+2.pdf>> accessed 19 February 2021 (FIDE).

⁷⁷² GDPR, art 4(12).

⁷⁷³ *ibid* art 77.

⁷⁷⁴ Quirine Tjeenk Willink, in: T&C Privacy- en gegevensbeschermingsrecht, art. 77 [Algemene verordening gegevensbescherming], aant. 1.1.

⁷⁷⁵ Autoriteit Persoonsgegevens, 'Meldingsformulier Klachten'
<<https://autoriteitpersoonsgegevens.nl/nl/meldingsformulier-klachten>> accessed 19 February 2021.

the AP's form has a broader application than required by Art. 77; not only can it be used by data subjects to lodge complaints involving potential personal data breaches, but individuals other than data subjects may also utilise it to alert the AP about alleged breaches of privacy by data controllers and processors.⁷⁷⁶

The AP will start by investigating the complaint's subject matter to the appropriate extent;⁷⁷⁷ it is obligated to inform the complainant on the progress of the complaint and its subsequent decision.⁷⁷⁸ Furthermore, it must also inform the complainant about the possible legal remedies available. A written response of the AP that rejects a complaint falls within the meaning of a decision according to the Awb; pursuant to Art. 3:45 thereof, the AP is obliged to give judicial options in its decision.⁷⁷⁹ The imperative wording of Art. 77 essentially deprives the AP from the freedom of choice when it comes to handling complaints; it must formulate a substantive response to all submitted complaints. Nevertheless, it does enjoy discretion in determining the extent to which it will conduct the investigation upon which its decision will be based,⁷⁸⁰ and may employ the use of prioritisation criteria.⁷⁸¹ Such investigations are subject to judicial review.

Should the AP consider there to be a data protection breach, it will, pursuant to its powers under Art. 58(2) GDPR, impose corrective measures. For instance, under Art. 16 UAVG, the AP can impose an administrative enforcement order to ensure fulfilment of the obligations set out in the GDPR or the UAVG, and/or enforce an order on the basis of Art. 5:20(1) Awb.⁷⁸² Furthermore, it also retains the authority to impose administrative fines on the controller or processor as established by Section 14(3) UAVG.⁷⁸³ The GDPR sets out the fine amounts for infringements under Art. 83. Non-compliance with an order of the AP may also lead to an administrative fine under Art. 83(6) GDPR.

However, should the data subject not be satisfied with the AP's decision, they may have recourse to an effective judicial remedy, pursuant to Art. 78 GDPR,⁷⁸⁴ and take the case before a Dutch administrative court. One may also exercise this right in the event that one's complaint is not handled, or the AP has not informed the complainant about the progress of the complaint within three months following its submission.⁷⁸⁵ In dealing with a complaint under Art. 78 GDPR, the relevant national court retains the right to submit a question for a preliminary ruling procedure under Art. 267 TFEU to the Court of Justice of the European Union (CJEU), should it deem the CJEU's interpretation or clarification on the matter to be necessary in rendering a decision.

⁷⁷⁶ Willink (n 774).

⁷⁷⁷ GDPR, art 57(1)(f).

⁷⁷⁸ *ibid* art 77(2).

⁷⁷⁹ Awb (n 768) art 3:45.

⁷⁸⁰ *Kamerstukken II* 2017/18, 34851, no 3, 28.

⁷⁸¹ Afdeling bestuursrechtspraak Raad van State (ABRvS) ECLI:NL:RVS:2014:1982

<<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2014:1982>> accessed 19 February 2021.

⁷⁸² UAVG (n 631) art 16.

⁷⁸³ *ibid* art 14(3).

⁷⁸⁴ GDPR, art 78.

⁷⁸⁵ Willink (n 774) aant. 2.1.

Nonetheless, a victim is not obliged to at first instance lodge a complaint with the AP; Dutch procedural law does not impose any such obligation either.⁷⁸⁶ Art. 79 GDPR entails the right to an effective judicial remedy against a controller or processor,⁷⁸⁷ meaning that in addition to the administrative law option under Art. 78, one also retains the right to seek recourse to a direct civil remedy against the concerned controller or processor. Therefore, a data subject has an alternative choice between choosing an administrative remedy or a civil one, although it may be practically advantageous to contact the AP first, as the AP's complaint mechanism is free of charge and the expertise contained in the AP's documented decision may later prove to be beneficial to the data subject in enforcement of their rights in court.⁷⁸⁸

5.4. Civil remedies

According to Art. 82 GDPR, data subjects have the right to be compensated for damages suffered for both tangible and intangible harm.⁷⁸⁹ As per Art. 6:95 of the Dutch Civil Code, damages may consist of material loss or other disadvantages, the latter however only insofar as the law gives a right to compensation thereof.⁷⁹⁰ While compensation for material loss is subject - at least in principle - to full compensation, the extent to which compensation is awarded for intangible harm is assessed by the courts in conformity with the standards of reasonableness and fairness.⁷⁹¹ Consequently, in calculating compensation for non-material damage on the basis of Art. 6:106 of the Dutch Civil Code, Dutch judges have discretionary powers; they may take into account all the circumstances of the case in making such a determination, and it remains entirely possible for them to not award compensation at all.⁷⁹²

In spite of the above, compensation for intangible harm has historically not been easily awarded in the Netherlands, and in any case not in large amounts. For example, in a 2007 hearing, the Court of Justice of The Hague recognised a breach of the applicant's right to privacy and that injury to her reputation had ensued, only 500 EUR was awarded in compensation.⁷⁹³ More recently, in January 2021, the Rechtbank Noord-Holland issued its verdict in a case involving a claimant who claimed a breach of his GDPR rights by the Municipality of Oldambt; due to multiple data leaks on the municipality's website, his e-mail address, telephone number and citizen service number had been repeatedly made public. While the court affirmed the existence of a breach of the GDPR, it stated that a violation thereof did not automatically translate to an impairment of a person's integrity and make the person eligible for compensable immaterial damage. Rather, the court held that it would be for the injured party to demonstrate harm to their person and substantiate the alleged damage with concrete data.⁷⁹⁴ The court did not

⁷⁸⁶ *ibid* art 79, aant. 2.2.

⁷⁸⁷ GDPR, art 79.

⁷⁸⁸ Willink (n 774).

⁷⁸⁹ GDPR, art 82.

⁷⁹⁰ *Burgerlijk Wetboek* Art 6:95.

⁷⁹¹ FIDE (n 771), 15.

⁷⁹² ECLI:NL:HR:2001:AB1337

<<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2001:AB1337>> accessed 19 February 2021.

⁷⁹³ ECLI: NL: RBSGR: 2007: BB8427

<<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2007:BB8427>> accessed 19 February 2021.

⁷⁹⁴ ECLI: NL: RBNNE: 2021: 106

consider the claimant to have sufficiently done so. Having regard to the nature and the circumstances of the data protection breach, the court awarded the claimant 500 EUR as immaterial damages.

5.5. Does the Dutch system enable effective data protection?

In conclusion, the Dutch legal system has been instrumental in securing the right to data protection of individuals. The AP has and continues to play a vital role in the safeguarding of this fundamental right. In its dominant role as a supervisory authority, it has tightened the rules for businesses as well as public authorities and has kept a vigilant eye on the processing of personal data, being strict in cases of data protection breaches, for example, by the imposition of heavy fines.⁷⁹⁵ In 2019, the AP received 27,871 complaints, which may arguably be said to indicate a certain trust in the system. Indeed, even public authorities are not exempt from the AP's scrutiny; in September 2018, the AP imposed a penalty payment of 40,000 EUR on the Dutch National Police for not having tightened up data protection measures sufficiently.⁷⁹⁶ On 17 July 2020, an investigation by the AP yielded the conclusion that the Allowances Department of the Tax and Customs Administration had engaged in data processing that was unlawful and discriminatory and thus constituted severe violations of the GDPR.⁷⁹⁷

The courts have also played an important role in the protection of the right to data protection. At the time of writing, a search on the judiciary's online database of court cases reveals a total of 418 cases involving the GDPR since its entry in force on 25 May 2018.⁷⁹⁸ The dual possibility to have access to justice through either an administrative or a civil route reinforces the effective judicial protection of the data subjects' right to data protection and privacy. As substantiated by the aforementioned case law, courts have indeed been instrumental in protecting this fundamental right; they have treated cases of data protection breaches gravely and imposed the appropriate administrative or civil sanctions on the offending entity.

That being said, the Netherlands still has areas of improvement before it may be confidently asserted that its system offers effective protection of data privacy. In promoting swift and effective recourse to justice in case of a data protection breach, one possible suggestion is for the AP to offer a complaint form on its website in English as well. The fact that the complaint procedure is solely in Dutch may prove to be an impediment in enabling effective protection of data privacy of all natural and legal persons within the Netherlands. Moreover, the AP itself has

<<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNNE:2021:106>> accessed 19 February 2021.

⁷⁹⁵ Letter from Autoriteit Persoonsgegevens to Stichting OLVG (26 November 2020)

<https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_olv.pdf> accessed 19 February 2021.

⁷⁹⁶ Autoriteit Persoonsgegevens, 'Nationale Politie voldoet aan last onder dwangsom'

<<https://autoriteitpersoonsgegevens.nl/nl/nieuws/nationale-politie-voldoet-aan-last-onder-dwangsom>> accessed 19 February 2021.

⁷⁹⁷ Autoriteit Persoonsgegevens, 'De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag'

<https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_belastingdienst_kinderopvangtoeslag.pdf> accessed 19 February 2021.

⁷⁹⁸ De Rechtspraak,

'Uitspraken' <[https://uitspraken.rechtspraak.nl/#zoekverfijn/zt\[0\]\[zt\]=%22algemene+verordening+gegevensbescherming%22&zt\[0\]\[fi\]=AlleVelden&zt\[0\]\[ft\]=Alle+velden&idx=19&so=UitspraakDatumAsc&ps\[\]=ps1&du\[\]=ud3&du\[\]=ud4&du\[\]=ud5](https://uitspraken.rechtspraak.nl/#zoekverfijn/zt[0][zt]=%22algemene+verordening+gegevensbescherming%22&zt[0][fi]=AlleVelden&zt[0][ft]=Alle+velden&idx=19&so=UitspraakDatumAsc&ps[]=ps1&du[]=ud3&du[]=ud4&du[]=ud5)> accessed 19 February 2021.

acknowledged being unable to sufficiently fulfil its supervisory duties due to limited manpower and budget.⁷⁹⁹ This has negative consequences for the effective protection of this fundamental right; the AP acknowledged in a report that it currently has insufficient capacity to impose fines. Only 0.04% of the 27,800 complaints and reported infringements in 2019 lead to sanctions, and as many as 1,850 complaints of citizens have been left on the shelf.⁸⁰⁰ This may have severe repercussions for the effective protection of citizens' right to data protection and privacy.

The courts, too, could adopt a more lenient position and raise the compensatory damages awarded in civil suits. This could potentially lead to an increase of the citizen's faith in the system and constitute a better system of judicial protection; the current damages awarded for intangible harm are arguably too low.

In conclusion, while the system in the Netherlands is in need of certain improvements, the work of the AP in conjunction with that of the courts has greatly bolstered the Dutch legal system's protection of the fundamental right to data protection and privacy. The multiple avenues for redress provided for by the GDPR have had a transformative effect on the Dutch legal landscape; it is hoped that in the coming years, the AP and the Dutch courts continue their endeavour to protect this fundamental right in one of the most digitised countries of the European Union.

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

6.1. Introduction

Judicial review is the ability of a national Court to scrutinise the actions of the legislative, executive, and administrative branches of the government, and to determine whether such actions are in consonance with the Constitution. The Dutch Constitution (*Grondwet voor het Koninkrijk der Nederlanden*) has forbidden judicial review against Acts of Parliament within their legislation since 1848;⁸⁰¹ However, in 1980, 'the supreme court began to openly review national laws' compliance with international laws of fundamental rights'.⁸⁰² The compatibility of judicial review in regard to clauses within the Dutch Constitution designed to prevent discrimination against a particular group of people will be evaluated. More specifically, whether anti-discrimination laws are laid down in Article 1 of the Dutch Constitution and Article 14 of the ECHR are respected as fundamental human rights and are consistent with the Constitution or international laws.

⁷⁹⁹ Autoriteit Persoonsgegevens, 'Groeit AP noodzakelijk voor bescherming burgers in digitaliserend Nederland' <<https://autoriteitpersoonsgegevens.nl/nl/nieuws/groeit-ap-noodzakelijk-voor-bescherming-burgers-digitaliserend-nederland>> accessed 19 February 2021.

⁸⁰⁰ Autoriteit Persoonsgegevens, 'Meerjarenbegroting Groeiplan' <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meerjarenbegroting_groeiplan_ap.pdf> accessed 19 February 2021.

⁸⁰¹ S. Brinkel, '(Judicial) Constitutional Review In The Netherlands: A Comparative Law Blog | Peace Palace Library': <<https://www.peacepalacelibrary.nl/2015/03/judicial-constitutional-review-in-the-netherlands-a-comparative-law-blog/>> accessed 18 February 2021.

⁸⁰² Jan ten Kate and Peter J. Van Koppen, 'Judicialization of politics in the Netherlands: towards a form of judicial review' Stage Publication Ltd: <<https://www.jstor.org/stable/1601562>> accessed 17 February 2021.

6.2. Which bodies conduct such review? What new elements are taken into consideration when such review is conducted?

The Dutch legal culture originates from the monist system whereby all national law, including the Constitution, is considered to be hierarchically inferior to international law, and therefore international law is automatically applied in the domestic legal order.⁸⁰³ As a result, the Netherlands still maintains the prohibition of constitutional review by the judiciary guaranteed by Article 120 of the Dutch Constitution 'the constitutionality of Acts of Parliament and treaties shall not be reviewed by courts'.⁸⁰⁴ Elucidating that the courts do not have the authority to evaluate whether a specific statutory provision is in breach with the Constitution or whether the legislative process followed the procedural rules accurately⁸⁰⁵. The Dutch Constitution does however allow for judicial fundamental rights review; being rights to equality, rights freedom, rights against exploitation to name a few. This permits the revoking of regulations that conflict with provisions of treaty law that is 'binding to everyone' on the basis of Article 94 of the Constitution which prescribes for statutes to be reviewed by the judicial for the compatibility provisions of international law.⁸⁰⁶ This provision therefore allows the Dutch judicial system to examine and review legislation in the event that it is called into question and challenged against the aforementioned fundamental rights.

There is a strong correlation between the awareness of fundamental human rights through the establishment of organisations and conventions, such as the European Convention on Human Rights and Fundamental Freedoms (ECHR), and the consciousness of the court's attitude towards parliamentary legislations⁸⁰⁷. This is heavily heightened by the Dutch courts having an obligation to ensure the effective application of European Union and international law into their domestic legal system as a matter of EU law itself due to the inheritance of a monist system⁸⁰⁸.

One of the prime fundamental rights implemented in the ECHR and the Dutch Constitutions is the right to equal treatment. The Dutch Constitution strictly prohibits direct and indirect discrimination on the grounds of religion, belief, political opinion, race or sex, or on any other grounds whatsoever, stated under Article 1 of the Constitution⁸⁰⁹. There are several ways in which the Dutch government upholds the right to equal treatment when individuals feel they have been discriminated against. The individuals can submit an application to either an administrative or criminal court, where the case will be evaluated with the principle of equality⁸¹⁰. Another solution is appealing to the Supreme Court, the highest court in the Netherlands for

⁸⁰³ J. Uzman, T. Barkhuysen & M.L. van Emmerik, 'The Dutch Supreme Court: A Reluctant Positive Legislator?' (2010) vol. 14.3 ELECTRONIC JOURNAL OF COMPARATIVE LAW
<<http://www.ejcl.org/143/art143-16.pdf>> accessed 15 February 2021.

⁸⁰⁴ Constitution of the Kingdom of the Netherlands 2008 (n9) art. 120.

⁸⁰⁵ Supreme Court judgment of 27 January 1961 (*Van den Bergh*). The courts consider themselves banned from interfering in the legislative process on the basis of procedural constitutional requirements as well. See Supreme Court judgment of 19 November 1999, NJ 2000/160 (*City of Tegelen v. Province of Limburg*)

⁸⁰⁶ Uzman, Barkhuysen & van Emmerik (n 803), 2.

⁸⁰⁷ *ibid.*

⁸⁰⁸ Case 26/62 *Van Gend & Loos* European Court of Justice (ECJ) [1963]; Case 6/64 *Costa v. E.N.E.L.* European Court of Justice [1964].

⁸⁰⁹ Constitution of the Kingdom of the Netherlands 2008, art. 1.

⁸¹⁰ J. H. Gerards '*Judicial review in equal treatment cases*', v.83 (Martinus Nijhoff publishers 2005), 2.

civil, criminal, and taxation cases.⁸¹¹ Cases under the administrative courts have a different highest court, the Administrative Jurisdiction Division of the council of states, which carries out the same function as the Supreme Court.⁸¹² For the sake of clarity, the Supreme Court will refer to the highest court for civil, criminal and administrative cases. When the Supreme Court reviews an anti-discrimination case, the court rules on the lawfulness and interpretation of statutory law, in regards to fundamental human rights as long as the right which has been violated is laid down in a self-executing traits provision.⁸¹³ If an individual's right to equality has been violated and the court concludes the national law is inconsistent with the treaty of international law after very careful examination. They have the right to interpret the provision in conformity with the treaty or, if that is impossible, set aside the national provision on the basis of Article 94 of the Constitution, which can be viewed as an exception to Article 120 of the Dutch Constitution. The exception, Article 94, does not however give the courts the authority to declare a statute void. It is important to note that it only allows the court to 'set aside' individual provisions in individual cases.⁸¹⁴

6.3. Does the review constitute effective protection against discrimination?

It has been suggested that the Supreme Court has a history of taking an ambiguous position in their review and interpretation of the law.⁸¹⁵ The judgments are seen to have retrospective effect as the courts assumed that the interpretation used to conclude the case as part of the law itself.⁸¹⁶ 'It is not the court shaping the law but rather the court finding the correct interpretation of the law as rightfully entered by the legislature'.⁸¹⁷ However, there has been significant improvement in the court's willingness to mitigate the temporal effect of its judgments.

If an individual has been discriminated against the court is usually prepared to set aside the statute to give the victim whose human rights were violated compensation.⁸¹⁸ It is important to be aware that 'the court does leave open the possibility of judicial lawmaking if it deems it necessary for an effective protection of fundamental rights'.⁸¹⁹ Viewed in this way, the easiest remedy of protection of judicial review, 'is the power of the civil courts to award damages for unlawful legislation'. Nevertheless, the effectiveness and discursiveness of the compensation paid to the victim must be proportionate to the severity of the situation. Moreover, there is no specific directive that prescribes possible sanctions, it falls upon the Dutch courts to choose a suitable solution to achieve its objective of equality. Notwithstanding, in the process of the Dutch courts choosing the appropriate means to aware compensation, 'it must be adequate in

⁸¹¹ Uzman, Barkhuysen & van Emmerik (n 803), 2.

⁸¹² See, for instance, two relatively recent judgments of the Administrative Jurisdiction Division of the Council of State on suffrage: ABRvS 29 October 2003, *JB 2004/3 (Suffrage for mentally handicapped)*; ABRvS 21 November 2006, *JB 2004/308 (Eman & Sevinger)*. See ABRvS 4 June 2008, *AB 2008/229*.

⁸¹³ Uzman, Barkhuysen & van Emmerik (n 803), 26.

⁸¹⁴ *ibid*, 24.

⁸¹⁵ *ibid*, 27.

⁸¹⁶ *ibid*.

⁸¹⁷ *ibid*.

⁸¹⁸ *ibid*, 30.

⁸¹⁹ *ibid*.

relation to the damage sustained and must therefore amount to more than purely nominal compensation to ensure that it is effective and that it has a deterrent effect'.⁸²⁰

Although it can be inferred that the Dutch legal system has respectable safety guards for the implementation of equality against discriminating acts. Yet it is 'essential that judicial review of the principle of equality is as predictable, objective and careful as possible' as predictability is a necessity in order to elevate as much ambiguity as possible.⁸²¹ This is done by 'developing clear and general rules which the courts apply without interpretation or complex application of the rules'.⁸²² Despite that, it is impossible for the legislator to create statutes for every situation, yet due to the principle of legality when the judges cannot base themselves on legislations, reliance must fall upon the 'formulated provision in the Constitution or treaties or mostly on the vague unwritten principle of equality - meaning it leaves much to be desired'.⁸²³ In practice, the fact that the degree of freedom of interpretation on the practice of equality is unrestricted, makes it a very undesirable feature of judicial assessment, as it allows for judges to apply the principle of equality and treaties based on their comprehension of it which will inevitably be different.⁸²⁴ Thus, while this ambiguity and confusion within the judicial review process remains there will continue to be a lack of certainty and doubts regarding its effectiveness.

6.4. What is a considered role of the technical aspect that results in discrimination? How are the problems tackled?

Our modernised society heavily relies on the use of artificial intelligence (AI) algorithms, automated data processing techniques, and immense architectures, such as Big Data, by the public and private sectors.⁸²⁵ These techniques serve the purpose of presenting data in a more organised and efficient manner which can serve a very beneficial purpose in society. The application of automated data processes are becoming more widespread in business in order to 'discover patterns, statistical correlations in order to optimise their services' and prevent fraud.⁸²⁶ Governmental institutions are relying on AI algorithms to prevent crimes, national security by developing profiles to identify potential terrorists, and within the healthcare sector.⁸²⁷ Nonetheless, processing techniques like Big Data and algorithms do promote efficiency, security, and justice to some extent, yet it also discriminates, violates the right to privacy, and infringes other fundamental human rights protected in the ECHR.⁸²⁸ Automated data processes and algorithms conduct a considerable amount of challenges, regarding its 'unpredictability and opacity',⁸²⁹ not only in the specific area of its function, but 'for society as a whole; the right to

⁸²⁰ See a.o. the *Pig farming Reform Act* judgment, *supra* note 117.

⁸²¹ J. H. Gerards, 'judicial review in equal treatment cases', v.83 (Martinus Nijhoff publishers 2005), 4.

⁸²² *ibid.*

⁸²³ *ibid.*

⁸²⁴ *ibid.*

⁸²⁵ Bart van der Sloot, Dennis Broeders & Erik Schrijvers, *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016), 11.

⁸²⁶ *ibid.*, 9.

⁸²⁷ *ibid.*

⁸²⁸ *ibid.*, 11.

⁸²⁹ Tim O'Reilly, 'The great question of the 21st century: Whose black box do you trust?', 13 September 2016,

available at

<<https://www.linkedin.com/pulse/great-question-21st-century-whose-black-box-do-you-trust-tim-o-reilly?trk=eml->

life, the right to a fair trial, and the presumption of innocence, the right to privacy and freedom of expression, workers' rights, the right to free elections, even the rule of law itself are all impacted'.⁸³⁰ There is an increasing body of evidence that artificial intelligence algorithms use from databases of human rights cases cause a rise of 'serious concerns with regard to article 6 of the ECHR and the principle of equality of arms and adversarial proceedings as established by the European Court of Human Rights'⁸³¹.

Within the criminal justice system the implementation of the use and reliance on data processing and AI algorithms has developed over the years while maintaining the benefits of processing massive data more efficiently and speedily.⁸³² More specifically, in regards to crime prevention and policing, the approach algorithms provide 'goes beyond the ability of human beings to draw conclusions from past offences, in order to predict possible future patterns in crime'. Moreover, it is possible to detect where further crimes might take place at a given time.⁸³³ However, these approaches can be driven by biased terms of ethnic and racial backgrounds whether it is intentional or not.⁸³⁴ Depending on previous crimes that were recorded and which crimes have been selected to be included within the analysis, it could be that previously the police stopped more people with an immigrant background.⁸³⁵ Therefore 'if police focus attention on certain ethnic groups and certain neighbourhoods, it is likely that police records will systematically over-represent those groups and neighbourhoods'.⁸³⁶ Thus, contributing to prejudicial decision-making and discriminatory outcomes because 'if biased data is used to train these predictive models, the models will reproduce (...) those same biases'.⁸³⁷

Moreover, the increased dependency on AI technology to streamline the civil and criminal justice system to augment or even replace the decision making process by human judges raises serious apprehension that such use of technology has proven to be too immature and inaccurate in that the rate of reliability is as low as 79% .⁸³⁸ This gives rise to alarming concerns regarding the use of algorithms 'on the standard of a fair trial provided under Article 6 of the ECHR, notably the presumption of innocence, the right to be informed promptly of the cause and nature of an

b2_content_ecosystem_digest-hero-22-null&midToken=AQGexvwxq0Q3iQ&fromEmail=fromEmail&ut=2SrYDZ8lkCS7o1>. Accessed 15 February 2021.

⁸³⁰ *Algorithms and human rights, study on the human rights dimensions of automated data processing techniques and possible regulatory implications* (Council of Europe 2018), 3.

⁸³¹ *ibid*, 11.

⁸³² *ibid*.

⁸³³ *ibid*, 10.

⁸³⁴ William Issac, Kristian Lum Kristian Lum and William Isaac, 'To predict and serve? Significance', October 10, 2016, The Royal Statistical Society, available at:

<<http://onlinelibrary.wiley.com/doi/10.1111/j.1740-9713.2016.00960.x/epdf>> accessed 11 February 2020.

⁸³⁵ *Algorithms and human rights, study on the human rights dimensions of automated data processing techniques and possible regulatory implications* (Council of Europe 2018), 10.

⁸³⁶ Frederik Zuiderveen Borgesius, 'Discrimination, artificial intelligence and algorithmic decisions-making' 2018, Directorate General of Democracy Council of Europe, 11.

⁸³⁷ *ibid*, 12.

⁸³⁸ Nikolaos Altreas et al 'Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective' PeerJ Computer Science Open Access (Published 24. October 2016), available at <<https://peerj.com/articles/cs-93.pdf>> at p.2; see also The Law society gazette, Monidipa Fouzder, 'Artificial Intelligence mimics judicial reasoning', 22 June 2016, available at: <<https://www.lawgazette.co.uk/law/artificial-intelligence-mimics-judicial-reasoning/5056017.article>> accessed 3 February 2021.

accusation, the right to a fair hearing and the right to defend oneself in person'.⁸³⁹ There are also expanding worries regarding Article 5 which gives protection against arbitrary deprivation of individual's liberty and Article 8 which gives the right to privacy.

As discussed previously, algorithm decision-making does have advantages in regards to speed, and volume of data processed over human decision-making. Moreover, algorithms may appear to be impartial, evenhanded and unbiased, but in reality, it creates unfair and illegal discrimination. A prime example is the data processing some companies used during their employment hiring process, in order to find a 'good' employee. There is a very large scope for the definition of a 'good employee' but let's imagine one of the aspects is someone who is never late to work, that categorisation does not seem discriminator at face value. However, presume individuals with less of an income would be less likely to live in the centre of town as it is more expensive, therefore they will require more time to get into the office than others, due to larger amounts of traffic for example. Suggesting that people who are less wealthy will arrive later to work, and therefore cannot be seen as a 'good employee'. Furthermore, it is known that on average employees with immigrant backgrounds are less wealthy, and therefore are more prone to live on the outskirts of town. Therefore, the algorithm would naturally put people with an immigrant background at a severe disadvantage, bordering discriminatory behaviour.⁸⁴⁰ Additionally, With the growing use of smart devices in our everyday lives, there is heightened surveillance which makes the right to privacy and data protection has become very challenging to maintain. Everything you search online, all the browsing patterns recorded by cookies are all generated in the algorithms to obtain a digital fingerprinting of your profile. Thus, highlighting how algorithms are a contradiction to an individual's fundamental right to private and family life guaranteed in Article 8 of the ECHR.⁸⁴¹

Due to the ambiguousness and biases of data processing techniques in all areas, the effectiveness of the system needs to be analysed. Companies and government entities that have automated data processes in place are trying to introduce tighter control and regulation most importantly in regards to the protection of human rights.⁸⁴² In the Netherlands, human rights are protected by national legislation and international conventions, provided in 'Article 13 of the ECHR which stipulates that everyone whose rights have been violated shall have an effective remedy before a national authority'.⁸⁴³ The Dutch government designed 'The National Action Plan on Human Rights to set out the ways in which the government fulfils its responsibility to protect and promote human rights in their legislation and to place the protection and promotion of human rights on a more systematic footing'.⁸⁴⁴ However, the negative impacts of AI algorithms and automated data processes have been a spiralling issue for many years and therefore no solution can arise overnight.

⁸³⁹ Council of Europe (n 618), 10.

⁸⁴⁰ Borgesius (n 836), 11.

⁸⁴¹ *ibid*, 12-13.

⁸⁴² The vote on 26 January 2016 in the French National Assembly for a new Bill on digital rights. The Bill includes provisions relating to algorithmic transparency and the duty of 'loyalty', or fairness, of online platforms and algorithmic decision-making' (Rosnay 2016).

⁸⁴³ Borgesius (n 836), 23.

⁸⁴⁴ 'National Action Plan on Human Rights', The Dutch Ministry of the Interior and Kingdom relations (2014).

6.5. Conclusion

To conclude, although the Netherlands has a strict prohibition of reviewing legislations against acts of the parliament, the Dutch Constitution does allow for the Supreme Court to review cases in relation to Fundamental Human Rights, in order to uphold the principle of equality. However, it is debatable whether judicial review for discrimination cases is efficient enough to a line with Article 1 of the Dutch Constitution, as judicial review can be seen as unpredictable and vague. Moreover, the increase in reliance of AI algorithms and data processes can be viewed as a threat to the protection of human rights, although extremely beneficial for companies, it violates people's right to privacy and equality. However, the Dutch government is very much aware about the disadvantages that accompany data processes, therefore, they are very adamant on strategically implementing moderations to these architectures that both support the benefits of technology and support individual's fundamental rights.

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?

Although promising substantial benefits, the use of AI may have severe consequences on human rights, especially article 8 ECHR, the right to respect the private life of individuals.⁸⁴⁵ Thus, 'through ... due diligence processes that involve the identification of the human rights risks associated with their AI systems, and taking effective action to prevent and/or mitigate the harms posed by such systems',⁸⁴⁶ governments must act to protect human rights. This section will specifically discuss Dutch legislation on restricting the usage of advanced digital technologies. However, there is also a slight dichotomy that one must remember when considering the aims of these legislations. While Dutch legislation focuses on the human aspect of AI, the EU is more concerned with the ethical usage of these technologies.⁸⁴⁷ The Netherlands thus uses a combination of both EU and domestic legislation in its own legislative system, combining both aims regarding AI usage. The Netherlands has implemented legislation in the past in order to simultaneously ensure the respect for the human rights most vulnerable against these technologies, and to place restrictions on the usage of AI and Big Data to process personal information.

The notions of AI, Big Data and the 'internet of things' (IoT) are deeply interconnected, and are often even used interchangeably. Big Data uses both AI and IoT to collect the data on a macroscopic level, which it then processes and extracts in order for companies to both understand and use the information. AI in particular, has come to be known as an umbrella term

⁸⁴⁵ European Convention on Human Rights, art. 8.

⁸⁴⁶ Commissioner for Human Rights, *Unboxing Artificial Intelligence: 10 steps to protect human rights* (Council of Europe 2019), for more information on AI, see the Council of Europe's (CoE) 'Unboxing Artificial Intelligence' recommendation.

⁸⁴⁷ Louis Junker, Berber Bosch, Heinsman 'AI, Machine Learning & Big Data 2020' (*Global Legal Insights*) <<https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/netherlands>> accessed 28 January 2021.

in recent times, and can be said to encompass the other terms in this section.⁸⁴⁸ Big Data allows for the possibility of companies and authorities to 'collect and analyse large amounts of data to identify attitude patterns and predict behaviours of groups and communities'.⁸⁴⁹ The Internet of Things can be defined as 'interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies'.⁸⁵⁰ It is a vital part in the processing and gathering of personal information, intrinsic to AI and big data, as it allows the two to gather real-time information, the effects of which can be seen in 'smart-cities' such as Eindhoven.⁸⁵¹ Legislation, therefore, often concerns itself with both the responsible, and ethical use of these technologies, in order to prevent any severe human rights breaches. This report will thus explore the domestic legislative acts in the Netherlands, prompted by the external legislative movements within the EU, that aim to ensure the protection of these human rights in light of the risks and dangers that these advanced digital technologies pose.

The Netherlands, as a Member State of the European Union, is an upholder of its wider legal order. It is thus to no surprise that the supranational EU legislature on the advanced technologies deeply impacts and influences the domestic legislative initiatives of the Netherlands. The 2018 Regulation 2016/679 (more commonly known as the 'GDPR'), which lays down the purposes for which controllers may process data information,⁸⁵² was the reason behind the preceding Dutch notification duty, and replaced both the EU Data Protection Directive 95/46/EC and the Dutch Personal Protection Act of 2018.⁸⁵³ The introduction of the GDPR led to the 'General Data Protection Regulation Implementation Act' ('the Act'),⁸⁵⁴ which through its Section 6 provision, and alongside article 51 GDPR, led to the establishment of the *Dutch Data Protection Authority* (AP) as the supervisory body in the Netherlands for the GDPR. The act can be seen as the transpositional mediator between the GDPR and the Netherlands. More importantly, the Act set out exceptions for various GDPR articles, including the right to restrictive processing (Articles 44, 47),⁸⁵⁵ automated individual decision-making (Article 40),⁸⁵⁶ and the right to rectification (Articles 44, 45, 47).⁸⁵⁷ Thus, the effect of this regulation on Dutch legislation cannot be overstated.

⁸⁴⁸ Commissioner for Human Rights.

⁸⁴⁹ Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* (Council of Europe 2017). For more information on Big Data, visit the Council of Europe's guidelines.

⁸⁵⁰ 'Internet of Things Global Standard Initiative' (ITU)

<<https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx>> accessed 30 January 2021. For more information, see the ITU's definition of IoT.

⁸⁵¹ Damion J. Bunders, Kristina Varró, *Problematizing data-driven urban practices: Insights from five Dutch 'smart cities'* (vol 93, Cities 2019) 145-152.

⁸⁵² Regulation 2016/679 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.

⁸⁵³ Chantal van Dam 'Netherlands - National GDPR Implementation Overview' (*OneTrust DataGuidance*) <<https://www.dataguidance.com/notes/netherlands-national-gdpr-implementation-overview>> accessed 1 February 2021.

⁸⁵⁴ UAVG (n 631) art.6

⁸⁵⁵ *ibid* arts 44, 47.

⁸⁵⁶ *ibid* art 40 .

⁸⁵⁷ *ibid* arts 44, 45, 47

There are also several legislative proposals concerning the wider legislative community of the EU that must be mentioned. The 2018 ‘European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment’ of the European Commission on the Efficacy of Justice (CEPEJ)⁸⁵⁸ helped solidify the EU’s stance on AI usage and ethicality. The work of the ‘Council of Europe Ad hoc Committee on Artificial Intelligence’ (CAHAI) is also noteworthy. More recently, the European Parliament issued 3 Resolutions; Res 2020/2012 (INL), Res 2020/2014 (INL) and Res 2020/2015 (INL), which call for an ‘effective, comprehensive and future-proof regulatory framework of Union law’ in order to ‘prevent practices that would undoubtedly undermine fundamental rights’.⁸⁵⁹ All three resolutions, controversially, did not provide legal personality to AI, cementing the view that the goal of AI is nothing more than to ‘serve humanity’.⁸⁶⁰ This laid down the path for future legislative movements that aim to build up the existing legal frameworks, applying them to more ‘modern issues’ of AI.

Domestically, AI is increasingly being used in the private sector to increase the efficacy of advertisements, for which companies often obtain and process personal information of potential clients. As the usage of these technologies - specifically AI and Big-Data - becomes the new status-quo, the possible risks posed to the civilian population cannot be underrated, and the ethicality of this usage must be kept in check. The Netherlands has implemented and enforced numerous legislations to regulate these technologies. Regarding the private sector, the first building block of this protection was the 1999 ‘Dutch Data Protection Act’ (*Wet bescherming persoonsgegevens*), which set out the rules regarding any processed information that corporations, authorities and businesses could possess.⁸⁶¹ Even prior to the implementation of the GDPR in 2018, the Netherlands had imposed their own ‘Dutch notification duty’,⁸⁶² which prescribed that any possible breaches of security measures that could have severe negative effects on data protection must be immediately reported to the *Dutch Data Protection Authority* (AP),⁸⁶³ and all the relevant information regarding the breach be recorded. Additionally, the notification duty also prescribed that data controllers notify individuals whose data could be negatively impacted in the breach.⁸⁶⁴ In the public sector, AI can increase the efficacy of bureaucratic work exponentially, a benefit that authorities cannot ignore in modern times. This has led to the use of AI in several forms, such as the ‘Crime Anticipation System’ (CAS), the Pro-Kid 12-SI, and the Online Fraud Intake System.⁸⁶⁵ However, these potential benefits also contain substantial risks of decreased

⁸⁵⁸ European Commission for the Efficacy of Justice (CEPEJ), *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment* (Council of Europe 2018).

⁸⁵⁹ Vagelis Papakonstantinou and Paul de Hert ‘Refusing to award legal personality to AI: Why the European Parliament got it wrong’ (*European Law Blog*, 25 November 2020) <<https://europeanlawblog.eu/2020/11/25/refusing-to-award-legal-personality-to-ai-why-the-european-parliament-got-it-wrong/>> accessed 5 February 2021, which draws from Parliament Resolution 2020/2012 of 28 September 2020 on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and related Technologies.

⁸⁶⁰ *ibid.*

⁸⁶¹ *Wet bescherming persoonsgegevens*, 1999, 25 892.

⁸⁶² DDPa ‘The data breach notification obligation as laid down in the Dutch Data Protection Act’.

⁸⁶³ Igor Gavic ‘Data protection regulation in the Netherlands in the wake of the GDPR’ (Tjip 2018) <<https://www.tjip.com/en/publications/data-protection-in-the-netherlands-in-the-wake-of-gdpr>> accessed 28 January 2021.

⁸⁶⁴ *ibid.*

⁸⁶⁵ Francien Dechesne and Virginia Dignum, *AI & Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police* (ver 1.2, Leiden/ Delft) 5.

transparency and trust in police work. Regulations against arbitrariness are therefore a necessity, and can be found in legislation, such as Section 126 of the Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), which lays out the rules for obtaining data from civilians,⁸⁶⁶ either through automated or personal means. Additionally, Article 7a of the ‘Police Data Act’ explicitly prohibits any ‘decision based solely on automated processing, including profiling, which has adverse legal effects or significantly affects the data subject’.⁸⁶⁷

Numerous other initiatives have also erupted in both sectors in recent times, which call for further regulations, and incorporation of AI in every-day life. The Dutch government has begun to develop several codes and standards, such as the ‘Code of Good Public Policy’ and the ‘Ethical Code on Artificial Intelligence’,⁸⁶⁸ which aims to regulate the usage of AI in the private sector. There also exist initiatives from the private sector itself, where substantial contributions such as the ECP’s code of conduct are being used as a framework for the Artificial Intelligence Impact Assessment (AIIA). Furthermore, there are also independent initiatives that have come into fruition, the Dutch AI coalition (*NL AIC*) being the most prominent one, which advocates for the incorporation of AI into competitive fields.⁸⁶⁹

In terms of domestic case law, one must note that there are limited cases available that address the specific usage of AI and other advanced technologies in both sectors in the Netherlands, as the processing of information makes up only a small portion of the GDPR rules (found in, for example, Articles 9 and 11 GDPR⁸⁷⁰), and so is often overshadowed by larger, more general issues of data protection and the right of access.⁸⁷¹

The most important of these cases is the recent *SyRI* landmark judgement, where the Hague district court found that the Dutch government, as controllers, did not adequately protect the rights of the population in the way they used their System Risk Indication (SyRI) algorithm system, the legal basis being the 2001 amendment to the SUWI act (*Wet structuur uitvoeringsorganisatie werk en inkomen, Wet SUWI*).⁸⁷² More specifically, the system violated the right to respect for private life under Article 8 ECHR.⁸⁷³ The ruling thus shows that, while these advanced technologies provide considerable advantages, there is an increased importance of human rights in times where digital technologies rapidly evolve.⁸⁷⁴ There must be safeguards and procedures to protect these human rights in place, in order to prevent arbitrary discrimination and biased decision-making based off of the processed information.

⁸⁶⁶ Art 126 of the act of 8 October 2012 van het Wetboek van Strafvordering, 2012, 32717.

⁸⁶⁷ article 7a of the law of 27 July 2007 on the Police Data Act, *Wpg* 2007, 22463.

⁸⁶⁸ Junker (n 847).

⁸⁶⁹ ‘Human Centric AI’ (NL AI Coalitie): <<https://nlaic.com/en/bouwsteen/human-centric-ai/>> accessed 2 February 2021.

⁸⁷⁰ GDPR, arts 9,11.

⁸⁷¹ Chantal van Dam (n 853).

⁸⁷² Jenny Gesley ‘Netherlands: Court Prohibits Government’s Use of AI Software to Detect Welfare Fraud’ (Library of Congress Law) <<https://www.loc.gov/law/foreign-news/article/netherlands-court-prohibits-governments-use-of-ai-software-to-detect-welfare-fraud/>> accessed 1 February 2021.

⁸⁷³ Case C/09/550982 *NJCM c.s./ De Staat der Nederlanden (SyRI)* NL:RBDHA:2020:865.

⁸⁷⁴ Gesley (n 872)

Additionally, the 2019 *Manfield Schoenen* case brought a ruling by the Amsterdam district court, that employers could not oblige their employees to 'use biometric data' to log onto the cash register system, as implementing this obligation would be considered contrary to the GDPR. Furthermore, the court also argued that the processing of information must be proportionate to the interests at stake on both sides. The processing of biometric data is thus prohibited, unless permission was given and/or the situation falls under the scope of the exceptions listed in Article 29 EU-AVG.⁸⁷⁵ This case can, therefore, be seen as a restriction to the usage of IoT for the processing of data, as biometric information distinguishes people from one another, and can easily be misused to discriminate or persecute people based on their personal information. Unsurprisingly, European Courts also do not explicitly rule on the regulation of these processing technologies, but primarily concern themselves with categorizing the scope of the GDPR and other similar legislation.

The prominent *Google Spain v AEPD* case before the Court of Justice of the European Union (CJEU) helped define the scope of 'processing' to incorporate the processing of data from search engines.⁸⁷⁶ Data that is connected to the name of the user must be erased - as this links the information to distinguishable personal information - and the human rights of the user prevail over the economic interests of the controller. Conversely, the CJEU in the *Worten* case decided that while information such as 'working hours' can be considered personal data, it is not inviolable. If this data is processed for legitimate purposes by an authority, then this act is justified and thus does not constitute a violation.⁸⁷⁷ The two cases show the tension between further incorporation of processing technologies and the protection of human rights, highlighting the policy of ethical usage in the wider European legislative community.

Likewise, in the *Facebook Ireland* case, the CJEU decided that the safeguards regulating the usage of AI, where processed data is transferred to a third country, must comply with the standards set out in the ECHR. The assessment of these standards thus, must incorporate the contextual factors. Additionally, the supervisory body must also suspend any data transfer that does not abide by this.⁸⁷⁸

There do not seem to be any cases where Dutch Courts have referenced specific EU case law. However, one can easily look to the relationship between EU and Dutch legislation to conclude that, while not explicitly mentioned, the European judicial decisions have certainly had an effect on the Dutch Court interpretations.

It can thus be concluded that the Netherlands uses a combination of its own domestic legislation, as well as the wider EU community legislation, to regulate the usage of AI in its jurisdiction. The Netherlands has attempted to unify both legislative approaches, and their respective aims - either protecting human rights or the ethicality of these technologies - to enforce the regulation of these technologies, in hopes of preventing mass breaches of the

⁸⁷⁵ Case 7728204 CV VERZ 19-9686 *Manfield Schoenen B.V.* NL: RBAMS: 2019: 6005, para 22.

⁸⁷⁶ Case C-131/12 *Google Spain SL*, para 100.

⁸⁷⁷ Case 342/12 *Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT)* EU:C:2013:355, para 46 (2).

⁸⁷⁸ Case 311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* EU:C:2020:559, para 203 (2).

fundamental right to privacy. This field of technology is one that is still rapidly developing, and the future remains unclear on what risks the deeper exposure to these technologies will bring to human rights. While separate foundational backbones to strict regulations in both sectors exist domestically, the new legal order of the European legislation will undoubtedly influence the future regulations to come.

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

8.1. General comments

Data encryption, which used to be reserved for governments and big corporations, has become increasingly common for consumers in the digital era. A very prominent example is the use of a strong password on a laptop or desktop drive that would make it impossible for a third-party to unlock it. Such development has not only advanced digital security but also the protection of fundamental rights such as data privacy. However, encryption has made it more difficult to perform law enforcement and criminal investigations, especially with the rise in instances and complexities of cybercrime, ranging from child pornography to computer-related fraud. Consequently, balancing these advancements with the importance of crime prevention and detection is a rather vulnerable and complicated dilemma. As a Member State of the European Union (EU), The Netherlands has committed to ensuring an effective and adequate regime of regulating criminal investigations in digital environments, without undermining the human rights enshrined in the Charter of Fundamental Rights of the European Union. In other words, it is important that measures of standard encryption are not compromised as a sanctuary for criminals and yet, guarantee a safe environment in which individuals enjoy their rights to privacy and data protection.

8.2. Scope of research

It remains unclear what personal messages exactly entail, since there is no official legal definition within the Dutch legal framework. Normally, the processing of personal data within the EU, to which the Netherlands is the Member State, is dealt with under the General Data Protection Regulation (GDPR). However, when it comes to the use of data processing in the context of law enforcement, including criminal investigation, the applicable law can be found in Directive (EU) 2016/680 (hereinafter referred as the Police Directive). Both of these legislations (Article 4(1) GDPR and Article 3(1) Police Directive) give the same definition on 'personal data' as the information that can directly or indirectly single out an identified or identifiable person. . Personal messages, therefore, are part of this very broad definition, as in many instances, police in the Netherlands have used personal messages to detect crime committed by specific individuals and collect evidence that renders a crime established. Particularly in 2018, Dutch police had successfully caught suspects involved in money laundering and in criminal organizations through the decryption of encrypted messages on the Ironchat application, by

using cryptophones.⁸⁷⁹ In this section, personal messages can thus be understood as any private communications collected from computer or electrical devices, between users of any given platform. Any encrypted communications between individuals that are lawfully collected and decrypted for the purpose of criminal investigations will fall within the scope of this research.

8.3. Existing legal framework

8.3.1. Structural overview

Since the question deals with the decryption of encrypted data for criminal investigations, the Dutch Code of Criminal Procedure (hereafter DCCP) is the most relevant legislation addressing the specific circumstances under which data processing is allowed and to what extent it can be conducted. Witnessing the shift from investigation of traditional crimes using collected electronic data to computer crimes, Dutch law surrounding the decryption of encrypted data during investigation has been promulgated in the trio of Computer Crime Act (Wet computercriminaliteit) of 1993, the Computer Crime II Act (Wet computercriminaliteit II) of 2006 and most recently the Computer Crime III Act (Wet computercriminaliteit III) of 2019.⁸⁸⁰ Computer crimes in this sense do not only include crimes committed with a computer but also those where telephones and bank cards are manipulated with computer chips. Since these legislations are not separate Acts but actually laws that amended the DCCP, they will be analysed in parallel with the DCCP provisions.

At the crux of our research question lies the proposal of *decryptiebevel* - the so-called decryption order. During the Dutch parliamentary discussions over the Computer Crime Act (CCA) in 1992, the legislature was aware of the potential problems cryptography posed to law enforcement.⁸⁸¹ The Netherlands actually went further to establish the extensive power of decryption order and became the first country to give it shape through the adoption of the CCA (1993). As a far-reaching ex-ante measure for the authorities to command someone to decrypt electronic data that has been encrypted in a manner that third parties cannot access it, any unjustified refusal to cooperate with the order is punishable. Punishment can range from a maximum of three-month imprisonment for not complying with a legal order (as under Article 184 Dutch Penal Code) to specific sentences stemming from other relevant provisions of the DCCP.⁸⁸² Moreover, it is necessary to distinguish between two types of decryption: while some provisions in the DCCP enable the decryption order to be imposed on a person who has knowledge or ability to encrypt data for the interest of criminal investigations, a similar order against the suspects is infeasible. In fact, the Dutch government did propose the possibility of a decryption order for suspects in a draft Bill, but eventually withdrew it after heavy criticism that it failed to respect the privilege against self-incrimination (hereafter the *nemo-tenetur* principle).⁸⁸³

⁸⁷⁹ Article published by the Dutch Police in November 2018, 'Apeldoorn Police have achieved a breakthrough in the interception and decryption of crypto-communication' <<https://www.politie.nl/en/news/2018/november/02-apeldoorn-police-have-achieved-a-breakthrough-in-the-interception-and-decryption-of-crypto-communication.html>> accessed 18 February 2021.

⁸⁸⁰ S Köksal, 'Het Nemo-Teneturbeginsel, Decryptiebevel en de Face ID' (Tilburg University, 2019), 15.

⁸⁸¹ B Kooops, 'Commanding Decryption And The Privilege Against Self-Incrimination' (Intersentia 2000) 2.

⁸⁸² *ibid*, 10.

⁸⁸³ Kamerstukken II (34 372 nr 3, 2015/16).

Although it is not specifically enshrined in Article 6 ECHR, the *nemo-tenetur* principle is an internationally recognised standard stemming from the normative scope of a fair trial under the Convention.⁸⁸⁴ For better understanding of the application and interpretation of Dutch law, it is useful to acknowledge that the Netherlands, as a monist state, applies standards of international law as a part of its domestic law, even in absence of implementation, most visible in the application of the European Convention of Human Rights and Fundamental Freedoms (ECHR).⁸⁸⁵ Therefore, a section will be dedicated to the legal implications of this principle on decryption orders in criminal investigation against suspects under Dutch law, by analysing pivotal ECHR case law.

8.3.2. Specific provisions concerning decryption orders in relevant Dutch legislations

Within the scope of this paper, rules governing the commission and investigation of (cyber)crimes in the DCCP will be divided into three main categories: provisions on criminal investigation of a concrete crime based on probable cause under Articles 126g through 126n(i), of committed and planned organised crime under Articles 120o through 126z, and of terrorist crimes under Article 126z(a) through 126z(u).⁸⁸⁶ In this section, analysis will be conducted on the specific circumstances in which investigation powers on decryption of encrypted data are allowed. Firstly, there are three instances that grant coercive powers for investigation of a concrete crime.

8.3.1.1. Production orders

The Computer Crime Act created a data production order in article 125i DCCP, enabling the investigating judge to order provision of data or its access, if these data have a certain connection to the crime or the suspect or to data logging.⁸⁸⁷ If the data is encrypted, the people targeted by the production order – excluding suspects – can be ordered to decrypt them, according to Article 126n(h) DCCP.⁸⁸⁸ Types of data to be collected and encrypted range from sensitive to identifying data, stipulated specifically in Articles 126n(c) to 126n(f) DCCP. This has an implication for the question at stake, that encrypted personal messages of the data type mentioned in these articles, if necessary for the purpose of criminal investigation of concrete crime under the DDCP, could be lawfully required to be decrypted.

8.3.1.2. Search and seizure procedures

A further ancillary power to the search and seizure procedures was introduced by the Computer Crime Act and finds its legal basis in article 125k DCCP, paragraph 1.⁸⁸⁹ Although this provision serves merely to command a person who is reasonably believed to or has knowledge on the security system or a computerised device, to provide access to it; the second paragraph of the provision applies accordingly to the data, rather than to the security system that comprises such data itself, if encrypted data is found in that system. This enables the investigating officers, the

⁸⁸⁴ B Koops, 'Het Decryptiebevel En Het Nemo-Teneturbeginsel Nopen Ontwikkelingen Sinds 2000 Tot Invoering Van Een Ontslentplicht Voor Verdachten?' (WODC, Ministerie van Veiligheid en Justitie 2012), 1-2.

⁸⁸⁵ B Koops, 'Cybercrime Legislation In The Netherlands' (Intersentia 2010) 3.

⁸⁸⁶ *ibid*, 21-22.

⁸⁸⁷ *ibid*, 22.

⁸⁸⁸ *ibid*.

⁸⁸⁹ *ibid*, 23.

examining magistrate, the public prosecutor, and the assistant public prosecutor to order the person who is reasonably expected to have knowledge on the encryption of data, its decryption, or handing over of a decryption key (Article 125k, para. 2 DCCP). The orders may not be given to suspects, in view of the privilege against self-incrimination (Article 125k, para. 3 DCCP). However, the wordings of Article 125k, paragraph 2 have been very clear in limiting such decryption order to be issued only under the application of Articles 125i and 125j, although this was originally not the intention of the legislators.⁸⁹⁰ That Article 125i only concerns a search to secure data, not a regular search on the basis of Articles 96b, 96c, 97, or 110 has been overlooked, despite the fact that a search will most often be conducted based on one of these other articles.⁸⁹¹ This implies, for the purpose of our paper, that only encrypted personal messages found in a security system or computerised device, during searches under section 125i or 125j, can be given security-undoing or decryption orders.

8.3.1.3. Interception of communications content

The decryption order has been extended by the Computer Crime Act II, in relation to encrypted intercepted communications.⁸⁹² Such an order may be directed at the person who is likely to know the decryption means, but not at the suspect, according to Article 126m, para. 6, 7 DCCP. This is possibly the most relevant provision for the question at stake, because it clearly stipulates that communications of which personal messages form a part, if needed for the purpose of criminal investigation of serious offences, can be lawfully ordered to be decrypted.

Secondly, application of Article 126u(h) DCCP means that, if personal messages are deemed necessary for the criminal investigation of organised or planned crime, the public prosecutor can order the person who may be reasonably presumed to have knowledge of the manner of encryption of the data referred to in these sections, to assist in decrypting the data by either undoing the encryption or providing this knowledge. Lastly, Article 126z(p) DCCP applies likewise, for crimes of a terrorist nature. Under both circumstances, issuing decryption orders against suspects is similarly not allowed.

8.4. The *nemo-tenetur* principle

As analysed above, the decryption order stipulated under Dutch law cannot be issued against suspects, due to its interference with the universal principle of not to incriminate oneself. There is no general definition of the principle in the Dutch legal system or any promulgation in either the Constitution or the DCCP. From the ECHR point of view, the scope of the *nemo-tenetur* principle has not undergone significant changes since 2000, as evident from its case law, despite being quite unclear.⁸⁹³ However, the Dutch Supreme Court has established a formula that 'there is no unconditional right or principle that a suspect can not in any way be obliged to cooperate in the obtaining of possibly incriminating evidence',⁸⁹⁴ meaning that although suspects cannot be forced to actively cooperate, they are still exposed to measures incriminating themselves, such as

⁸⁹⁰ *ibid.*, 24.

⁸⁹¹ *ibid.*

⁸⁹² *ibid.*, 26.

⁸⁹³ Koops (n 612), 2.

⁸⁹⁴ Koops (n 612), 5; Hoge Raad, 15 Februari 1977, C-68586 AC3994.

taking blood samples or fingerprints.⁸⁹⁵ This has created a very clear line between the legality of the decryption of encrypted data against suspects, and that of the collection of biometric data. The ECHR, in paragraph 69 of *Saunders v The UK*, established the Saunders criteria, which is of utmost importance for the interpretation of the *nemo-tenetur* principle. The Saunders criteria has confirmed the Dutch approach by stating that such a principle is not applicable when materials are obtained independently of the will of the suspects for criminal proceedings, such as blood and urine samples.⁸⁹⁶ Decryption keys cannot be obtained independently of the will of the suspect - they can be only when the will of the suspect is weakened under duress.⁸⁹⁷ Subsequently, decryption orders against suspects can hardly be sanctioned without consequences on the *nemo-tenetur* principle.⁸⁹⁸

8.5. The future possibility of decryption order against suspects

Noticeably, the Computer Crime Act III (Wet Computercriminaliteit III) entered into force in 2019, with adaptations in connection with the improvement and strengthening of the detection and prosecution of computer crimes, especially when they are committed in a more ever-complicated and serious manner. In fact, the infamous Amsterdam sex crime case that targeted 83 children, has fueled the restless debate on the decryption order against suspects.⁸⁹⁹ Subsequently, a draft legislation proposed that in the future, such command (for data decryption) can also be given to suspects (in the case of child pornography or terrorist offenses) under penalty of imprisonment of up to 3 years.⁹⁰⁰ However, the proposal has been rejected because it is difficult to not only overcome its tension with the *nemo-tenetur* principle, but also prove the intent of the suspects using the grounds of refusal to comply with the decryption, in order to punish them.⁹⁰¹ Until now, such an order could and can only be given to non-suspects, at least within the context of criminal investigation and the DCCP.⁹⁰² However, other *lex specialis*, which will not be discussed in this paper, can be different.⁹⁰³ Furthermore, Dutch case law does indicate that there are good possibilities to command decryption from suspects if the refusal to cooperate is not punishable.⁹⁰⁴ The suspects then bear the litigation risk that the judge can use his refusal to make decisions against the suspects 'in situations where the presence of protected files clearly raises questions'.⁹⁰⁵

8.6. Level of protection for individuals

As being directly affected by a decryption order, interest parties whose fundamental rights are

⁸⁹⁵ *ibid.*, 5.

⁸⁹⁶ Rijksoverheid, 'Regulering Van Opsporingsbevoegdheden In Een Digitale Omgeving' (2018) 105.

⁸⁹⁷ *ibid.*, 105.

⁸⁹⁸ *ibid.*

⁸⁹⁹ Koops (n 885), 2.

⁹⁰⁰ 'Wetsvoorstel Computercriminaliteit III (Decryptiebevel En Andere Voorstellen)'

<<http://nicokwakman.blogspot.com/2013/05/wetsvoorstel-computercriminaliteit-iii.html>> accessed 19 February 2021.

⁹⁰¹ Rijksoverheid, 'Ontleutplicht' (2019)

<<https://www.rijksoverheid.nl/documenten/rapporten/2019/07/03/tk-bijlage-4-ontleutplicht>> accessed 19 February 2021.

⁹⁰² Wetsvoorstel Computercriminaliteit III (n292).

⁹⁰³ *ibid.*

⁹⁰⁴ Koops (n 885), 2.

⁹⁰⁵ *ibid.*

possibly jeopardised should be given adequate protection under Dutch law, pursuant to other international standards that the Netherlands has committed itself to, prominently the ECHR. This includes not only the protection of substantial rights such as the right to privacy, right to data protection, but also procedural rights such as the right to a fair trial, the right to legal remedies. The Computer Crime Act III has amended Article 552a, paragraph 1 DCCP, which now reads that interest parties can file a written complaint about the order to provide access to encrypted data, instead of 'on the claim to cooperate in the decryption of data' as it was in the past. Such wordings are clear on the relation between the decryption order and the right to judicial remedy of individuals. This article also stipulates that the complaint has to be decided promptly. The complainant and the public prosecutor can appeal in cassation against the decision on the notice of complaint (Article 552d paragraph 2 DCCP).

At the moment, circumstances in which decryption orders against non-suspects can be issued have been stipulated in a rather clear and detailed manner, within the framework of the DCCP. Only authorities with official capacity to deal with criminal investigations, such as public prosecutors or investigating officers, are vested with the power to issue decryption orders on encrypted data specifically required in the interest of the investigation. However, such wordings can be problematic in the sense that they fail to take into account basic principles relating to processing personal data under Article 4 (1) of the Police Directive, such as data minimization or storage limitation.

Lastly, the definitive scope of the *nemo-tenetur* principle and its interpretation requires a more clear legal basis in cases where decryption orders for the purpose of criminal investigations are issued. This will have an important influence on not only the possibility of legality for the decryption order against suspects in the future, using the overriding public interests as justifications, but also on the legal implications and application of the necessity and proportionality test when such interferences occur.

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

As one of the surveys demonstrates, the Netherlands cares more about human rights protection than many other countries in the world.⁹⁰⁶ Although much has been done to establish a balance between fast-changing digital advancements and the protection of human rights online, there is still great potential to improve this area.

The Dutch Constitution enshrines several fundamental human rights; however, its wording leaves significant room for interpretation.⁹⁰⁷ The Dutch Constitution provides for the highest protection of rights compared to other domestic legislation. This is due to the complex amendment procedure, which requires the House of Representatives (in Dutch: *Tweede Kamer der*

⁹⁰⁶ 'Countries Seen to Care About Human Rights'

<<https://www.usnews.com/news/best-countries/articles/the-10-countries-that-care-the-most-about-human-rights-according-to-perception>> accessed 14 February 2021.

⁹⁰⁷ Constitution of the Kingdom of the Netherlands, art 13(2).

Staten-Generaal) to vote by a simple majority in favour of the proposed amendment,⁹⁰⁸ followed by the dissolution of that chamber.⁹⁰⁹ Once an election is held, the proposal is to be read for the second time, and approval requires a supermajority of the votes in both chambers.⁹¹⁰ This complex procedure guarantees the highest possible protection of any right laid down in the Dutch Constitution. Conversely, the vague terminology allows the judicial branch to exercise more discretionary power; however, this discretion is blocked, to some extent, by other legislation on the national and European level.

As explained in the previous chapters, one of the most important laws in the area of data protection is the General Data Protection Regulation (Regulation (EU) 2016/679 (hereinafter: 'GDPR'))⁹¹¹ and the Dutch Implementation Act (in Dutch: *Uitvoeringswet Algemene verordening gegevensbescherming*, hereinafter: UAVG).⁹¹² According to the *Survey 2020*, the Netherlands has the highest number of GDPR breaches amongst all the countries in the EU. Not only is the total number the highest (40'647 breaches within a 20 months period), but the number per citizen is as well.⁹¹³ This can appear quite worrying, as the number is relatively high compared to other countries; however, this also demonstrates that the Dutch authorities are more aware of the GDPR and possible breaches, and are willing to intervene when such a breach may have occurred. According to a report published by the Dutch Data Protection Authority (in Dutch: *Autoriteit Persoonsgegevens*, hereinafter: 'AP'), more than 94% of the Dutch citizens are concerned about protection of their personal data.⁹¹⁴

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).

9.1.1. Wet op de inlichtingen- en veiligheidsdiensten 2017

In 2017, the Dutch government announced the implementation of the Intelligence and Security Services Act 2017 (in Dutch: *Wet op de inlichtingen- en veiligheidsdiensten 2017*, hereinafter: 'Wiv'), in the area of special investigatory powers granted to the General Intelligence and Security Service of the Netherlands (in Dutch: *Algemene Inlichtingen- en Veiligheidsdienst*, hereinafter: 'AIVD'). Wiv entered into force on 1 May 2018.⁹¹⁵ The newly adopted act permits AIVD to observe and follow people, to make use of agents and to monitor and tap any form of telecommunications.⁹¹⁶ In addition, AIVD is allowed to break through security and recover encrypted data.⁹¹⁷ However, as per Wiv, decryption can only be conducted with ministerial authorization and permission from

⁹⁰⁸ *ibid* art 137(2).

⁹⁰⁹ *ibid* art 137(3).

⁹¹⁰ *ibid* art 137(4).

⁹¹¹ GDPR.

⁹¹² UAVG (n 631)

⁹¹³ 'GDPR Data Breach Survey 2020'

<<https://www.dlapiper.com/en/us/insights/publications/2020/01/gdpr-data-breach-survey-2020/>> accessed 19 February 2021.

⁹¹⁴ Autoriteit Persoonsgegevens, 'Balans - Jaarverslag 2019' (Report, 2019)

⁹¹⁵ 'The Intelligence and Security Services Act 2017'

<<https://english.aivd.nl/about-aivd/the-intelligence-and-security-services-act-2017>> accessed 16 February 2021.

⁹¹⁶ Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv) art 25 and 40 [The Intelligence and Security Services Act].

⁹¹⁷ *ibid* art 45.

the Review Board for the Use of Powers (in Dutch: *Toetsingscommissie Inzet Bevoegdheden*, hereinafter ‘TIB’).⁹¹⁸ This demonstrates that the scope of powers provided for in Wiv is quite broad. In fact, AIVD favours the possibility of issuing such a decryption order directly by their own agency.⁹¹⁹ This would grant AIVD more independence, and allow for faster and more efficient work; however, such orders impact the right to privacy of the citizens. Moreover, there exists a possibility of abuse by third parties, such as criminals or terrorists.⁹²⁰ Bearing those risks in mind, the Dutch government announced in 2016 that it would not take any legal measures to hinder the use of encryption in the country.⁹²¹

In spite of these issues, the Act is not indifferent to the concerns of society or non-governmental organizations (eg. Amnesty International).⁹²² Before entering into force, a consultative referendum initiated by Dutch students was conducted. The majority of voters opposed the Act.⁹²³ Although the referendum was not binding, the Dutch government adjusted several points which the public found worrisome. Despite these adjustments, the Public Interest Litigation Project (in Dutch: *Strategisch procederen voor mensenrechten*, hereinafter: ‘PILP’) argued that Wiv still provides inadequate safeguards to protect fundamental human rights, including the right to privacy.⁹²⁴ The list of all responses to Wiv was published on the official government website.⁹²⁵

On 18 April 2018, the PILP, together with other national and international organizations such as Greenpeace, Bits of Freedom, Free Press Unlimited and a few private companies, requested that the Dutch government postpone Wiv’s entry into force. Their request was rejected.⁹²⁶ The coalition initiated the urgency procedure against the Dutch government before the District Court of the Hague, to prevent Wiv from entering into force. The hearing was held on 7 June 2018; however, their claims were rejected and the Court decided the case for the State.⁹²⁷

Due to the unprecedented level of societal reaction, both from the Dutch citizens and the (inter)national organisations, the Evaluation Committee Wiv (in Dutch: *Evaluatiecommissie Wiv 2017*, hereinafter: Committee) was established. Following the decision of 24 April 2020, the Committee began its work on 1 May 2020.⁹²⁸ Their main task was to examine the effectiveness of

⁹¹⁸ The Intelligence and Security Services Act 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*) (Wiv) arts 32-33.

⁹¹⁹ Q Eijkman, N van Eijk and R van Schaik, *Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?* (Institute for Information Law, UvA 2018) 17.

⁹²⁰ *ibid.*

⁹²¹ ‘Kabinetsstandpunt Encryptie’ <<https://zoek.officielebekendmakingen.nl/kst-26643-383.html>> accessed 19 February 2021

⁹²² ‘Veiligheid en mensenrechten’ <<https://www.amnesty.nl/wat-we-doen/themas/veiligheid-en-mensenrechten>> accessed 14 February 2021.

⁹²³ ‘Nationaal referendum 21 maart 2018’ <<https://verkiezingsuitslagen.nl/verkiezingen/detail/NR20180321/667205>> accessed 16 February 2021.

⁹²⁴ ‘NJCM publishes concerns regarding proposed amendments to the Bill for the Intelligence and Security Services Act (Wiv)’ <<https://pilpnjcm.nl/en/njcm-publishes-concerns-regarding-proposed-amendments-bill-intelligence-security-services-act-wiv>> accessed 15 February 2021.

⁹²⁵ ‘Wijziging Wiv 2017’ <<https://www.internetconsultatie.nl/wiv2017/reacties>> accessed 13 February 2021.

⁹²⁶ ‘Bill for the Intelligence and Security Services Act (Wiv)’ <<https://pilpnjcm.nl/en/dossiers/bill-intelligence-security-services-act-wiv/>> accessed 19 February 2021.

⁹²⁷ Rechtbank Den Haag, 26 Juni 2018, C-09-553023-KG ZA 18-476.

⁹²⁸ ‘Evaluatiecommissie Wiv’ <<https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen-en-veiligheidsdiensten/evaluatiecommissie-wiv>> accessed 14 February 2021.

Wiv, and to analyse the substantive content in light of other national legislation. The Committee's report was published on 20 January 2021.⁹²⁹ It found that Wiv is an important safeguard added to the system; however, the Committee also proposed some amendments to the current version of Wiv. Firstly, the collection and use of bulk data must be safeguarded by more limitations, in response to the concerns of the citizens. Moreover, the Committee recommended that additional safeguards should be introduced for the exchange of data with foreign services. The Committee also endorsed a role for the administrative judge, to adjudicate on differences of opinion between the executive branch and AIVD.⁹³⁰

As stated in the report, Wiv falls short regarding its substantive content, considered in light of the relevant Dutch law. It can therefore be expected that in the (near) future, new amendments may be added to Wiv providing for more safeguards and further protection of fundamental human rights.

9.1.2. Proctoring the exam v. right to privacy

One example of a controversial situation is the use of a proctoring system for exams. In June 2020, one student sued the University of Amsterdam for using the Proctorio system for monitoring students while taking their exams at home. The applicant claimed that this system violated his right to privacy, as the software records a student's webcam, microphone, internet traffic and inputs.⁹³¹

The Amsterdam Court of First Instance rejected the claims presented by the student. It was argued that the use of such a software is justifiable under Art. 6(1)(e) of the GDPR. The task of organizing and conducting exams falls into the category of public tasks.⁹³² In addition, due to the pandemic, the University could not offer a more suitable option to monitor the exams. Art. 9(1) of the GDPR⁹³³ lists the personal data of special categories. As explained in the judgement, webcam recordings do not fall into any of the categories due to the fact that the student's private environment is not personal data of a special category. The software does not track the user's eyes, respiration, biometrics or stress. In addition to the aforementioned arguments, the Court did not find any violation of the principles enshrined in Art. 5 of the GDPR.⁹³⁴

Although the case was rejected by the Court of the First Instance, the use of monitoring software during the exams generated heated societal debate, not only in the Netherlands. The system uses full algorithmic functions (Artificial Intelligence), and as explained on the official website, it utilizes 'machine learning and advanced facial detection technologies'.⁹³⁵ The software records each movement that the student makes via webcam, and sends it to the supervisor in case any suspicion is present. Additionally, Proctorio has access to the student's desktop,

⁹²⁹ 'Evaluatiecommissie Wiv: enkele wijzigingen wet noodzakelijk' <<https://www.defensie.nl/actueel/nieuws/2021/01/20/evaluatiecommissie-wiv-enkele-wijzigingen-wet-noodzakelijk>> accessed 19 February 2021.

⁹³⁰ *ibid.*

⁹³¹ Rechtbank Amsterdam, 11 Juni 2020, C-13-684665-KG ZA 20-481.

⁹³² GDPR, art 6(1)(e).

⁹³³ *ibid* art 9(1).

⁹³⁴ *ibid* art 5.

⁹³⁵ 'About' <<https://proctorio.com/about>> accessed 15 February 2021.

including the possibility to follow when each button is pressed or when and how the copy-paste function is used.⁹³⁶

The Asva Student Union (in Dutch: *De Asva Studentenunie*, hereinafter: ‘Asva’) opposes the use of Proctorio. As ruled by the Court of First Instance in Amsterdam, the use of Proctorio is justifiable in case there are no other methods allowed for conducting the exam and it is used as a last resort measure; however, that is not the situation in many cases, if at all. Asva argues that, depending on the Faculty, the exam uses Proctorio or it does not, which demonstrates that other methods of examination exist, such as writing an essay.⁹³⁷

9.2. Conclusion

The Netherlands has a variety of legal instruments regarding digital advancements and the protection of fundamental human rights, including European legislation; however, due to the fact that the digital advancements evolve exceptionally fast, new problems regarding protection of human rights online arise frequently. As explained in this section, not only can Dutch legislation create problems with regards to safeguarding human rights online, but also the use of AI software at universities has caused concern. These issues were analysed to illustrate that the balance between digital developments and fundamental rights is delicate, and that much must still be done in this area.

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?

10.1 Introduction

The situation regarding the area of human rights and technology in the Netherlands is quite concerning. In the last two decades, The Netherlands has enacted several laws to provide protections to individuals, such as the 2018 Dutch Personal Protection Act (*Wet bescherming persoonsgegevens*) and the 1999 Dutch Data Protection Act. These laws have since been replaced in favor of the 2018 Regulation (EU) 2016/679 (GDPR).⁹³⁸ The Netherlands uses a combination of national and EU law, therefore, alongside the GDPR, the Netherlands also uses the Dutch General Data Protection Regulation Implementation Act (*Uitvoeringswet Algemene verordening gegevensbescherming*). The country has also established the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) hereinafter Dutch DPA which supervises personal data processing.

Although the Netherlands has previously taken great strides to illustrate the importance of human rights with regards to technology, there is a possibility that the country is regressing on this front. The Netherlands relies on the monist system of law; therefore, while the country has previously enacted laws protecting rights on the national level, the country now primarily relies on the GDPR. Additionally, the Netherlands has not had recent discussions regarding laws that

⁹³⁶ More on Artificial Intelligence in Question 6.

⁹³⁷ Marlie van Zoggel, ‘Studenten delen luiers uit als protest tegen surveillanceprogramma UvA’ <<https://www.parool.nl/amsterdam/studenten-delen-luiers-uit-als-protest-tegen-surveillanceprogramma-uva~b6aa57a0/>> accessed 12 February 2021.

⁹³⁸ GDPR.

enhance protection of human rights. The country has instead passed laws, such as the Act on the Intelligence and Security Services (*Wetsvoorstel Wet op de inlichtingen en veiligheidsdiensten*), which many have claimed violates the right to privacy.⁹³⁹

Dutch law, particularly with regard to the online protection of human rights and the regulation of advanced digital technologies, is heavily influenced by European Union law. In regard to data protection, the GDPR is one of the most influential pieces of legislation in the entire EU.⁹⁴⁰ Such influential legislation also exists - or is being created on the national level - for advanced digital technologies, such as AI, IoT and big data.⁹⁴¹

The principal aim of this section is to outline the current state of legislation protecting human rights online, after which the major trends and developments are discussed. The primary trend in legislation protecting human rights online is one of the stricter and more specific regulation.

10.2 Modern Law in the Netherlands

The Netherlands uses a combination of national and regional law in regards to human rights and technology. At national level, the Netherlands uses the Dutch General Data Protection Implementation Act,⁹⁴² which works in conjunction with the GDPR to protect rights associated with technology. The Dutch Data Protection Implementation Act maintains rights from the original national data protection law, the Dutch Data Protection Act.⁹⁴³

While the above laws protect human rights, there are some laws that have sparked controversy for potentially allowing the stripping of rights. The 1993 Computer Crime Act (*Wet computercriminaliteit*), the 2006 Computer Crime Act II (*Wet computercriminaliteit II*) and most recently the 2019 Computer Crime Act III (*Wet computercriminaliteit III*) are the three laws that amended the Dutch Code of Criminal Procedure. The aforementioned three laws allow law enforcement to request encrypted messages be decrypted by individuals in a criminal investigation.⁹⁴⁴ This was controversial as it was considered a violation of privacy. Furthermore, the third Act of 2019 proposed that suspects of a criminal investigation would also be forced to decrypt encrypted messages under a penalty of three years in prison. While this proposal was rejected due to privacy concerns, similar laws may enter into force in the Netherlands in the near future as security concerns grow.⁹⁴⁵

Privacy has also been threatened under the Act on the Intelligence and Security Services, another controversial law recently introduced in the Netherlands for national security. The law targets areas with potential terrorist activity, and allows for law enforcement to perform a complete

⁹³⁹ Kiesraad, Nationaal referendum 21 maart 2018

<<https://verkiezingsuitslagen.nl/verkiezingen/detail/NR20180321/667205>> accessed 16 February 2021.

⁹⁴⁰ GDPR.

⁹⁴¹ *ibid.*

⁹⁴² UAVG (n 631), art 6.

⁹⁴³ *ibid.*

⁹⁴⁴ Het Nemo-Teneturbeginsel, decryptiebevel en de face ID (2019): <<http://arno.uvt.nl/show.cgi?fid=147999>> accessed 19 February 2021 15.

⁹⁴⁵ 'Ontslutplicht' (*Rijksoverheid.nl*, 2019):

<<https://www.rijksoverheid.nl/documenten/rapporten/2019/07/03/tk-bijlage-4-ontslutplicht>> accessed 19 February 2021.

surveillance sweep over entire neighborhoods or towns.⁹⁴⁶ While this law has been criticised extensively, the law remains in effect.⁹⁴⁷

Aside from specific laws, the Netherlands also has specific institutions tasked with the protection of human rights in relation to technology. The Dutch DPA monitors and protects the processing of data within the country.⁹⁴⁸ The *College voor de Rechten van de Mens*,⁹⁴⁹ the *Nationale Ombudsman*,⁹⁵⁰ and the *Autoriteit Persoonsgegevens* are all institutions that oversee human rights complaints that relate to advanced digital technologies (ADT).

As provided in the earlier chapters, the EU plays a significant role in the protection of human rights online. Regarding data protection law, the Treaty on the Functioning of the European Union (TFEU) lays out the right to protection of personal data in Article 16 (1).⁹⁵¹ On top of that, the GDPR has been thoroughly discussed as being one of the most influential pieces of legislation. The GDPR does not only safeguard the right to privacy, but also entails the right to be forgotten. It also requires a supervisory authority to be set up, in order to monitor the application of the GDPR. The application of the GDPR by means of such an authority seems quite effective, with the DPA receiving over 27,000 complaints in the year 2019 and handing out over €2.5 million in fines.⁹⁵²

While self-regulation is encouraged under the GDPR, the first code of conduct was only approved by the DPA in August 2020.⁹⁵³ So far, therefore, self-regulation has not been practiced much in the Netherlands on the basis of the GDPR. Regarding AI, it is clear that the EU is more concerned with ethical usage of ADTs than the Dutch legislation, which focuses more on the human aspect of AI.

However, the EU alone does not provide the Netherlands with data protection legislation. The European Convention on Human Rights (ECHR) also provides protection of personal data under Article 8 on respect for private and family life. The use of AI algorithms in the courtroom is also controversial under the ECHR particularly under Articles 5 and 6, which provide protection against arbitrary deprivation of one's liberty and the right to a fair trial respectively.

Current Dutch law covers a fair portion of human rights issues posed by ADT. Despite the legislation currently implemented, Dutch legislation could benefit from the strengthening of rights protection in light of regional and international standards. For example, while privacy is an issue discussed extensively in the Netherlands, there are some current laws that violate privacy, and therefore created controversy. The country may need to make adjustments to these laws in the future in order to protect the rights of citizens.

⁹⁴⁶ See articles 18 and 19 Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv).

⁹⁴⁷ Kiesraad, Nationaal referendum 21 maart 2018:

<<https://verkiezingsuitslagen.nl/verkiezingen/detail/NR20180321/667205>> accessed 16 February 2021.

⁹⁴⁸ Autoriteit Persoonsgegevens, 'Tasks and Powers of the Dutch DPA'

<<https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/tasks-and-powers-dutch-dpa>> accessed 8 March 2021.

⁹⁴⁹ 'Instellingen en taken van het College Voor de Rechten Van de Mens':

<<https://mensenrechten.nl/nl/digitalisering>>, accessed 29 January 2021.

⁹⁵⁰ Wet op de Nationale Ombudsman, 4 februari 1981, as amended on 1 January 2020 (WNO).

⁹⁵¹ TFEU, art. 16 (1).

⁹⁵² Autoriteit Persoonsgegevens, 'Feiten en cijfers over de AP'

<<https://autoriteitpersoonsgegevens.nl/nl/publicaties/feiten-en-cijfers-over-de-ap>> accessed 8 March 2021.

⁹⁵³ *ibid.*

10.3 Potential Future Law

As previously mentioned, the Netherlands has come to a standstill in enacting laws to ensure the protection of rights for citizens in relation to ADT. Recently, laws in the Netherlands have decreased rather than increased human rights protections in relation to technology. For example, the Act on the Intelligence and Security Services, despite being extremely controversial, has been enacted. This has been considered as a breach of privacy rights of Dutch citizens and illustrates that privacy rights are being stripped away rather than protected.

Furthermore, many of the recent laws in the Netherlands regarding technology have been controversial due to their clash with privacy rights. These laws have been enacted for the benefit of national security and criminal investigations. In the future, it is likely similar laws will be created. National security has become an issue globally, with many nations enacting laws as a preventative measure for terrorist activity. The Netherlands has already enacted a law relating to this and may become more strict as time passes. Similarly, the Dutch Code of Criminal Conduct may see a law amending it to include suspects in criminal investigations. Despite the decline in 2020, it is likely that similar issues will remerge in the near future.

However, the Netherlands has increased the protection of rights for citizens through European Union norms rather than through national legislation. The EU has suggested several new regulations for the internet and technology which, if enforced, the Netherlands would be obliged to follow.

The EU has a fairly comprehensive digital strategy, based on their Data Strategy and the February 2020 White Paper on Artificial Intelligence (AI).⁹⁵⁴ In the White Paper, the Commission explicitly acknowledges several risks AI poses for fundamental rights. The Commission also states that, while the GDPR and the ePrivacy Directive address these risks, 'there might be a need to examine whether AI systems pose additional risks'.⁹⁵⁵

One way in which the Commission is dealing with these additional risks is through proposing an ePrivacy Regulation.⁹⁵⁶ In short, this Regulation is meant to supplement the GDPR to ensure user data protection across the EU. While the ePrivacy Regulation has not yet been adopted, it is likely to be adopted in the next five years, as the need for regulation will only grow with the progress of technology. Additionally, in 2012 the Commission adopted a European Strategy for a Better Internet for Children, which aims to protect children from potentially harmful content delivered through the internet and safeguard children's privacy. It can be expected that more

⁹⁵⁴ European Commission, 'A European strategy for data'

<<https://ec-europa-eu.proxy-ub.rug.nl/digital-single-market/en/european-strategy-data>> accessed 8 March 2021.

⁹⁵⁵ European Commission, 'White paper on artificial intelligence- a European approach to excellence and trust', 19 Feb 2020.

<https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 8 March 2021.

⁹⁵⁶ European Commission, '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)' 10 Jan 2017

<<https://eur-lex-europa-eu.proxy-ub.rug.nl/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>> accessed 8 March 2021.

specific legislation to safeguard children's rights online will also be provided in the next five years.⁹⁵⁷

One other area in which much regulation is taking place is that of consumer protection for online trading of goods and services. Here, the EU has adopted Directive 2019/2161, which requires Member States to apply measures from May 2021. While not traditionally seen as human rights, it has been argued that consumer rights may develop as the next 'generation' of international human rights law.⁹⁵⁸

Conclusion

The Netherlands takes fair consideration in balancing human rights and the development of advanced digital technologies in the modern era. As a Member State of the European Union, the country uses a mixture of laws and regulations from the EU and national laws. Many human rights protections granted by the Netherlands can be found within the Dutch Constitution (*Grondwet voor het Koninkrijk der Nederlanden*), such as the right to privacy granted in Article 10, the freedom of expression in Article 7, and the right to non-discrimination granted in Article 1.⁹⁵⁹ These articles can be applied to rights online. Furthermore, the Netherlands also subscribes to the rights detailed within the European Convention on Human Rights (ECHR) which can also be applied to advancing technology and rights online. The Charter of Fundamental Rights of the European Union also provides rights followed by the Netherlands.

Human rights related specifically to technology can be found within several pieces of legislation. For example, the GDPR governs most of the technology rights in the Netherlands. The regulation replaced several national laws implemented by the Netherlands specifically for technology and rights online.⁹⁶⁰ The General Data Protection Implementation Act describes further rights in relation to technology within the country, and maintains rights from the Dutch Data Protection Act.⁹⁶¹ It also gives power to the Dutch DPA, which acts as a supervisory body to protect the processing of data within the country.⁹⁶² The rights prescribed by these pieces of legislation make up the basis of the rights in the Netherlands that relate to technology.

These pieces of legislation, however, are not the only parts acting to protect human rights related to technology in the Netherlands. The Netherlands also has several institutions responsible for overseeing human rights complaints in relation to advanced digital technologies. These are the

⁹⁵⁷ European Commission, 'Towards a European strategy on business-to-government data sharing for public interest' pp. 56 <https://ec-europa-eu.proxy-ub.rug.nl/newsroom/dae/document.cfm?doc_id=64954> accessed 8 March 2021.

⁹⁵⁸ Iris Benohr, 'EU consumer law and human rights' (2013) Oxford Scholarship Online <<https://oxford-universitypressscholarship-com.proxy-ub.rug.nl/view/10.1093/acprof:oso/9780199651979.001.0001/acprof-9780199651979-chapter-3>> accessed 8 March 2021.

⁹⁵⁹ Grondwet, 24 August 1815, as amended 21 December 2018 (Gw).

⁹⁶⁰ GDPR.

⁹⁶¹ UAVG (n 631) art 6.

⁹⁶² Autoriteit Persoonsgegevens, 'Tasks and Powers of the Dutch DPA' (*Autoriteit Persoonsgegevens*) <<https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/tasks-and-powers-dutch-dpa>> accessed 10 February 2021.

College voor de Rechten van de Mens,⁹⁶³ the *Nationale Ombudsman* ⁹⁶⁴, and the *Autoriteit Persoonsgegevens*.⁹⁶⁵ Together, these institutions ensure human rights in the Netherlands are being protected, and that laws related to human rights are not violated.

While the Netherlands clearly seeks to protect the technological human rights of its citizens through the legislation and institutions discussed above, there have been some controversies as of 2020, and some that may occur in the future that threaten rights in the digital era. The Dutch *grondwet*, while outlining human rights protections, remains outdated in its terminology.⁹⁶⁶ Protections are applied to ADT in an analogous manner, which may be problematic. The potential applicability of these articles to advancing forms of technology can therefore be called into question.

Another form of controversy comes from parts of the Dutch Criminal Code. The Netherlands allows for decryption of the encrypted messages of criminals through three laws that amended the Dutch Code of Criminal Procedure: the Computer Crime Act (*Wet computercriminaliteit*) of 1993, the Computer Crime II Act (*Wet computercriminaliteit II*) of 2006 and most recently the Computer Crime III Act (*Wet computercriminaliteit III*) of 2019.⁹⁶⁷ The most recent Act allows for the decryption of encrypted messages in criminal investigations, but was also initially proposed for suspects. While this proposal was declined,⁹⁶⁸ a similar law could be seen in the future that would target the encrypted messages of suspects.

Furthermore, the Act on the Intelligence and Security Services is a recent controversial law introduced in the Netherlands that allows for complete surveillance sweeps on neighborhoods or towns for national security.⁹⁶⁹ Such a law violates a right to privacy as described within Article 10 of the *Grondwet*. While objections have been made by Dutch students and human rights agencies,⁹⁷⁰ the law remains in effect.

Finally, while the Netherlands has Net Neutrality enforced by law since 2011,⁹⁷¹ censorship of some content on the internet has been proposed. Such websites include those with child pornography and websites hosting material that infringes on copyright. While the former proposal was withdrawn,⁹⁷² the latter proposal went into force in 2012. This proposal received

⁹⁶³ 'Instellingen en taken van het College Voor de Rechten Van de Mens' <<https://mensenrechten.nl/nl/digitalisering>>, accessed 29 January 2021.

⁹⁶⁴ Wet op de Nationale Ombudsman, as amended on 1 January 2020 (WNO) 4 februari 1981.

⁹⁶⁵ UAVG (n 631)

⁹⁶⁶ Bunschoten, *Tekst en Commentaar Grondwet* (Kluwer 2015), 6-11.

⁹⁶⁷ Het Nemo-Teneturbeginsel, Decryptiebevel en de Face ID <<http://arno.uvt.nl/show.cgi?fid=147999>> accessed 19 February 2021.

⁹⁶⁸ Rijksoverheid, 'Ontleutplicht'

<<https://www.rijksoverheid.nl/documenten/rapporten/2019/07/03/tk-bijlage-4-ontleutplicht>> accessed 19 February 2021.

⁹⁶⁹ Wet op de inlichtingen- en veiligheidsdiensten 2017 (WiV), arts 18 and 19.

⁹⁷⁰ Kiesraad, 'Nationaal referendum'

<<https://verkiezingsuitslagen.nl/verkiezingen/detail/NR20180321/667205>> accessed 16 February 2021.

⁹⁷¹ Kamerstuk (24095 nr 281, 2010/2011).

⁹⁷² Joost Schellevis, 'Politiek zegt 'nee' tegen internetfilter'

<<https://tweakers.net/nieuws/74508/politiek-zegt-nee-tegen-internetfilter.html>> accessed 19 February 2021.

major controversy, but as of 2017, all internet providers must block the Pirate Bay, a known host of copyrighted material.⁹⁷³

The Netherlands has previously made great strides to protecting human rights online, but has slowed in its progression towards realizing human rights in relation to technology. More recently, proposals have been made that violate rights prescribed in the *Grondwet* for national security, and in the future, more laws like the ones previously mentioned could appear. While outcry has been made by citizens against these pieces of legislation, they still remain in effect.

It should be said that, while this research has overwhelmingly focused on the risks ADTs pose to human rights, they can also be valuable in safeguarding them. For older persons, robotics, AI and other assistive technologies can help fulfil their rights to autonomy, non-discrimination and safety.⁹⁷⁴ With the help of satellite imagery, ADTs can also help identify and monitor serious human rights violations and facilitate grassroots mobilisation.⁹⁷⁵

⁹⁷³ Joost Schellevis, 'Ook andere providers moeten The Pirate Bay blokkeren' <<https://tweakers.net/nieuws/81883/ook-andere-providers-moeten-the-pirate-bay-blokkeren.html>> accessed 19 February 2021.

⁹⁷⁴ Rosa Kornfeld-Matte, 'Report of the Independent Expert on the Enjoyment of All Human Rights by Older Persons on her mission to Georgia' <<https://digitallibrary.un.org/record/1638448>> accessed 19 February 2021. <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/219/52/PDF/G1721952.pdf?OpenElement>> accessed 19 February 2021.

⁹⁷⁵ UHCHR 'More satellite images assist human rights work'. <<https://www.ohchr.org/EN/NewsEvents/Pages/MoresatelliteimagestoassistHRwork.aspx>> accessed 19 February 2021.

Table of legislation

Provision in Dutch language	Corresponding translation in English
De Nederlandse Grondwet, Artikel 1: Allen die zich in Nederland bevinden, worden in gelijke gevallen gelijk behandeld. Discriminatie wegens godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht of op welke grond dan ook, is niet toegestaan.	The Constitution of the Netherlands, Article 1: All persons in the Netherlands shall be treated equally in equal circumstances. Discrimination on the grounds of religion, belief, political opinion, race or sex or any other grounds whatsoever shall not be permitted.
De Nederlandse Grondwet, Artikel 7: 1. Niemand heeft voorafgaand verlof nodig om door de drukpers gedachten of gevoelens te openbaren, behoudens ieders verantwoordelijkheid volgens de wet. 2. De wet stelt regels op omtrent radio en televisie. Er is geen voorafgaand toezicht op de inhoud van een radio- of televisieuitzending. 3. Voor het openbaren van gedachten of gevoelens door andere dan in de voorgaande leden genoemde middelen heeft niemand voorafgaand verlof nodig wegens de inhoud daarvan, behoudens ieders verantwoordelijkheid volgens de wet. De wet kan het geven van vertoningen toegankelijk voor personen jonger dan zestien jaar regelen ter bescherming van de goede zeden. 4. De voorgaande leden zijn niet van toepassing op het maken van handelsreclame	The Constitution of the Netherlands, Article 7: 1. No one shall require prior permission to publish thoughts or opinions through the press, without prejudice to the responsibility of every person under the law. 2. Rules concerning radio and television shall be laid down by Act of Parliament. There shall be no prior supervision of the content of a radio or television broadcast. 3. No one shall be required to submit thoughts or opinions for prior approval in order to disseminate them by means other than those mentioned in the preceding paragraphs, without prejudice to the responsibility of every person under the law. The holding of performances open to persons younger than sixteen years of age may be regulated by Act of Parliament in order to protect good morals. 4. The preceding paragraphs do not apply to commercial advertising
De Nederlandse Grondwet, Artikel 10: 1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.	The Constitution of the Netherlands, Article 10: 1. Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of

2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. 3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.	Parliament. 2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data. 3. Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament.
De Nederlandse Grondwet, Artikel 13: 1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter. 2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.	The Constitution of the Netherlands, Article 13: 1. The secret of correspondence is inviolable, except, in the cases laid down by the law, by order of the court. 2. The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament.
De Nederlandse Grondwet, Artikel 93: Bepalingen van verdragen en van besluiten van volkenrechtelijke organisaties, die naar haar inhoud een ieder kunnen verbinden, hebben verbindende kracht nadat zij zijn bekendgemaakt.	The Constitution of the Netherlands, Article 93: Provisions and treaties and of resolutions by international institutions which may be binding on all persons by virtue their contents shall become binding after they have been published.
De Nederlandse Grondwet, Artikel 94: Binnen het Koninkrijk geldende wettelijke voorschriften vinden geen toepassing, indien deze toepassing niet verenigbaar is met een ieder verbindende bepalingen van verdragen en van besluiten van volkenrechtelijke organisaties.	The Constitution of the Netherlands, Article 94: Statutory regulations in force within the Kingdom shall not be applicable if such application is in conflict with provisions of treaties that are binding on all persons or of resolutions by international institutions.
De Nederlandse Grondwet, Artikel 120:	The Constitution of the Netherlands, Article 120:

De rechter treedt niet in de beoordeling van de grondwettigheid van wetten en verdragen.	The constitutionality of Acts of Parliament and treaties shall not be reviewed by the courts.
De Nederlandse Grondwet, Artikel 137: 1. De wet verklaart, dat een verandering in de Grondwet, zoals zij die voorstelt, in overweging zal worden genomen 2. De Tweede Kamer kan, al dan niet op een daartoe door of vanwege de Koning ingediend voorstel, een voorstel voor zodanige wet splitsen. 3. Na de bekendmaking van de wet, bedoeld in het eerste lid wordt de Tweede Kamer ontbonden. 4. Nadat de nieuwe Tweede Kamer is samengekomen, overwegen beide kamers in tweede lezing het voorstel tot verandering, bedoeld in het eerste lid. Zij kunnen dit alleen aannemen met ten minste twee derden van het aantal uitgebrachte stemmen. 5. De Tweede Kamer kan, al dan niet op een daartoe door of vanwege de Koning ingediend voorstel, met ten minste twee derden van het aantal uitgebrachte stemmen een voorstel tot verandering splitsen.	The Constitution of the Netherlands, Article 137: 1. An Act of Parliament shall be passed stating that an amendment to the Constitution in the form proposed shall be considered. 2. The Lower House may divide a Bill presented for this purpose to the King or otherwise. 3. The Lower House shall be dissolved after the Bill referred to in the first paragraph has been published. 4. After the new Lower House has assembled, the two Houses of the States General shall consider, at second reading, the Bill referred to in the first paragraph. The Bill shall be passed only if at least two thirds of the votes cast are in favour. 5. The Lower House may divide a Bill for the amendment of the Constitution into a number of separate Bills, either upon a proposal presented by or on behalf of the king or otherwise, if at least two-thirds of the votes cast are in favour.
Wetboek van Strafvordering, Artikel 125i: Aan de rechter-commissaris, de officier van justitie, de hulpofficier van justitie en de opsporingsambtenaar komt onder dezelfde voorwaarden als bedoeld in de artikelen 96b, 96c, eerste, tweede en derde lid, 97, eerste tot en met vierde lid, en 110, eerste en tweede lid, de bevoegdheid toe tot het doorzoeken van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd. In het belang van het onderzoek	Dutch Code of Criminal Procedure, Article 125i: The power to search a place for the purpose of recoding data stored or recorded in a data carrier at this place shall be conferred on the examining magistrate, the public prosecutor, the assistant public prosecutor and the investigating officer under the same conditions as referred to in sections 96b, 96c(1), (2) and (3), 97 (1) to (4) inclusive, and 110 (1) and (2). They may record this data in

kunnen zij deze gegevens vastleggen. De artikelen 96, tweede lid, 98, 99 en 99a zijn van overeenkomstige toepassing.	the interest of the investigation. Sections 96(2), 98, 99 and 99a shall apply mutatis mutandis.
Wetboek van Strafvordering, Artikel 125j: 1. In geval van een doorzoeking kan vanaf de plaats waar de doorzoeking plaatsvindt, in een elders aanwezig geautomatiseerd werk onderzoek worden gedaan naar in dat werk opgeslagen gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen. Worden dergelijke gegevens aangetroffen, dan kunnen zij worden vastgelegd. 2. Het onderzoek reikt niet verder dan voor zover de personen die plegen te werken of te verblijven op de plaats waar de doorzoeking plaatsvindt, vanaf die plaats, met toestemming van de rechthebbende tot het geautomatiseerde werk, daartoe toegang hebben.	Dutch Code of Criminal Procedure, Article 125j: 1. In the case of a search, a computerised device or system located elsewhere may be searched for data stored in that device or system that is reasonably required in order to reveal the truth from the place where the search takes place. If such data is found, then it may be recorded. 2. The search shall be limited to the extent that the persons, who normally work or reside at the place where the search is being conducted, have access thereto from that place with the consent of the person entitled to use the computerised device or system.
Wetboek van Strafvordering, Artikel 125k: 1. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan indien toepassing is gegeven aan artikel 125i of artikel 125j tot degen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging van een geautomatiseerd werk, het bevel worden gericht toegang te verschaffen tot de aanwezige geautomatiseerde werken of delen daarvan. Degeen tot wie het bevel is gericht, dient desgevraagd hieraan gevolg te geven door de kennis omtrent de beveiliging ter beschikking te stellen. 2. Het eerste lid is van overeenkomstige toepassing indien in een geautomatiseerd werk versleutelde gegevens worden aangetroffen. Het bevel richt zich tot degen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van deze gegevens.	Dutch Code of Criminal Procedure, Article 125k: 1. Insofar as is specifically required in the interest of the investigation, the person who may be reasonably believed to have knowledge of the security system of a computerised device or system may be ordered, if section 125i or section 125j is applied, to provide access to the computerised devices or systems present or parts thereof. The person who is ordered to do so must comply with this order, if requested, by providing the knowledge about the security system. 2. Subsection (1) shall apply mutatis mutandis if encrypted data is found in a computerised device or system. The order shall be directed to the person who may be reasonably believed to have knowledge of the manner of encryption of this data.

3. Het bevel, bedoeld in het eerste lid, wordt niet gegeven aan de verdachte. Artikel 96a, derde lid, is van overeenkomstige toepassing.	3. The order, referred to in subsection (1), shall not be given to the suspect. Section 96a(3) shall apply mutatis mutandis.
Wetboek van Strafvordering, Artikel 126i(1): 1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, kan de officier van justitie in het belang van het onderzoek bevelen dat een opsporingsambtenaar: a. goederen afneemt van de verdachte, b. gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van een geautomatiseerd werk, door tussenkomst van een openbaar telecommunicatienetwerk afneemt van de verdachte, of c. diensten verleent aan de verdachte.	Dutch Code of Criminal Procedure, Article 126i(1) 1. In the case of suspicion of a serious offence as defined in section 67(1) the public prosecutor may, in the interest of the investigation, order an investigating officer to: a. purchase goods from the suspect, b. purchase data which is stored, processed or transferred through a public telecommunication network by means of a computerised device or system from the suspect, or c. provide services to the suspect.
Wetboek van Strafvordering, Artikel 126m: 1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, aan een opsporingsambtenaar bevelen dat met een technisch hulpmiddel niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst, wordt opgenomen. 2. Het bevel is schriftelijk en vermeldt: a. het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte; b. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;	Dutch Code of Criminal Procedure, Article 126m: 1. In the case of suspicion of a serious offence as defined in section 67(1), which serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order, the public prosecutor may, if urgently required by the investigation, order an investigating officer to record by means of a technical device non-public communications which are conducted by use of the services of a provider of a communication service. 2. The warrant shall be in writing and shall state: a. the serious offence and if known, the name or otherwise the most precise description possible of the suspect; b. the facts or circumstances which show that the conditions, referred to in

c. het nummer of een andere aanduiding waarmee de individuele gebruiker van de communicatiedienst wordt geïdentificeerd of de naam en, voor zover bekend, het adres van de gebruiker; d. de geldigheidsduur van het bevel; e. een aanduiding van de aard van het technisch hulpmiddel of de technische hulpmiddelen waarmee de communicatie wordt opgenomen. 3. Indien het bevel betrekking heeft op communicatie die plaatsvindt via een openbaar telecommunicatienetwerk of met gebruikmaking van een openbare telecommunicatiedienst in de zin van de Telecommunicatiewet, wordt – tenzij zulks niet mogelijk is of het belang van strafvordering zich daartegen verzet – het bevel ten uitvoer gelegd met medewerking van de aanbieder van het openbare telecommunicatienetwerk of de openbare telecommunicatiedienst en gaat het bevel vergezeld van de vordering van de officier van justitie aan de aanbieder om medewerking te verlenen. 4. Indien het bevel betrekking heeft op andere communicatie dan bedoeld in het derde lid, wordt – tenzij zulks niet mogelijk is of het belang van strafvordering zich daartegen verzet – de aanbieder in de gelegenheid gesteld medewerking te verlenen bij de tenuitvoerlegging van het bevel. 5. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. De rechter-commissaris kan, op vordering van de officier van justitie, in zijn machtiging bepalen dat deze geldt voor alle nummers of	subsection (1), have been met; c. where possible, the number or another indication by means of which the individual user of the communication service is identified as well as, insofar as is known, the name and the address of the user; d. the term of validity of the warrant; e. a description of the nature of the technical device or the technical devices by means of which the communications are recorded. 3. If the warrant relates to communications which are conducted through a public telecommunication network or by use of a public telecommunication service within the meaning of the Telecommunications Act, the warrant shall – unless such is impossible or is not permitted in the interest of the criminal proceedings – be executed with the assistance of the provider of the public 55 telecommunication network or the public telecommunication service and the warrant shall be accompanied by the request for assistance from the public prosecutor to the provider. 4. If the warrant relates to communications other than the communications referred to in subsection (3), the provider shall – unless such is impossible or is not permitted in the interest of the criminal proceedings – be given the opportunity to assist in the execution of the warrant. 5. The warrant, referred to in subsection (1), may only be issued following written authorisation to be granted by the examining magistrate on application of the public prosecutor. Section 126l(5) to (8) inclusive shall apply mutatis mutandis.

andere aanduidingen als bedoeld in het tweede lid, onder c, die gedurende de geldigheidsduur van de machtiging bij de gebruiker in gebruik zijn. Artikel 126l, vijfde tot en met achtste lid, is van overeenkomstige toepassing. 6. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan indien toepassing is gegeven aan het eerste lid tot degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de communicatie, de vordering worden gericht medewerking te verlenen aan het ontsleutelen van de gegevens door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken. 7. De in het zesde lid bedoelde vordering wordt niet gericht tot de verdachte. 8. Op de in het zesde lid bedoelde vordering zijn artikel 96a, derde lid, en artikel 126l, vierde, zesde en zevende lid, van overeenkomstige toepassing. 9. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de wijze waarop het in het eerste lid bedoelde bevel en de in het derde en zesde lid bedoelde vorderingen kunnen worden gegeven en over de wijze waarop daaraan wordt voldaan.	6. Insofar as is specifically required in the interest of the investigation, the person, who may be reasonably presumed to have knowledge of the manner of encryption of the communications, may be requested, if subsection (1) is applied, to assist in decrypting the data by either providing this knowledge, or undoing the encryption. 7. The request referred to in subsection (6) shall not be directed to the suspect. 8. Section 96a(3) and section 126l(4), (6) and (7) shall apply mutatis mutandis to the request referred to in subsection (6). 9. Rules pertaining to the manner in which the order referred to in subsection (1) and the requests referred to in subsections (3) and (6) may be given and the manner of compliance with such requests shall be set by Governmental Decree.
Wetboek van Strafvordering, Artikel 126nh: 1. De officier van justitie kan, indien het belang van het onderzoek dit vordert, bij of terstond na de toepassing van artikel 126nd, eerste lid, 126ne, eerste of derde lid, of 126nf, eerste lid, degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de in deze artikelen bedoelde gegevens, bevelen medewerking te verlenen aan het ontsleutelen van de gegevens door de versleuteling ongedaan te maken, dan wel deze	Dutch Code of Criminal Procedure, Article 126nh: 1. The public prosecutor may, if required in the interest of the investigation, in or immediately after the application of section 126nd(1), 126ne(1) or (3), or 126nf(1), order the person who may be reasonably presumed to have knowledge of the manner of encryption of the data referred to in these sections to assist in decrypting the data by either undoing the encryption, or providing

kennis ter beschikking te stellen. 2. Het bevel wordt niet gegeven aan de verdachte. Artikel 96a, derde lid, is van overeenkomstige toepassing.	this knowledge. 2. The order shall not be given to the suspect. Section 96a(3) shall apply mutatis mutandis
Wetboek van Strafvordering, Artikel 126uh: 1. De officier van justitie kan, indien het belang van het onderzoek dit vordert, bij of terstond na de toepassing van artikel 126ud, eerste lid, 126ue, eerste of derde lid, of 126uf, eerste lid, degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de in deze artikelen bedoelde gegevens, bevelen medewerking te verlenen aan het ontsleutelen van de gegevens door de versleuteling ongedaan te maken, dan wel deze kennis ter beschikking te stellen. 2. Het bevel wordt niet gegeven aan de verdachte. Artikel 96a, derde lid, is van overeenkomstige toepassing.	Dutch Code of Criminal Procedure, Article 126uh: 1. The public prosecutor may, if urgently required in the interest of the investigation, in or immediately after the application of section 126ud(1), 126ue(1) or (3), or 126uf(1), order the person who may be reasonably presumed to have knowledge of the manner of encryption of the data referred to in these sections to assist in decrypting the data by either undoing the encryption, or providing this knowledge. 2. The order shall not be given to the suspect. Section 96a(3) shall apply mutatis mutandis
Wetboek van Strafvordering, Artikel 126zp: 1. De officier van justitie kan, indien het belang van het onderzoek dit vordert, bij of terstond na de toepassing van artikel 126zl, eerste lid, 126zm, eerste of derde lid, of 126zn, eerste lid, degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de in deze artikelen bedoelde gegevens, bevelen medewerking te verlenen aan het ontsleutelen van de gegevens door de versleuteling ongedaan te maken, dan wel deze kennis ter beschikking te stellen. 2. Artikel 126nh, tweede lid, is van overeenkomstige toepassing.	Dutch Code of Criminal Procedure, Article 126zp: 1. The public prosecutor may, if required in the interest of the investigation, in or immediately after the application of section 126zl(1), 126zm(1) or (3), or 126zn(1), order the person who may be reasonably presumed to have knowledge of the manner of encryption of the data referred to in 75 these sections to assist in decrypting the data by either undoing the encryption, or providing this knowledge. 2. Section 126nh(2) shall apply mutatis mutandis.
Wetboek van Strafvordering, Artikel 552a(1): 1. De belanghebbenden kunnen zich schriftelijk beklagen over inbeslagneming, over het gebruik van in beslag genomen voorwerpen, over het	Dutch Code of Criminal Procedure, Article 552a(1): The interested parties may file a written complaint about the seizure, about the use of

uitblijven van een last tot teruggave, over het al dan niet toepassen van de in artikel 116, vierde lid, neergelegde bevoegdheid, over de vordering van gegevens, over het bevel toegang te verschaffen tot een geautomatiseerd werk of delen daarvan, tot een gegevensdrager of tot versleutelde gegevens dan wel kennis omtrent de beveiliging daarvan ter beschikking te stellen, over de kennisneming of het gebruik van gegevens, vastgelegd tijdens een doorzoeking of op vordering verstrekt, over de kennisneming of het gebruik van gegevens, opgeslagen, verwerkt of overgedragen door middel van een geautomatiseerd werk en vastgelegd bij een onderzoek in zodanig werk, over de kennisneming of het gebruik van gegevens als bedoeld in de artikelen 100, 101 en 114, over de vordering gegevens te bewaren en beschikbaar te houden, alsmede over de ontoegankelijkmaking van gegevens, aangetroffen in een geautomatiseerd werk, bedoeld in de artikelen 125o en 126cc, vijfde lid, de opheffing van de desbetreffende maatregelen of het uitblijven van een last tot zodanige opheffing. 2. De belanghebbenden kunnen zich voorts schriftelijk beklagen over een bevel tot het ontoegankelijk maken van gegevens, bedoeld in artikel 125p. Over het beklag, bedoeld in de vorige volzin, beslist het gerecht zo spoedig mogelijk.	the objects seized, about the failure to issue an order to return the objects, about the request of data, about the request to assist in the decryption of data, about the inspection or the use of data, recorded during a search or provided on request, about the inspection or the use of data, stored, processed or transferred by means of a computerised device or system and recorded during a search in such device or system, about the inspection or the use of data as referred to in sections 100, 101 and 114, about the request to store and keep data available, and about the disablement of data, found in a computerised device or system as referred to in section 125o, the revocation of the measures concerned or the failure to issue such revocation order.
Wetboek van Strafvordering, Artikel 552d: 1. Een beschikking ingevolge artikel 552a, 552ab of 552b wordt onverwijld aan de klager betekend. 2. Beroep in cassatie kan door het openbaar ministerie worden ingesteld binnen veertien dagen na de dagtekening der beschikking, en door de klager binnen veertien dagen na de	Dutch Code of Criminal Conduct, Article 552d: 1. A decision pursuant to article 552a, 552ab or 552b will be served on the complainant without delay. 2. An appeal in cassation can be lodged by the Public Prosecution Service within fourteen days after the date of the decision, and by the

betekening. 3. Indien het klaagschrift is ingediend door een persoon met de bevoegdheid tot verschoning als bedoeld in artikel 218 beslist de Hoge Raad binnen negentig dagen na indiening van de schriftuur. Artikel 447 is van overeenkomstige toepassing, met dien verstande dat de termijn voor indiening van middelen van cassatie veertien dagen bedraagt. 4. Indien het beklag ingevolge artikel 552a betrekking heeft op de uitvoering van een verzoek om rechtshulp van een vreemde staat, beslist de Hoge Raad binnen negentig dagen na indiening van de schriftuur. Artikel 447 is van overeenkomstige toepassing, met dien verstande dat de termijn voor indiening van middelen van cassatie veertien dagen bedraagt.	complainant within fourteen days after notification. 3. If the notice of complaint has been submitted by a person with the authority to excuse the complaint as referred to in Article 218, the Supreme Court will make a decision within ninety days of the submission of the written notice. Article 447 shall apply mutatis mutandis, on the understanding that the term for submitting appeals for cassation is fourteen days. 4. If the complaint pursuant to Article 552a relates to the execution of a request for legal assistance from a foreign state, the Supreme Court will decide within ninety days after the submission of the document. Article 447 shall apply mutatis mutandis, on the understanding that the term for submitting appeals for cassation is fourteen days
Wetboek van Strafvordering, Artikel 5.1.4.: 1. Tenzij Onze Minister van Veiligheid en Justitie aanstonds van oordeel is dat het verzoek om rechtshulp van een vreemde staat niet kan worden ingewilligd, stelt hij het verzoek en de daarbij behorende stukken in handen van de officier van justitie. 2. Voor zover het verzoek om rechtshulp van een vreemde staat is gegrond op een verdrag wordt daaraan zoveel mogelijk het verlangde gevolg gegeven. 3. In gevallen waarin het betreft een verzoek dat niet op een verdrag is gegrond, alsmede in gevallen waarin het toepasselijke verdrag niet tot inwilliging verplicht, kan een verzoek om rechtshulp van een bevoegde autoriteit van een vreemde staat worden ingewilligd indien de inwilliging niet in strijd is met een wettelijk voorschrift of dient te worden geweigerd in het	Criminal procedural code, Article 5.1.4 1. Unless Our Minister of Security and Justice is immediately of the opinion that the request for legal assistance from a foreign state cannot be granted, he will submit the request and the accompanying documents to the public prosecutor. 2. Insofar as the request for legal assistance from a foreign state is based on a treaty, it shall be given effect as far as possible. 3. In cases involving a request not based on a treaty, including in cases where the applicable treaty does not require compliance, a request for legal assistance from a competent authority from a foreign state can be granted, provided that the request does not contest with a legal requirement or has to be denied in the context of the common good. 4. When a treaty provides for the transmission of requests to judicial

kader van het algemeen belang. 4. Wanneer een verdrag voorziet in rechtstreekse toezending van verzoeken aan justitiële autoriteiten, is de officier van justitie in het arrondissement waarin de in het verzoek gevraagde handeling moet worden verricht, dan wel een officier van justitie bij het landelijk parket of bij het functioneel parket, zelfstandig bevoegd tot inwilliging van het verzoek, tenzij de inwilliging op grond van artikel 5.1.5 een beslissing van Onze Minister van Veiligheid en Justitie verlangt. Indien het verzoek niet tot die officier van justitie is gericht, wordt het door de geadresseerde onverwijld aan hem doorgezonden. 5. Indien het verzoek niet kan worden ingewilligd, worden de autoriteiten van de verzoekende staat daarvan zo spoedig mogelijk op de hoogte gesteld. In geval het verzoek niet kan worden ingewilligd omdat het onvolledig is, wordt de autoriteiten van de verzoekende staat eerst in de gelegenheid gesteld om het verzoek aan te vullen.	authorities, the public prosecutor in the district in which the action requested in the request must be carried out, or a public prosecutor at the national court requests as such, unless the granting requires a decision by the Minister of Security and Justice on the basis of Article 5.1.5. If the request is not addressed to that public prosecutor, it will be forwarded to him by the addressee without delay. 5. If the request cannot be granted, the authorities of the requesting State shall be informed as soon as possible. In case the request cannot be granted because it is incomplete, the authority of the requesting State shall first be given the opportunity to complete the request.
Wet op de inlichtingen- en veiligheidsdiensten 2017, Artikel 18: 1. De verwerking van gegevens vindt slechts plaats voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van deze wet of de Wet veiligheidsonderzoeken. 2. De verwerking van gegevens geschiedt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze. 3. De gegevens die in het kader van de taakuitvoering van de diensten worden verwerkt, zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron	The Intelligence and Security Services Act 2017, article 18 1. Data processing only takes place for a specific purpose and only insofar as this is necessary for the proper implementation of this Act or the Security Investigations Act. 2. Data is processed in accordance with the law and in a correct and careful manner. 3. Data that is processed in the context of the performance of the services shall be provided with an indication of the degree of reliability or a reference to the document and the source from which the data were derived.

waaraan de gegevens zijn ontleend.	
Wet op de inlichtingen- en veiligheidsdiensten 2017, Artikel 19: 1. De verwerking van persoonsgegevens door de Algemene Inlichtingen- en Veiligheidsdienst kan slechts betrekking hebben op personen: a. die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat; b. die toestemming hebben verleend voor een veiligheidsonderzoek; c. omtrent wie dat noodzakelijk is in het kader van het onderzoek betreffende andere landen; d. over wie door een andere inlichtingen- of veiligheidsdienst gegevens zijn ingewonnen; e. wier gegevens noodzakelijk zijn ter ondersteuning van een goede taakuitvoering door de dienst; f. die werkzaam zijn of zijn geweest voor een dienst; g. omtrent wie dat noodzakelijk is in het kader van het opstellen van de dreigings- en risicoanalyses, bedoeld in artikel 8, tweede lid, onderdeel e; h. omtrent wie dat noodzakelijk is in het kader van het doen van een mededeling als bedoeld in artikel 8, tweede lid, onderdeel f. 2. De verwerking van persoonsgegevens door de Militaire Inlichtingen- en Veiligheidsdienst kan slechts betrekking hebben op personen: a. die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen	The Intelligence and Security Services Act 2017, article 19 1. The processing of personal data by the General Intelligence and Security Service can only concern persons: a. which give rise to the serious suspicion that they pose a danger to the democratic legal order, or to the security or other important interests of the state; b. who have authorised a security investigation; c. about whom this is necessary in the context of the investigation concerning other countries; d. about whom information has been obtained by another intelligence or security service; e. whose data is necessary to support the proper performance of tasks by the service; f. who are or have worked for a service; g. about whom this is necessary in the context of drawing up the threat and risk analysis referred to in Article 8, second paragraph, under e; h. about whom this is necessary in the context of making a notification as referred to in Article 8, second paragraph, under f. 2. The processing of personal data by the Military Intelligence and Security Service can only concern persons: a. which give rise to a serious suspicion that they pose a threat to the security or readiness of the armed forces;

voor de veiligheid of de paraatheid van de krijgsmacht; b. die toestemming hebben verleend voor een veiligheidsonderzoek; c. omtrent wie dat noodzakelijk is in het kader van het onderzoek betreffende andere landen; d. over wie door een andere inlichtingen- of veiligheidsdienst gegevens zijn ingewonnen; e. wier gegevens noodzakelijk zijn ter ondersteuning van een goede taakuitvoering door de dienst; f. die werkzaam zijn of zijn geweest voor een dienst; g. omtrent wie dat noodzakelijk is in het kader van een onderzoek als bedoeld in artikel 10, tweede lid, onderdeel a, sub 2°; h. omtrent wie dat noodzakelijk is in het kader van het opstellen van de dreigingsanalyses, bedoeld in artikel 10, tweede lid, onderdeel f; i. omtrent wie dat noodzakelijk is in het kader van het opstellen van een analyse door de Militaire Inlichtingen- en Veiligheidsdienst, in opdracht van onze minister van Defensie, van potentiële dreigingen tegen een bij de krijgsmacht werkzaam persoon of een bij de krijgsmacht in gebruik zijnd object, welke niet ingevolge de artikelen 4, derde lid, onderdeel b, en 42, eerste lid, onderdeel c, onderscheidenlijk artikel 16 van de Politiewet 2012 is aangewezen; j. omtrent wie dat noodzakelijk is in het kader van het doen van een mededeling als bedoeld in artikel 10, tweede lid, onderdeel g.	b. who have authorised a security investigation; c. about whom this is necessary in the context of the investigation concerning other countries; d. about whom information has been obtained by another intelligence or security service; e. whose data is necessary to support the proper performance of tasks by the service; f. who are or have worked for a service; g. about whom this is necessary in the context of an investigation as referred to in Article 10, second paragraph, under a, under 2 °; h. about whom this is necessary in the context of the preparation of the threat analysis referred to in Article 10, second paragraph, under f; i. regarding whom this is necessary in the context of drawing up an analysis by the Military Intelligence and Security Service, on behalf of our Minister of Defense, of potential threats against a person employed by the armed forces or an object in use by the armed forces, which has not been designated pursuant to Articles 4, third paragraph, under b, and 42, first paragraph, under c, or Article 16 of the Police Act 2012 respectively; j. about whom this is necessary in the context of making a notification as referred to in Article 10, second paragraph, under g. 3. The processing of personal data on grounds of a person's religion or belief, race,

3. De verwerking van persoonsgegevens wegens iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven vindt niet plaats. 4. De verwerking van persoonsgegevens die betrekking hebben op de in het derde lid bedoelde kenmerken vindt slechts plaats in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is. 5. Onverminderd de verwerking van persoonsgegevens als bedoeld in het eerste en tweede lid, zijn de diensten bevoegd tot verwerking van gegevens omtrent andere personen, indien die gegevens een logisch en onlosmakelijk onderdeel vormen van de door de diensten te verwerven of verworven gegevensbestanden.	trade union membership, health and sexual life does not take place. 4. The processing of personal data relating to the characteristics referred to in the third paragraph only takes place in addition to the processing of other data and only insofar as this is unavoidable for the purpose of the data processing. 5. Without prejudice to the processing of personal data as referred to in the first and second paragraph, the services are authorised to process data concerning other persons, if those data form a logical and inseparable part of the data files to be acquired or acquired by the services.
Wet op de inlichtingen- en veiligheidsdiensten 2017, Artikel 25: 1. De diensten zijn, met inachtneming van het bepaalde bij of krachtens deze wet, in ieder geval bevoegd tot het verzamelen van gegevens: a. uit voor een ieder toegankelijke informatiebronnen; b. uit informatiebronnen waarvoor aan de dienst een recht op kennisneming van de aldaar berustende gegevens is verleend; c. via raadpleging van informanten als bedoeld in artikel 39; d. met uitoefening van bijzondere bevoegdheden als bedoeld in paragraaf 3.2.5; e. in het kader van de samenwerking tussen inlichtingen- en	The Intelligence and Security Services Act 2017, Article 25: 1. With due observance of the provisions of or pursuant to this Act, the services are in any case authorised to collect data: a. from information sources accessible to everyone; b. from information sources for which the service has been granted a right to access the data contained therein; c. through consultation of informants as referred to in Article 39; d. exercising special powers as referred to in section 3.2.5; e. in the context of cooperation between intelligence and security services and with other authorities.

veiligheidsdiensten en met andere instanties. 2. Onze betrokken Minister kan, indien de onder hem ressorterende dienst het noodzakelijk acht gegevens te verzamelen uit een andere informatiebron als bedoeld in het eerste lid, op een daartoe strekkend verzoek van het hoofd van de dienst daarvoor toestemming verlenen. In het verzoek wordt met redenen omkleed aangegeven waarom van de desbetreffende informatiebron gebruik dient te worden gemaakt.	2. The relevant Minister may, if the service under him deems it necessary to collect data from another information source as referred to in the first paragraph, upon a request from the head of the service, grant permission to do so. The request shall state the reasons why the relevant source of information should be used.
Wet op de inlichtingen- en veiligheidsdiensten 2017, Artikel 32: 1. Er is een toetsingscommissie inzet bevoegdheden. 2. De toetsingscommissie is belast met het toetsen van de rechtmatigheid van de door Onze betrokken Minister verleende toestemming als bedoeld in de artikelen 40, derde lid, 42, vierde lid, 43, tweede en vierde lid, 45, derde, vijfde en tiende lid, 47, tweede lid, 48, tweede lid, 49, vierde lid, 50, tweede en vierde lid, 53, tweede lid, 54, tweede lid en 57, tweede lid. Het oordeel van de toetsingscommissie is bindend.	The Intelligence and security Services Act 2017, Article 32: 1. There is an assessment committee for the use of powers. 2. The review committee is charged with reviewing the lawfulness of the permission granted by the relevant Minister as referred to in Articles 40, third paragraph , 42, fourth paragraph , 43, second and fourth paragraph , 45, third, fifth and tenth paragraphs , 47 , second paragraph , 48, second paragraph , 49, fourth paragraph , 50, second and fourth paragraph , 53, second paragraph , 54, second paragraph and 57, second paragraph . The assessment committee's judgment is binding.
Wet op de inlichtingen- en veiligheidsdiensten 2017, Artikel 33: 1. De toetsingscommissie bestaat uit drie leden, waaronder de voorzitter. De leden worden benoemd bij koninklijk besluit op voordracht van Onze betrokken Ministers gezamenlijk voor een tijdvak van zes jaar en kunnen eenmaal worden herbenoemd. 2. Ten minste twee van de drie leden, waaronder de voorzitter, dienen ten minste zes jaar de functie van rechterlijk ambtenaar met	The Intelligence and Security Services Act 2017, Article 33: 1. The assessment committee consists of three members, including the chair. The members are appointed by Royal Decree on the nomination of the relevant Ministers jointly for a term of six years and can be reappointed once. 2. At least two of the three members, including the chairman, must have fulfilled the position of judicial officer charged with the

rechtspraak belast, bedoeld in artikel 1, onderdeel c, van de Wet op de rechterlijke organisatie, te hebben vervuld, dan wel ten minste zes jaar als lid van de Afdeling bestuursrechtspraak van de Raad van State, als lid belast met rechtspraak bij het College van Beroep voor het bedrijfsleven of als lid belast met rechtspraak bij de Centrale Raad van Beroep werkzaam te zijn geweest. 3. De leden van de toetsingscommissie kunnen niet tevens lid zijn van de commissie van toezicht of van de afdeling klachtbehandeling van de commissie van toezicht. 4. De artikelen 99, eerste, tweede, vijfde, zesde, achtste en negende lid, 100, 101 en 102 zijn van overeenkomstige toepassing.	administration of justice, as referred to in Article 1 (c) of the Judicial Organization Act , for at least six years , or at least six years as a member of the Administrative Jurisdiction Division of the Council of State, as a member charged with jurisdiction at the Trade and Industry Appeals Tribunal or as a member charged with jurisdiction at the Central Board of Appeal. 3. The members of the review committee cannot also be a member of the supervisory committee or of the complaints handling department of the supervisory committee. 4. The articles 99, first, second, fifth, sixth, eighth and ninth members , 100 , 101 and 102 are mutatis mutandis.
Wet op de inlichtingen- en veiligheidsdiensten 2017, Artikel 40: 1. De diensten zijn bevoegd tot: a. het observeren en in het kader daarvan vastleggen van gegevens betreffende gedragingen van natuurlijke personen of gegevens betreffende zaken, al dan niet met behulp van observatie- en registratiemiddelen; b. het volgen en in het kader daarvan vastleggen van gegevens betreffende natuurlijke personen of zaken, al dan niet met behulp van volgmiddelen, plaatsbepalingsapparatuur en registratiemiddelen. 2. De uitoefening van de bevoegdheid, bedoeld in het eerste lid, is slechts toegestaan, indien Onze betrokken Minister of namens deze het hoofd van een dienst daarvoor toestemming heeft verleend. Het hoofd van een dienst kan aan hem ondergeschikte ambtenaren bij schriftelijk besluit aanwijzen die de	The Intelligence and Security Services Act 2017, Article 40: 1. The services are authorised to: a. observing and, in this context, recording data on the behavior of natural persons or data on matters, whether or not with the aid of observation and registration means; b. tracking and, in this context, recording data relating to natural persons or property, whether or not with the aid of tracking devices, positioning equipment and registration devices. 2. The exercise of the power referred to in the first paragraph is only permitted if the relevant Minister or the head of a service on his behalf has given permission for this. The head of a service may designate officials subordinate to him by written decision to

toestemming, bedoeld in de eerste volzin, namens hem verlenen. Onze betrokken Minister wordt een afschrift van het besluit, bedoeld in de tweede volzin, gezonden. 3. De toepassing van observatie- en registratiemiddelen, bedoeld in het eerste lid, onder a, binnen woningen is slechts toegestaan, indien daarvoor door Onze betrokken Minister schriftelijk toestemming is verleend aan het hoofd van de dienst. 4. Het verzoek om toestemming als bedoeld in het derde lid wordt gedaan door het hoofd van de dienst en bevat in aanvulling op hetgeen in artikel 29, tweede lid, is bepaald: a. het adres van de woning waarbinnen het middel dient te worden toegepast; b. een omschrijving van het soort middel dat wordt toegepast.	grant the permission referred to in the first sentence on his behalf. A copy of the decision referred to in the second sentence will be sent to the relevant Minister. 3. The use of means of observation and registration, as referred to in the first paragraph, under a, within dwellings is only permitted if the head of the service has given written permission for this by the relevant Minister. 4. The request for permission as referred to in the third paragraph is made by the head of the service and, in addition to the provisions of Article 29, second paragraph , contains: a. the address of the home in which the agent is to be applied; b. a description of the type of agent used.
Wet op de inlichtingen- en veiligheidsdiensten 2017, Artikel 137 1. Indien in een bestuursrechtelijke procedure inzake de toepassing van deze wet of de Wet veiligheidsonderzoeken Onze betrokken Minister of de commissie van toezicht door de bestuursrechter ingevolge artikel 8:27, 8:28 of 8:45 van de Algemene wet bestuursrecht wordt verplicht tot het verstrekken van inlichtingen dan wel het overleggen van stukken en de desbetreffende inlichtingen worden verstrekt onderscheidenlijk de stukken worden overgelegd waarbij door Onze betrokken Minister dan wel de commissie van toezicht is aangegeven dat vanwege het bestaan van gewichtige redenen als bedoeld in artikel 8:29, eerste lid, van de Algemene wet bestuursrecht uitsluitend de bestuursrechter kennis zal mogen nemen van de desbetreffende inlichtingen onderscheidenlijk de stukken, en de	The Intelligence and Security Services Act 2017, Article 137 If, in administrative proceedings regarding the application of this Act or the Security Investigations Act, Our relevant Minister or the supervisory committee is obliged by the administrative judge pursuant to Article 8:27, 8:28 or 8:45 of the General Administrative Law Act to provide information or the submission of documents and the relevant information shall be provided or the documents submitted whereby the relevant Minister or the supervisory committee has indicated that due to the existence of compelling reasons as referred to in section 8:29, subsection 1, of the General Administrative Law Act, only the administrative judge will be allowed to take cognisance of the relevant information or the documents, and the administrative judge, on

bestuursrechter op grond van artikel 8:29, derde lid, van de Algemene wet bestuursrecht tot het oordeel komt dat ten onrechte een beroep op gewichtige redenen wordt gedaan, worden de stukken aan Onze betrokken Minister dan wel de commissie van toezicht teruggezonden. De bestuursrechter stelt daaraan voorafgaand Onze betrokken Minister dan wel de commissie van toezicht in de gelegenheid de desbetreffende inlichtingen onderscheidenlijk stukken alsnog zonder het voorbehoud dat uitsluitend de bestuursrechter er kennis van kan nemen te verstrekken.

2. Indien in een bestuursrechtelijke procedure inzake de toepassing van deze wet of de Wet veiligheidsonderzoeken Onze betrokken Minister of de commissie van toezicht door het Gerecht of het Hof ingevolge artikel 23, 28 en 29 van de Wet administratieve rechtspraak BES wordt verplicht tot het verstrekken van inlichtingen dan wel het overleggen van stukken en de desbetreffende inlichtingen worden verstrekt onderscheidenlijk de stukken worden overgelegd waarbij door Onze betrokken Minister dan wel de commissie van toezicht is aangegeven dat vanwege het bestaan van gewichtige redenen als bedoeld in artikel 24, eerste lid, van de Wet administratieve rechtspraak BES uitsluitend het Gerecht of het Hof kennis zal mogen nemen van de desbetreffende inlichtingen onderscheidenlijk de stukken, en het Gerecht of het Hof op grond van artikel 24, derde lid, van de Wet administratieve rechtspraak BES tot het oordeel komt dat ten onrechte een beroep op gewichtige redenen wordt gedaan, worden de stukken aan Onze betrokken Minister dan wel de commissie van toezicht teruggezonden. Het Gerecht of het Hof stelt daaraan voorafgaand Onze betrokken Minister dan wel de commissie

the basis of Article 8:29, third paragraph, of the General Administrative Law Act, concludes that it is wrong to rely on serious reasons is done, the documents are sent to the relevant Minister the supervisory committee. Prior to this, the administrative judge shall give the relevant Minister or the supervisory committee the opportunity to provide the relevant information or documents, respectively, without the reservation that only the administrative judge can take cognisance thereof.

2. If, in administrative proceedings regarding the application of this Act or the Security Investigations Act, Our relevant Minister or the supervisory committee is required by the General Court or the Court of Appeal pursuant to Article 23, 28 and 29 of the BES Administrative Justice Act to provide information, then the submission of documents and the relevant information are provided or the documents are submitted whereby the relevant Minister or the supervisory committee has indicated that due to the existence of important reasons as referred to in Article 24, first paragraph, of the Administrative Justice Act BES only the General Court or the Court of Appeal will be allowed to take cognisance of the relevant information or the documents, and the General Court or the Court of Justice, on the basis of Article 24, third paragraph, of the BES Administrative Justice Act, has come to the weighty reasons are made to pieces The relevant Minister or the supervisory committee returned. Prior to this, the General Court or the Court of Appeal shall give the relevant Minister or the supervisory committee the opportunity to provide the relevant information or documents, without

van toezicht in de gelegenheid de desbetreffende inlichtingen onderscheidenlijk stukken alsnog zonder het voorbehoud dat uitsluitend het Gerecht of het Hof er kennis van kan nemen te verstrekken. 3. Het eerste en tweede lid is van overeenkomstige toepassing ingeval Onze betrokken Minister, niet zijnde partij in de bestuursrechtelijke procedure, wordt verplicht tot het geven van inlichtingen dan wel het overleggen van stukken in verband met door de dienst gedane mededelingen als bedoeld in artikel 62, eerste lid, onder a en b. 4. Indien door Onze betrokken Minister of de commissie van toezicht aan de bestuursrechter onderscheidenlijk het Gerecht of het Hof stukken dienen te worden overgelegd, kan worden volstaan met het ter inzage geven van de desbetreffende stukken. Van de desbetreffende stukken mag op generlei wijze een afschrift worden vervaardigd.	the reservation that only the General Court or the Court of Appeal may take cognizance thereof. 3. Subsections 1 and 2 apply mutatis mutandis if the relevant Minister, who is not a party to the administrative procedure, is obliged to provide information or submit documents in connection with communications made by the service as referred to in Article 62, first paragraph, under a and b. 4. If the relevant Minister or the supervisory committee must submit documents to the administrative judge or the General Court or the Court of Appeal, it will suffice to make the relevant documents available for inspection. No copies may be made of the relevant documents in any way.
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 1: In deze wet en de daarop berustende bepalingen wordt verstaan onder: bijzondere categorieën van persoonsgegevens: de categorieën van persoonsgegevens, bedoeld in artikel 9, eerste lid, van de verordening Onze Minister: Onze Minister voor Rechtsbescherming; persoonsgegevens van strafrechtelijke aard: persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de verordening, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk	General Data Protection Regulation Implementation Act, Article 1: The following terms will be defined as follows in this Act and in provisions based upon it: Special categories of personal data: The categories of personal data referred to in Article 9(1) of the Regulation; Our Minister: Our Minister for Legal Protection; Personal data relating to matters of criminal law: Personal data relating to criminal convictions and offenses or related security measures as referred to in Article 10 of the Regulation as well as personal data regarding a court-ordered injunction due to unlawful or objectionable conduct;

gedrag; verordening: verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).	Regulation: 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) (PbEU 2016, L 119).
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 6: 1. Er is een Autoriteit persoonsgegevens. 2. De Autoriteit persoonsgegevens is de toezichthoudende autoriteit, bedoeld in artikel 51, eerste lid, van de verordening. 3. Onverminderd artikel 57 van de verordening, heeft de Autoriteit persoonsgegevens tot taak toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de verordening of de wet bepaalde. 4. Ter uitvoering van een bindende EU-rechtshandeling kunnen, gehoord de Autoriteit persoonsgegevens, bij regeling van Onze Minister aan de Autoriteit persoonsgegevens taken worden opgedragen.	General Data Protection Regulation Implementation Act, Article 6: 1. There is a Dutch Data Protection Authority. The Dutch Data Protection Authority obtains legal personality. 2. The Dutch Data Protection Authority is the supervisory authority referred to in Article 51(1) of the Regulation. 3. Without prejudice to Article 57 of the Regulation, the Dutch Data Protection Authority is charged with the supervision of the processing of personal data in accordance with the provisions laid down by and pursuant to the Regulation or the law. 4. To implement a binding EU legal act, tasks may be assigned to the Dutch Data Protection Authority pursuant to a regulation by the Minister after the Dutch Data Protection Authority has been consulted
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 14(3): 3. De Autoriteit persoonsgegevens kan in geval van overtreding van het bepaalde in artikel 83, vierde, vijfde of zesde lid, van de verordening een bestuurlijke boete opleggen van ten hoogste de in deze leden genoemde bedragen.	General Data Protection Regulation Implementation Act, Article 14(3): 3. The Dutch Data Protection Authority may impose an administrative fine not exceeding the amounts referred to in these subsections for violation of any of the provisions of Article 83(4), (5) or (6) of the Regulation.
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 15(1):	General Data Protection Regulation Implementation Act, Article 15(1):

1. Met het toezicht op de naleving van de verordening en op de verwerking van persoonsgegevens overeenkomstig het bij of krachtens de wet bepaalde zijn belast de leden en buitengewone leden van de Autoriteit persoonsgegevens, de ambtenaren van het secretariaat van de Autoriteit persoonsgegevens, alsmede de bij besluit van de Autoriteit persoonsgegevens aangewezen personen.	1. The members and extraordinary members of the Data Protection Authority, the officials of the secretariat of the Data Protection Authority and the persons designated by a resolution of the Data Protection Authority are responsible for monitoring compliance with the Regulation and with the processing of personal data in accordance with the provisions under or pursuant to the law.
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 16: 1. De Autoriteit persoonsgegevens kan een last onder bestuursdwang opleggen ter handhaving van de bij of krachtens de verordening of deze wet gestelde verplichtingen. 2. De Autoriteit persoonsgegevens kan een last onder bestuursdwang opleggen ter handhaving van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht, voor zover het betreft de verplichting tot het verlenen van medewerking aan een vordering van een bij of krachtens artikel 15, eerste lid, aangewezen persoon. 3. De te betalen geldsom van een verbeurde dwangsom komt toe aan de Staat.	General Data Protection Regulation Implementation Act, Article 16: 1. The Dutch Data Protection Authority may impose an administrative enforcement order to enforce obligations laid down by or pursuant to this Act. 2. The Dutch Data Protection Authority may impose an administrative enforcement order to enforce Section 5:20(1) of the General Administrative Law Act insofar as it concerns the obligation to cooperate with a request by an official designated by or pursuant to Section 15(1). 3. The amount of a forfeited penalty shall accrue to the State.
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 22: 1. Overeenkomstig artikel 9, eerste lid, van de verordening zijn verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid verboden.	General Data Protection Protocol Regulation Implementation Act, Article 22: 1. In accordance with Article 9(1) of the Regulation, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited.

2. Overeenkomstig artikel 9, tweede lid, onderdelen a, c, d, e en f, van de verordening is het verbod om bijzondere categorieën van persoonsgegevens te verwerken niet van toepassing, indien:

- a. de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden;
- b. de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon, indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;
- c. de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt;
- d. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt; of
- e. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer gerechten handelen in het kader van

2. In accordance with Article 9(2)(a), (c), (d), (e) and (f) of the Regulation, the prohibition on processing special categories of personal data does not apply if:

- a. the data subject has given explicit consent for the personal data in question to be processed for one or more clearly defined purposes;
- b. the processing is necessary in order to protect the vital interests of the data subject or of another natural person where the data subject is not physically or legally capable of giving consent;
- c. the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside that body without the consent of the data subjects;
- d. the processing relates to personal data that is manifestly made public by the data subject; or
- e. the processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.

hun rechtsbevoegdheid.	
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 23: Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om bijzondere categorieën van persoonsgegevens te verwerken niet van toepassing, indien: a. de verwerking noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting; b. de gegevens worden verwerkt door de Autoriteit persoonsgegevens of een ombudsman als bedoeld in artikel 9:17 van de Algemene wet bestuursrecht, en voor zover de verwerking noodzakelijk is voor de uitvoering van de hun wettelijk opgedragen taken, onder voorwaarde dat bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad; of c. de verwerking noodzakelijk is in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard voor de doeleinden waarvoor deze gegevens worden verwerkt.	General Data Protection Protocol Regulation Implementation Act, Article 23: In view of Article 9(2)(g) of the Regulation, the prohibition on processing special categories of personal data does not apply if: a. the processing is necessary in order to satisfy an obligation under international law; b. the data is processed by the Data Protection Authority or an ombudsman as referred to in Article 9:17 of the Dutch general administrative law act, and if processing is necessary for the performance of their legal duties, on the condition that adequate safeguards are provided to prevent disproportionate infringement of the data subject's privacy; or c. the processing is necessary in addition to the processing of personal data relating to matters of criminal law for the purposes for which this data is processed.
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 24: Gelet op artikel 9, tweede lid, onderdeel j, van de verordening, is het verbod om bijzondere categorieën van persoonsgegevens te verwerken niet van toepassing, indien: a. de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, eerste lid,	General Data Protection Protocol Regulation Implementation Act, Article 24: In view of Article 9(2)(j) of the Regulation, the prohibition on processing special categories of personal data does not apply if: a. the processing is necessary for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1) of the Regulation;

van de verordening; b. het onderzoek, bedoeld in onderdeel a, een algemeen belang dient; c. het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost; en d. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.	b. the research referred to in point (a) serves a public interest; c. requesting explicit consent proves to be impossible or requires disproportionate effort; and d. adequate safeguards are provided to prevent disproportionate infringement of the data subject's privacy.
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 25: Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om persoonsgegevens te verwerken waaruit ras of etnische afkomst blijkt, niet van toepassing, indien de verwerking geschiedt: a. met het oog op de identificatie van de betrokkene, en slechts voor zover de verwerking voor dat doel onvermijdelijk is; of b. met het doel personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen teneinde feitelijke nadelen, verband houdende met de grond ras of etnische afkomst, op te heffen of te verminderen, en slechts voor zover: 1°. de verwerking voor dat doel noodzakelijk is; 2°. de gegevens betrekking hebben op het geboorteland van de betrokkene, diens ouders of diens grootouders, dan wel op andere, bij wet vastgestelde criteria op grond waarvan op objectieve wijze vastgesteld kan worden of iemand tot een bepaalde etnische of culturele minderheidsgroep behoort; en	General Data Protection Protocol Regulation Implementation, Article 25: In view of Article 9(2)(g) of the Regulation, the prohibition on processing personal data revealing race or ethnic origin does not apply if the processing occurs: a. for the purpose of identifying the data subject, and only insofar as processing for that purpose is unavoidable; or b. for the purpose of giving a certain ethnic or cultural minority group a preferential position with the aim of eliminating or reducing actual disadvantages experienced on the grounds of race or ethnic origin, and only if: 1. the processing is necessary to that aim; 2. the data pertains to the country of birth of the data subject or the data subject's parents or grandparents, or to other legally defined criteria allowing for the objective determination of whether or not a natural person belongs to a certain ethnic or cultural minority group; and 3. the data subject has not objected in writing to the processing.

3°. de betrokkene tegen de verwerking geen schriftelijk bezwaar heeft gemaakt.	
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 26: Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om persoonsgegevens te verwerken waaruit politieke opvattingen blijken, niet van toepassing, indien de verwerking geschiedt met het oog op de eisen die met betrekking tot politieke opvattingen in redelijkheid kunnen worden gesteld in verband met de vervulling van functies in bestuursorganen en adviescolleges.	General Data Protection Protocol Regulation Implementation Act, Article 26: In view of Article 9(2)(g) of the Regulation, the prohibition on processing personal data revealing political opinions does not apply if the processing is carried out in connection with reasonable requirements regarding political opinions imposed with a view to filling openings in administrative and advisory bodies.
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 27: 1. Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om persoonsgegevens te verwerken waaruit religieuze of levensbeschouwelijke overtuigingen blijken, niet van toepassing, indien de verwerking geschiedt door andere instellingen dan de instellingen, bedoeld in artikel 22, tweede lid, onderdeel c, en voor zover de verwerking noodzakelijk is met het oog op de geestelijke verzorging van de betrokkene, tenzij deze daartegen schriftelijk bezwaar heeft gemaakt. 2. In de gevallen, bedoeld in het eerste lid, worden geen persoonsgegevens aan derden verstrekt zonder toestemming van de betrokkene.	General Data Protection Protocol Regulation Implementation Act, Article 27: 1. In view of Article 9(2)(g) of the Regulation, the prohibition on processing personal data revealing religious or philosophical beliefs does not apply if the processing is carried out by institutions other than the institutions referred to in Article 22(2)(c), and insofar as the processing is necessary with a view to the spiritual counseling of the data subject unless the data subject has objected in writing. 2. In the cases referred to in Paragraph 1, no personal data is to be shared with third parties without the data subject's consent.
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 28 1. Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om genetische gegevens te verwerken niet van	General Data Protection Protocol Regulation Implementation Act, Article 28: 1. In view of Article 9(2)(g) of the Regulation, the prohibition on processing genetic data does not apply if this processing occurs in

toepassing, indien deze verwerking plaatsvindt met betrekking tot de betrokkene bij wie de desbetreffende gegevens zijn verkregen. 2. In andere gevallen dan bedoeld in het eerste lid, is het verbod om genetische gegevens te verwerken uitsluitend niet van toepassing, indien: a. een zwaarwegend geneeskundig belang prevaleert; of b. de verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoek dat een algemeen belang dient of ten behoeve van statistiek, indien: 1°. de betrokkene uitdrukkelijke toestemming heeft gegeven; en 2°. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. 3. Toestemming als bedoeld in het tweede lid, onderdeel b, is niet vereist, indien het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning vergt.	relation to the data subject from whom said data has been received. 2. In cases other than those referred to in Paragraph 1, the prohibition on processing genetic data does not apply only if: a. a serious medical interest prevails; or b. the processing is necessary for scientific research serving a public interest or for statistical purposes if: 1. the data subject has given explicit consent; and 2. adequate safeguards are provided to prevent disproportionate infringement of the data subject's privacy. 3. Consent as referred to in Paragraph 2(b) is not required if requesting explicit consent proves to be impossible or requires disproportionate effort.
Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 29: Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.	General Data Protection Protocol Regulation Implementation Act, Article 29: In view of Article 9(2)(g) of the Regulation, the prohibition on processing biometric data for the purposes of uniquely identifying a natural person does not apply if the processing is necessary for authentication or security purposes.

Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Artikel 30: 1. Gelet op artikel 9, tweede lid, onderdeel b, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing, indien de verwerking geschiedt door bestuursorganen, pensioenfondsen, werkgevers of instellingen die te hunnen behoeve werkzaam zijn, en voor zover de verwerking noodzakelijk is voor: a. een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene; of b. de re-integratie of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid. 2. Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing, indien de verwerking geschiedt door: a. scholen, voor zover de verwerking met het oog op de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is; b. een reclasseringsinstelling, een bijzondere reclasseringsambtenaar, de raad voor de kinderbescherming, de gecertificeerde instelling, bedoeld in artikel 1.1 van de Jeugdwet, of de rechtspersoon, bedoeld in artikel 256, eerste lid, of artikel 302, tweede lid, van Boek 1 van het Burgerlijk Wetboek, voor zover de verwerking noodzakelijk	General Data Protection Protocol Regulation Implementation Act, Article 30: 1. In view of Article 9(2)(b) of the Regulation, the prohibition on processing health data does not apply if the processing is carried out by administrative bodies, pension funds, employers or agencies working for the benefit of the data subjects and insofar as the processing is necessary for: a. proper execution of statutory regulations, pension schemes or collective employment contracts providing benefits that are contingent on the health of the data subject; or b. the reintegration or assistance of employees or individuals entitled to government assistance in connection with illness or work disability. 2. In view of Article 9(2)(g) of the Regulation, the prohibition on processing health data does not apply if the processing is carried out by: a. schools, insofar as the processing is necessary with a view to providing special assistance to students or special accommodations related to their health; b. a probation institution, a special probation officer, the Raad voor de Kinderbescherming (Dutch council for child protection), the certified agency referred to in Article 1.1 of the Jeugdwet (Dutch youth act) or the legal entity referred to in Article 256(1) or Article 302(2) of Book 2 of the Burgerlijk Wetboek (Dutch civil code), insofar as the processing is necessary for the performance of the legal duties for which they are responsible; or

is voor de uitvoering van de aan hen opgedragen wettelijke taken; of c. Onze Minister en Onze Minister van Justitie en Veiligheid voor zover de verwerking in verband met de tenuitvoerlegging van vrijheidsbenemende maatregelen noodzakelijk is. 3. Gelet op artikel 9, tweede lid, onderdeel h, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing indien de verwerking geschiedt door: a. hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk; of b. verzekeraars als bedoeld in artikel 1:1 van de Wet op het financieel toezicht of financiële dienstverleners die bemiddelen in verzekeringen als bedoeld in artikel 1:1 van die wet, voor zover de verwerking noodzakelijk is voor: 1°. de beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt; of 2°. de uitvoering van de overeenkomst van verzekering dan wel het assisteren bij het beheer en de uitvoering van de verzekering. 4. Indien toepassing wordt gegeven aan het eerste, tweede of derde lid, worden de gegevens alleen verwerkt door personen die uit hoofde	c. Our Minister and Our Minister of Justice and Security, insofar as the processing is necessary for the implementation of measures entailing the deprivation of liberty. 3. In view of Article 9(2)(h) of the Regulation, the prohibition on processing health data does not apply if the processing is carried out by: a. professionals, agencies or facilities for health care or social services, insofar as the processing is necessary for the data subject's proper treatment or care or the management of the agency or professional practice; or b. insurers as referred to in Article 1:1 of the Wet op het financieel toezicht (Dutch financial supervision act) or financial service providers who act as insurance agents as referred to in Article 1:1 of said act, insofar as the processing is necessary for: 1. the evaluation of the risk to be insured by the insurer and the data subject has no objections; or 2. the implementation of the insurance contract or assistance with the management and implementation of the insurance. 4. If Paragraphs 1, 2 or 3 are applied, the data is to be processed solely by persons required to observe confidentiality by virtue of their office, profession or a statutory regulation or pursuant to an agreement. If the controller processes personal data and is not already bound to observe confidentiality by virtue of office, profession or a statutory regulation, the controller is required to observe confidentiality in respect of the data, except insofar as the law requires the controller to disclose the data or the task entails the need

van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Indien de verwerkingsverantwoordelijke persoonlijk gegevens verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voor zover de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan anderen die krachtens het eerste, tweede of derde lid bevoegd zijn tot verwerking daarvan. 5. Het verbod om andere bijzondere categorieën van persoonsgegevens te verwerken is niet van toepassing, indien de verwerking noodzakelijk is in aanvulling op de verwerking van gegevens over gezondheid, bedoeld in het derde lid, aanhef en onderdeel a, met het oog op een goede behandeling of verzorging van de betrokkene. 6. Bij algemene maatregel van bestuur kunnen omtrent de toepassing van het eerste lid en het derde lid, aanhef en onderdeel b, nadere regels worden gesteld.	to disclose the data to others who are authorised to process the data pursuant to Paragraphs 1, 2 or 3. 5. The prohibition on processing other special categories of personal data does not apply if the processing is necessary in addition to the processing of data regarding health as referred to in Paragraph 3, opening words and point (a), for the data subject's proper treatment or care. 6. Further rules regarding the application of Paragraph 1 and Paragraph 3, opening words and point (b), may be made by an order in council.
Uitvoeringswet Algemene Verordening Gegevensbescherming, Artikel 36(1): 1. De belanghebbende kan zich ook binnen de termijn bepaald voor het instellen van beroep op grond van de Algemene wet bestuursrecht, dan wel die, bedoeld in artikel 35, tweede lid, tot de Autoriteit persoonsgegevens wenden met het verzoek te bemiddelen of te adviseren in zijn geschil met de verwerkingsverantwoordelijke, dan wel gebruik maken van een geschillenbeslechtsingsregeling als bedoeld in artikel 40, tweede lid, onderdeel k, van de verordening, op grond van een	General Data Protection Regulation Implementation Act, Article 36(1): 1. The interested party may also file a request with the Dutch Data Protection Authority, within the time limit set for the appeal under the General Administrative Law Act or within the time limit referred to in Section 35(2), to mediate in or advise on his or her dispute with the controller or to use a dispute resolution scheme as referred to in Article 40(2)(k) of the Regulation under an approved code of conduct as referred to in Article 40(5) of the Regulation. In that case, in derogation from

goedgekeurde gedragscode als bedoeld in artikel 40, vijfde lid, van de verordening. In dat geval kan het beroep in afwijking van artikel 6:7 van de Algemene wet bestuursrecht nog worden ingesteld dan wel de procedure ingevolge artikel 35 nog aanhangig worden gemaakt nadat de belanghebbende van de Autoriteit persoonsgegevens bericht heeft ontvangen dat de behandeling van de zaak is beëindigd of ingevolge de geschillenbeslechtsregeling, bericht heeft ontvangen dat de behandeling van de zaak is beëindigd, doch uiterlijk zes weken na dat tijdstip.	Section 6:7 of the General Administrative Law Act, the appeal may still be filed or the proceedings referred to in Section 35 may still be issued after the interested party has been notified – either by the Dutch Data Protection Authority or pursuant to the dispute resolution scheme – that the case has been closed, but not more than six weeks after such date.
Uitvoeringswet Algemene Verordening Gegevensbescherming, Artikel 40(1): 1. Artikel 22, eerste lid, van de verordening geldt niet indien de in die bepaling bedoelde geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang.	General Data Protection Protocol Regulation Implementation, Article 40: Article 22, first paragraph, of the Regulation does not apply if the automated individual decision-making referred to in that provision, other than on the basis of profiling, is necessary to comply with a legal obligation that rests on the controller or is necessary for the fulfillment of a task in the public interest.
Uitvoeringswet Algemene Verordening Gegevensbescherming, Artikel 41: 1. De verwerkingsverantwoordelijke kan de verplichtingen en rechten, bedoeld in de artikelen 12 tot en met 21 en artikel 34 van de verordening, buiten toepassing laten voor zover zulks noodzakelijk en evenredig is ter waarborging van: - de nationale veiligheid; - landsverdediging; - de openbare veiligheid; - de voorkoming, het onderzoek, de	General Data Protection Regulation Implementation Act, Article 41: 1. The controller may render the obligations and rights referred to in Articles 12 through 21 and Article 34 of the Regulation inapplicable if necessary and proportionate, for the purpose of: - national security; - national defense; - public safety; - prevention, investigation, detection and prosecution of criminal offenses or

opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid; e. andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid; f. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures; g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscode voor gereguleerde beroepen; h. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g; i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of j. de inning van civielrechtelijke vorderingen. k. 2. Bij de toepassing van het eerste lid houdt de verwerkingsverantwoordelijke rekening met in ieder geval, voor zover van toepassing: a. de doeleinden van de verwerking of van de categorieën van verwerking;	enforcement of punishments, including protection against and prevention of public safety hazards; e. other significant objectives of public interest of the European Union or of the Netherlands, in particular any significant economic or financial interest of the European Union or the Netherlands, including monetary, budgetary and fiscal matters, public health and social security; f. protection of the independence of the judiciary and judicial proceedings; g. prevention, investigation, detection and prosecution of violations of the professional codes for regulated professions; h. a monitoring, inspection or legislation duty that is associated, even incidentally, with the exercise of public authority in the cases referred to in points (a), (b), (c), (d), (e) and (g); i. protection of the data subject or of the rights and freedoms of others; or j. enforcement of claims under civil law. 2. When applying Paragraph 1, the controller is to take at least the following into consideration, insofar as applicable: a. the objectives of the processing or of the categories of processing; b. the categories of personal data; c. the scope of application of the implemented restrictions; d. safeguards to prevent misuse or unlawful access or transfer; e. the specification of the controller or of the categories of controller; f. the archiving periods and applicable safeguards, considering the nature, scope and

b. de categorieën van persoonsgegevens; c. het toepassingsgebied van de ingevoerde beperkingen; d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte; e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken; f. de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking; g. de risico's voor de rechten en vrijheden van de betrokkenen; en h. het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.	objectives of the processing or of the categories of processing; g. the risks to the data subject's rights and freedoms; and h. the data subject's right to be notified of any restriction, unless such notification could be prejudicial to the purpose of the restriction.
Uitvoeringswet Algemene Verordening Gegevensbescherming, Artikel 42: Artikel 34 van de verordening is niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht.	General Data Protection Protocol Regulation Implementation Act, Article 42: Article 34 of the Regulation does not apply to financial enterprises as referred to in the Dutch financial supervision act.
Uitvoeringswet Algemene Verordening Gegevensbescherming, Artikel 44: Indien een verwerking wordt verricht door instellingen of diensten voor wetenschappelijk onderzoek of statistiek, en de nodige voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische of wetenschappelijke doeleinden kunnen worden gebruikt, kan de verwerkingsverantwoordelijke de artikelen 15,	General Data Protection Protocol Regulation Implementation Act, Article 44: The controller may refrain from observing Articles 15, 16 and 18 of the Regulation when processing is carried out by agencies or services for scientific research or statistical purposes and the necessary measures have been taken to ensure that personal data can only be used for statistical or scientific purposes.

16 en 18 van de verordening buiten toepassing laten.	
Uitvoeringswet Algemene Verordening Gegevensbescherming, Artikel 45: 1. Bij de verwerking van persoonsgegevens die deel uitmaken van archiefbescheiden als bedoeld in artikel 1, onderdeel c, van de Archiefwet 1995, die berusten in een archiefbewaarplaats als bedoeld in artikel 1, onderdeel f, van die wet, zijn de artikelen 15, 16, 18, eerste lid, onderdeel a, en 20 van de verordening niet van toepassing. 2. Betrokkene heeft het recht om inzage te verkrijgen in de archiefbescheiden, tenzij verzoeken om inzage zodanig ongericht zijn dat deze in redelijkheid niet kunnen worden ingewilligd. 3. Betrokkene heeft het recht om, in geval van onjuiste persoonsgegevens, zijn eigen lezing aan de desbetreffende archiefbescheiden toe te voegen.	General Data Protection Protocol Regulation Implementation Act, Article 45: 1. Articles 15, 16, 18(1)(a) and 20 of the Regulation do not apply to the processing of personal data comprising part of an archive of documents as referred to in Article 1(c) of the Archiefwet 1995 (Dutch public records act of 1995) and kept in an archive repository as referred to in Article 1(f) of that act. 2. The data subject is entitled to access the archived documents unless requests for access are so broad that they cannot reasonably be granted. 3. The data subject is entitled to annotate the relevant archived documents if the personal data is incorrect.
Uitvoeringswet Algemene Verordening Gegevensbescherming, Artikel 47: 1. De artikelen 15, 16, 18 en 19 van de verordening zijn niet van toepassing op bij de wet ingestelde openbare registers, indien bij of krachtens die wet een bijzondere procedure voor de verbetering, aanvulling, verwijdering of afscherming van gegevens is geregeld. 2. Artikel 21 van de verordening is niet van toepassing op bij de wet ingestelde openbare registers.	General Data Protection Protocol Regulation Implementation Act, Article 47: 1. Articles 15, 16, 18 and 19 of the Regulation do not apply to public registers established by law if a special procedure for the correction, addition, removal or protection of data is stipulated under or pursuant to such legislation. 2. Article 21 of the Regulation does not apply to public registers established by law.

Algemene Wet Bestuursrecht, Artikel 3:45: 1. Indien tegen een besluit bezwaar kan worden gemaakt of beroep kan worden ingesteld, wordt daarvan bij de bekendmaking en bij de mededeling van het besluit melding gemaakt. 2. Hierbij wordt vermeld door wie, binnen welke termijn en bij welk orgaan bezwaar kan worden gemaakt of beroep kan worden ingesteld.	Dutch General Administrative Law Act, Article 3:45: 1. If an objection may be made or an appeal may be lodged against an order, this shall be stated when notifying and giving communication of the order. 2. At the same time it shall be stated by whom, within what time limit and with which authority an objection may be made or an appeal may be lodged.
Burgerlijk Wetboek Boek 6, Artikel 95(1): De schade die op grond van een wettelijke verplichting tot schadevergoeding moet worden vergoed, bestaat in vermogensschade en ander nadeel, dit laatste voor zover de wet op vergoeding hiervan recht geeft.	Dutch Civil Code Book 6, Article 95(1): The damage that must be compensated on the basis of a legal obligation to pay compensation consists of financial loss and other disadvantages, the latter insofar as the law entitles the holder to compensation.
Wetboek van Strafrecht, Artikel 54a: Een tussenpersoon die een communicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt bij een strafbaar feit dat met gebruikmaking van die dienst wordt begaan als zodanig niet vervolgd indien hij voldoet aan een bevel als bedoeld in artikel 125p van het Wetboek van Strafvordering.	Dutch Criminal Code, Article 54a: An intermediary which provides a telecommunication service that consists of the transfer or storage of data from a third party, shall not be prosecuted when a criminal act is conducted with use of that service, provided that it meets the order as laid down in Article 125p of the Criminal Code.
Wetboek van Strafrecht, Artikel 80quinquies: Onder gegevens wordt verstaan iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken.	Dutch Criminal Code, Article 80quinquies: Data shall be understood to mean any representation of facts, concepts or instructions in an agreed upon form suitable for transfer, interpretation or processing by human beings or by computerised devices and systems.

Wet Bescherming Persoonsgegevens, Artikel 2(1): Deze wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.	Dutch Data Protection Act (DDPA), Article 2(1): This Act applies to the fully or partly automated processing of personal data, and the non-automated processing of personal data entered in a file or intended to be entered therein.
Wet Bescherming Persoonsgegevens, Artikel 16: De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.	Dutch Data Protection Act (DDPA), Article 16: It is prohibited to process personal data concerning a person's religion or philosophy of life, race, political persuasion, health and sexual life, or personal data concerning trade union membership, except as otherwise provided in this Section. This prohibition also applies to personal data concerning a person's criminal behaviour, or unlawful or objectionable conduct connected with a ban imposed with regard to such conduct.
Wet Politiegegevens, Artikel 7a(1): Een besluit dat uitsluitend op geautomatiseerde verwerking is gebaseerd, met inbegrip van profilering, dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft, is verboden, tenzij wordt voorzien in voorafgaande menselijke tussenkomst door of namens de verwerkingsverantwoordelijke en in specifieke voorlichting aan de betrokkene.	Dutch Police Act, Article 7a(1): A decision based solely on automated processing, including profiling, which has adverse legal effects or significantly affects the data subject is prohibited unless foreseen for prior human intervention by or on behalf of the controller and specific information to the data subject.

Bibliography

English titles

Legislation

Charter of Fundamental Rights of the European Union [2012] OJ C326/02

Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended by Protocols Nos 11 and 14 supplemented by Protocols Nos 1, 4, 6, 7, 12, 13 and 16) CETS 155

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

Parliament Resolution 2020/2012 of 28 September 2020 on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and related Technologies

Regulation 2016/679 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

Reservation made by the Netherlands to the International Covenant on Civil and Political Rights (signed 25 June 1969, entered into force 11 March 1979)

Universal Declaration of Human Rights (adopted 10 December 1948) UNGA res 217 A(III)

Reports

Article 29 Working Party, 'Guidelines On Personal Data Breach Notification Under Regulation 2016/679' (WP250rev01, 2018)

Article 29 Working Party, 'Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP 169, 2010)

Borgesius FZ, 'Discrimination, Artificial Intelligence and Algorithmic Decisions-making' (Directorate General of Democracy Council of Europe 2018)

Bychawska-Siniarska D, 'Protecting the Right to Freedom of Expression under the European Convention on Human Rights' (Council of Europe 2017)

Commissioner for Human Rights, 'Unboxing Artificial Intelligence: 10 steps to protect human rights' (Council of Europe 2019)

Committee of Experts on Internet Intermediaries (MSI-NET), 'Algorithms and human rights, study on the human rights dimensions of automated data processing techniques and possible regulatory implications' (Council of Europe 2017)

Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 'Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data' (Council of Europe 2017)

Dechesne F and Dignum V, 'AI & Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police' (Leiden/ Delft 2019)

European Commission for the Efficacy of Justice (CEPEJ), 'European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment' (Council of Europe 2018)

European Network of Legal Experts in Gender Equality and Non-discrimination, 'Country Report - Non-discrimination - Netherlands' (European Commission 2016)

Gloria F, 'Artificial Intelligence and Law Enforcement - Impact on Human Rights' (DG Internal Policies 2020)

Hagenauw D and Hijmans H, 'The New EU Data Protection Regime' (Fédération Internationale Pour Le Droit Européen XXIX Congress, 2020)

Koops B, 'Commanding Decryption and The Privilege Against Self-Incrimination' (Intersentia 2000)

Koops B, 'Cybercrime Legislation in The Netherlands' (Intersentia 2010)

National Cyber Security Centre, 'National Cyber Security Agenda' (Ministry of Justice and Security 2018)

Wardle C and Derakhshan H, 'Information Disorder: Towards an Interdisciplinary Framework for Research and Policy Making' (Council of Europe 2017)

Books

Brkan M and Psychogiopoulou E (eds), *Courts, Privacy and Data Protection in the Digital Environment* (Edward Elgar Publishing 2017)

Eijkman Q, van Eijk N and van Schaik R, *Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?* (Institute for Information Law, UvA 2018)

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Publications Office of the European Union 2018)

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Publications Office of the European Union 2018)

Gerards JH, *Judicial review in equal treatment cases* (Martinus Nijhoff Publishers 2005)

Jongen H, Bernard N and Yildirim E, 'The Privacy, Data Protection and Cybersecurity Law Review: Netherlands' in A Charles Raul and S Austin (eds), *The Privacy, Data Protection and Cybersecurity Law Review* (The Law Reviews 2020)

Junker L and Bosch B Heinsman L, *AI, Machine Learning & Big Data 2020* (Global Legal Insights 2020)

Koops BJ, 'Criteria for Normative Technology – The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values', in R Brownsword and K Yeung (eds), *Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008)

Krzysztofek M, *Post-Reform Personal Data Protection in the European Union: General Data Protection Regulation* (Wolters Kluwer 2017)

Kuner C, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013)

Reiding H, *The Netherlands and the Development of International Human Rights Instruments* (Kaaten 1996)

van den Berg E, 'Acting Normal and doing good: the Dutch and human rights', in I Lintel, A Buyse and B McGonigle Leyh (eds), *Defending Human Rights: Tools for Social Justice* (Cambridge Intersentia 2012)

van der Sloot B, Broeders D and Schrijvers E, *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016)

Periodicals

Adams M and van der Schyff G, 'Constitutional Review by the Judiciary in the Netherlands: a Matter of Politics and Democracy or Compensating Strategy?' [2006] 66(2) *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 399

Altreas N, Tsarapatsanis D, Preotiu-Pietro D and Lampos V, 'Predicting Judicial Decisions of the European Court of Human Rights: a Natural Language Processing Perspective' [2016] *PeerJ Computer Science* e93

Barocas S and Selbst AD, 'Big Data's Disparate Impact' [2016] 104 *California Law Review* 671

Bunder D and Varró K, 'Problematizing Data-driven Urban Practices: Insights from Five Dutch "Smart Cities"' [2019] 93 *Elsevier Cities* 145

de Poorter JCA, 'Constitutional Review: in the Netherlands: A joint Responsibility' [2013] 9(2) *Utrecht Law Review* 89

Kamara I, 'Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate' [2017] 8(1) *EJLT*

<<https://ejlt.org/index.php/ejlt/article/view/545/723>> accessed 12 February 2021

Kate JT and Van Koppen PJ, 'Judicialization of Politics in the Netherlands: Towards a Form of Judicial Review' [1994] 15(2) *International Political Science Review* 143

Piątek W, 'The right to an effective remedy in European law: significance, content and interaction' (2019) 6 *China-EU Law Journal* 163

van der Schyff G and Meuwese A, 'Dutch constitution law in globalizing world' [2013] 9(2) *Utrecht Law Review* 1

Digital resources

'About' <<https://proctorio.com/about>> accessed 15 February 2021

'Anti-Discrimination Laws In The Netherlands - L&E Global Knowledge Centre'

<<https://knowledge.leglobal.org/anti-discrimination-laws-in-the-netherlands/>> accessed 19 February 2021

'Artificial Intelligence mimics judicial reasoning'

<<https://www.lawgazette.co.uk/law/artificial-intelligence-mimics-judicial-reasoning/5056017.article>> accessed 3 February 2021

‘Bill for the Intelligence and Security Services Act (Wiv)’

<<https://pilpnjcm.nl/en/dossiers/bill-intelligence-security-services-act-wiv/>> accessed 19 February 2021

‘Countries Seen to Care About Human Rights’

<<https://www.usnews.com/news/best-countries/articles/the-10-countries-that-care-the-most-about-human-rights-according-to-perception>> accessed 14 February 2021

‘Data Protection Laws of the World – The Netherlands’

<<https://www.dlapiperdataprotection.com/index.html?t=law&c=NL>> accessed 30 January 2021

‘Data protection regulation in the Netherlands in the wake of the GDPR’

<<https://www.tjip.com/en/publications/data-protection-in-the-netherlands-in-the-wake-of-gdpr>> accessed 28 January 2021

‘Discrimination Cases In The Netherlands Rose 16 Percent In 2019’

<<https://nltimes.nl/2020/01/16/discrimination-cases-netherlands-rose-16-percent-2019>> accessed 19 February 2021

‘European Union – Countries’ <https://europa.eu/european-union/about-eu/countries_en> accessed 30 January 2021

‘GDPR Data Breach Survey 2020’

<<https://www.dlapiper.com/en/us/insights/publications/2020/01/gdpr-data-breach-survey-2020/>> accessed 19 February 2021

‘Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679’

<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf> accessed 15 February 2021

‘Inter-Institutional Agreement on Better Lawmaking’

<<http://www.europarl.europa.eu/legislative-train/theme-union-of-democratic-change/file-interinstitutional-agreement-on-better-law-making>> accessed 8 February 2021

‘Internet of Things Global Standard Initiative’

<<https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx>> accessed 30 January 2021

‘(Judicial) Constitutional Review In The Netherlands: A Comparative Law Blog’

<<https://www.peacepalacelibrary.nl/2015/03/judicial-constitutional-review-in-the-netherlands-a-comparative-law-blog/>> accessed 18 February 2021

‘KPMG Technology innovation hubs’

<<https://info.kpmg.us/content/dam/info/en/innovation-enterprise-solutions/pdf/2019/technology-innovation-hubs-2019.pdf>> accessed 10 February 2021

‘National Action Plan on Human Rights, the protection and promotion of human rights within the Netherlands’

<<https://www.government.nl/documents/publications/2020/05/31/national-action-plan-on-human-rights-2020>> accessed 19 February 2021

‘Netherlands: Court Prohibits Government’s Use of AI Software to Detect Welfare Fraud’
<<https://www.loc.gov/law/foreign-news/article/netherlands-court-prohibits-governments-use-of-ai-software-to-detect-welfare-fraud/>> accessed 1 February 2021

‘Netherlands - National GDPR Implementation Overview’
<<https://www.dataguidance.com/notes/netherlands-national-gdpr-implementation-overview>>
accessed 1 February 2021

‘Police have achieved a breakthrough in the interception and decryption of crypto communication’
<<https://www.politie.nl/en/news/2018/november/02-apeldoorn-police-have-achieved-a-breakthrough-in-the-interception-and-decryption-of-crypto-communication.html>> accessed 18 February 2021

‘Refusing to award legal personality to AI: Why the European Parliament got it wrong’
<<https://europeanlawblog.eu/2020/11/25/refusing-to-award-legal-personality-to-ai-why-the-european-parliament-got-it-wrong/>> accessed 5 February 2021

‘Tasks and Powers of the Dutch DPA’
<<https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/tasks-and-powers-dutch-dpa>>
accessed 10 February 2021

‘The Council of Europe in Brief – Member States’
<<https://www.coe.int/en/web/about-us/our-member-states>> accessed 30 January 2021

‘The data breach notification obligation as laid down in the Dutch Data Protection Act’
<https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/policy_rules_data_breach_notification_obligation.pdf> accessed 5 February 2021

‘The great question of the 21st century: Whose black box do you trust?’
<https://www.linkedin.com/pulse/great-question-21st-century-whose-black-box-do-you-trust-tim-o-reilly?trk=eml-b2_content_ecosystem_digest-hero-22-null&midToken=AQGexvwxq0Q3iQ&fromEmail=fromEmail&ut=2SrYDZ8lkCS7o1> accessed 15 February 2021

‘The Intelligence and Security Services Act 2017’
<<https://english.aivd.nl/about-aivd/the-intelligence-and-security-services-act-2017>> accessed 16 February 2021

‘To predict and serve?’
<<http://onlinelibrary.wiley.com/doi/10.1111/j.1740-9713.2016.00960.x/epdf>> accessed 11 February 2021

Uzman J, Barkhuysen T and van Emmerik ML, ‘The Dutch Supreme Court: A Reluctant Positive Legislator?’ [2010] 14(3) Electronic Journal of Comparative Law
<<http://www.ejcl.org/143/art143-16.pdf>> accessed 15 February 2021

Case-law

Blokhin v Russia App no 47152/06 (ECtHR, 13 April 2016)

Case 6/64 Costa v. ENEL (Court of Justice of the European Communities, 15 July 1964)

Case 311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Grand Chamber, 16 July 2020)

Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (GC, 13 May 2014)

Case 26/62 *Van Gend & Loos* (Court of Justice of the European Communities, 5 February 1963)

Case 342/12 *Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT)* (Third Chamber, 30 May 2013)

Jespers v Belgium App no 8404/78 (ECtHR, 15 October 1980)

S and Marper v the United Kingdom App nos 3056/04 and 30566/04 (ECtHR, 4 December 2008)

Salduz v Turkey App no 36391/02 (ECtHR, 17 November 2008)

Saunders v United Kingdom App no 19187/91 (ECtHR, 17 December 1996)

Dutch titles

Legislation

Algemene wet bestuursrecht 1992 (AwB)

Burgerlijk Wetboek 1992 (BW)

Telecommunicatiewet 1998, as amended 21 December 2020 (Tw)

Grondwet voor het Koninkrijk der Nederlanden 1815, as amended 21 December 2018 (Gw)

Uitvoeringswet Algemene Verordening Gegevensbescherming 2018 (UAVG)

Wet Bescherming Persoonsgegevens 1999 (WBP)

Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv)

Wet op de Nationale Ombudsman 1981, as amended 1 January 2020 (WNO)

Wet politiegegevens 2007 (Wpg)

Wetboek van Strafvordering 1921, as amended 1 January 2021 (Sv)

Reports

Appendices to the reports of the Second Chamber (17 600 ch V nr 2, 1982/83)

Appendices to the reports of the Second Chamber, (25 600 ch V nr 2, 1997/98)

Autoriteit Persoonsgegevens, ‘Balans - Jaarverslag 2019’ (2019)

Autoriteit Persoonsgegevens, ‘Meerjarenbegroting Groeiplan’ (2020)

Kamerstuk (24095 nr. 281, 2010/2011)

Kamerstukken II (13 872 nr 2, 1975/76)

Kamerstukken II (30 300 nr 32, 2005/06)

Kamerstukken II (30 517 nr 11-13, 2008/09)

Kamerstukken II (32 417 nr 14-25, 2010/11)

Kamerstukken II (34 372 nr 3, 2015/16)

Kamerstukken II (34851 3, 2017/18)

Köksal S, 'Het Nemo-Teneturbeginsel, Decryptiebevel en de Face ID' (Tilburg University, 2019)

Koops B, 'Het Decryptiebevel En Het Nemo-Teneturbeginsel Nopen Ontwikkelingen Sinds 2000 Tot Invoering Van Een Ontsleutelplicht Voor Verdachten?' (WODC, Ministerie van Veiligheid en Justitie 2012)

Rijksoverheid, 'Juridische aspecten van algoritmen die besluiten nemen Een verkennend onderzoek' (2020)

Rijksoverheid, 'Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA)' (2017)

Rijksoverheid, 'Ontsleutelplicht' (2019)

Rijksoverheid, 'Regulering Van Opsporingsbevoegdheden In Een Digitale Omgeving' (2018)

Books

Bunschoten DE, Hoogers HG, Broeksteeg JLW, Fleuren JWA, Bovend'Eert PPT, *Tekst en Commentaar Grondwet* (Kluwer 2015)

Foqué R and 't Hart AC, *Instrumentaliteit en rechtsbescherming* (Gouda Quint/ Kluwer Rechtswetenschappen 2011)

Hildebrandt M, Leenes RE and Lokin M, *Technologie en wetgeving in Cyberspace* (RegelMaat 2012)

Kortmann C, *Constitutioneel recht*, (Kluwer 2016)

Vegter T, *T&C arbeidsrecht* (Kluwer 2016)

Zwenne GJ and Kranenborg HR, *Tekst & Commentaar Privacy- en gegevensbeschermingsrecht* (7th edn, Wolters Kluwers 2021)

Periodicals

Sakkers H, 'Decentralisaties' en mensenrechten in Nederland - Lokale praktijken in een nationale én internationale context' (2017) 42 Nederlands Tijdschrift voor de Mensenrechten/Nederlands Juristen Comité voor de Mensenrechten Bulletin 3, 367

Digital resources

'Algemene Inlichtingen- en Veiligheidsdienst, 'Evaluatiecommissie Wiv',

<<https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen-en-veiligheidsdiensten/evaluatiecommissie-wiv>> accessed 14 February 2021

'Data Pro Code' <<https://www.nldigital.nl/data-pro-code/>> accessed 15 February 2020

'De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag'

<https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_belastingdienst_kinderopvangtoeslag.pdf> accessed 19 February 2021

'Evaluatiecommissie Wiv: enkele wijzigingen wet noodzakelijk'

<https://www.defensie.nl/actueel/nieuws/2021/01/20/evaluatiecommissie-wiv-enkele-wijzigingen-wet-noodzakelijk>> accessed 19 February 2021

‘Groei AP noodzakelijk voor bescherming burgers in digitaliserend Nederland’

<<https://autoriteitpersoonsgegevens.nl/nl/nieuws/groei-ap-noodzakelijk-voor-bescherming-burgers-digitaliserend-nederland>> accessed 19 February 2021

‘Human Centric AI’ <<https://nlaic.com/en/bouwsteen/human-centric-ai/>> accessed 2 February 2021

‘Instellingen en taken van het College Voor de Rechten Van de Mens’

<<https://mensenrechten.nl/nl/digitalisering>> accessed 29 January 2021

‘Jaarrapportage Meldplicht Datalekken’

<<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2019>> accessed 18 February 2021

‘Kabinetsstandpunt Encryptie’ <<https://zoek.officielebekendmakingen.nl/kst-26643-383.html>> accessed 19 February 2021

Letter from Autoriteit Persoonsgegevens to Stichting OLVG

<https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_olv.pdf> accessed 19 February 2021

‘Meldingsformulier Klachten’

<<https://autoriteitpersoonsgegevens.nl/nl/meldingsformulier-klachten>> accessed 19 February 2021

‘Nationaal referendum 21 maart 2018’

<<https://verkiezingsuitslagen.nl/verkiezingen/detail/NR20180321/667205>> accessed 16 February 2021

‘Nationale Politie voldoet aan last onder dwangsom’

<<https://autoriteitpersoonsgegevens.nl/nl/nieuws/nationale-politie-voldoet-aan-last-onder-dwangsom>> accessed 19 February 2021

‘Ontsluitplicht’

<<https://www.rijksoverheid.nl/documenten/rapporten/2019/07/03/tk-bijlage-4-ontsluitplicht>> accessed 19 February 2021

‘Studenten delen luiers uit als protest tegen surveillanceprogramma UvA’

<<https://www.parool.nl/amsterdam/studenten-delen-luiers-uit-als-protest-tegen-surveillanceprogramma-uva~b6aa57a0/>> accessed 12 February 2021

‘Taken en bevoegdheden’

<<https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/tasks-and-powers-dutch-dpa>> accessed 10 February 2021

‘Uitslag referendum over Wiv: meerderheid tegen’

<<https://www.kiesraad.nl/actueel/nieuws/2018/03/29/uitslag-referendum-over-wiv-meerderheid-tegen>> accessed 10 February 2021

‘Veiligheid en mensenrechten’

<<https://www.amnesty.nl/wat-we-doen/themas/veiligheid-en-mensenrechten>> accessed 14 February 2021

'Wetsvoorstel Computercriminaliteit III (Decryptiebevel En Andere Voorstellen)'
<<http://nicokwakman.blogspot.com/2013/05/wetsvoorstel-computercriminaliteit-iii.html>>
accessed 19 February 2021

'Wijziging Wiv 2017' <<https://www.internetconsultatie.nl/wiv2017/reacties>> accessed 13
February 2021

Case-law

Gerechtshof Arnhem-Leeuwarden, 3 December 2019, 200-256-387

Hoge Raad, 15 Februari 1977, C-68586 AC3994

Hoge Raad, 9 Januari 1987, 12/717

Hoge Raad, 27 April 2001, C99/243HR

Parket bij de Hoge Raad, 15 Februari 1977, 68586

Parket bij de Hoge Raad, 12 April 2002, C00-189HR

Raad van State, 4 Juni 2014, 201308060/1/A4

Rechtbank 's-Gravenhage, 21 November 2007, KG 07/1158

Rechtbank Amsterdam, 5 Januari 2018, 5560948 CV EXPL 16-34981, 5560970 CV EXPL
16-34982, 5603589 CV EXPL 16-36813, 5603605 CV EXPL 16-36814

Rechtbank Amsterdam, 12 Augustus 2019, 7728204 CV VERZ 19-9686

Rechtbank Amsterdam, 25 September 2019, AWB-18-7146

Rechtbank Amsterdam, 11 Juni 2020, C-13-684665-KG ZA 20-481

Rechtbank Den Haag, 26 Juni 2018, C-09-553023-KG ZA 18-476

Rechtbank Den Haag, 5 Februari 2020, C-09-550982-HA ZA 18-388

Rechtbank Den Haag, 5 Februari 2020, C-09-550982-HA ZA 18-388

Rechtbank Noord-Nederland, 12 December 2019, C18/190912 HA RK 19-19

Rechtbank Noord-Nederland, 12 December 2021, 8187989

ELSA NORTH MACEDONIA

Contributors

National Coordinator

Bojana Rusevska

National Academic Coordinator

Filip Ivkovski

National Researchers

Maja Veljanova

Jovica Dimitroski

Ivona Stojcevska

Elena Petkovska

National Academic Supervisor

Fani Dimoska

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

North Macedonia has ratified most international human rights instruments. The legal framework on the protection of fundamental rights is largely in line with European standards.

The Macedonian Institute for Media prepared a study as a part of the Project Macedonia in the digital age – between the rights and responsibilities while communicating on the Internet, financed by the US Embassy in Skopje. The study comes to the conclusion that North Macedonia is a signatory of the European Convention for the Protection of Human Rights and Fundamental Freedoms, so this document is directly applicable in the country. In accordance with article 118 of the Constitution, international treaties ratified in accordance with the Constitution are part of the international legal order and cannot be changed by law.⁹⁷⁶ Hence, in Macedonia, article 10 of the European Convention⁹⁷⁷ and the other international standards ratified by the Macedonian Parliament are directly applicable. Freedom of press and expression is guaranteed, and censorship is prohibited. In the context of the Criminal Code, this important part of the legislation in Macedonia covers the area of public communication on public platforms on the Internet that contain speech or incitement to violence and hatred. Hate speech is rarely explicit but often occurs in hidden form, combined with information from unidentified sources and information that are offered as facts, insult, slander, and so on. Implicit hate speech is not a regular practice, though it often appears on some online media, and is particularly visible in viral media/social networks, forums, as well as in user-generated content. The Criminal Code provides punishment for offenses related to hate in several articles – incitement of violent change of the constitutional order⁹⁷⁸(article 318), hate speech (art. 319, 417),⁹⁷⁹ and the penalty against the person who by using the information system publicly denies, roughly minimizes, approves or justifies genocide, crimes against humanity or war crimes (art. 407-a).⁹⁸⁰

The Criminal Code has provisions on hate crime through computer systems and, more recently, surveillance on digital communication in cases of organized crime, the country also has a Law for Protection of Personal Data,⁹⁸¹ which also shows its functionality in practice. North Macedonia has ratified the Convention on Cybercrime⁹⁸² more than a decade ago and shows results in the struggle against it. Macedonia has labor laws, laws on obligations, procedural law, etc.

With the development of the ADT other human rights issues are defamation and insult for published information on media and social networks as opposed to freedom of expression and freedom of speech. Insult is defined in article 6 of the Law of Civil Liability for insult and

⁹⁷⁶ Constitution of Republic of North Macedonia 8th September 1991, International relations, article 118.

⁹⁷⁷ European Convention on Human rights, Section 1: Human rights, article 10: freedom of expression, 3rd September 1953.

⁹⁷⁸ Criminal Code, Official journal of Republic of North Macedonia no. 37/96, 80/99, 4/2002, 43/03 , 19/04.

⁹⁷⁹ *ibid.*

⁹⁸⁰ *ibid.*

⁹⁸¹ Law for Protection of Personal Data, Official journal of Republic of North Macedonia no. 42/2020.

⁹⁸² Convention on Cybercrime ratified 15th September, 2004 in Budapest.

defamation.⁹⁸³ According to the Law for Civil Liability for Insult and Defamation, the Website shall not be considered responsible if the insult is made in serious criticism, in the exercise of the journalistic profession, in the defence of the freedom of public expression of opinion or other justified rights, or in the protection of the public interest or other legitimate interests, and if in the coverage of the humiliating opinion for the other it is concluded that: 1) from the manner of expression or from its other circumstances it turns out that it has no meaning of an insult; 2) it has not caused any significant damages to the honor and reputation of the person and 3) it has not been disclosed exclusively in order to humiliate the personality of others or to belittle his honor and reputation. Also, the Law foresees that there is no responsibility for insult if someone expresses a humiliating opinion for a holder of a public function in the public interest and if he proves that this is based on truthful facts, or if he proves that he had reasonable cause to believe in the veracity of such facts, or if the statement contains a justified critique or encourages a discussion of public interest or it is given in accordance with the professional standards and ethics of the journalistic profession. Liability for defamation should be determined in accordance with article 8 of the Law on Civil Liability for Insult and Defamation. In relation to civil liability for defamation, the one who is sued in a court procedure will need to prove the truthfulness of the facts contained in the assertions or in the text with an author. In the case of transferred news, text, or other content, if it is attributed, the Website which is sued will need to prove that it has been transferred and that it is not its author. In relation to providing evidence, it is sufficient to prove that there is a basic reason to believe in the veracity of the claims.

The implementation of legislation works well in some area, but deficiencies persist, which includes some serious problems, which have produced a culture of serious violations and discourage citizens and entities to use legislative instruments.

With the development of ADT several issues that can lead to the breaking of fundamental human rights have occurred. Although Advanced Digital Technology has its advantages, it has its drawbacks too. The development itself comes with data security issues, crime and terrorism, privacy concerns, digital media manipulation, plagiarism, copyright infringement, and many others. Thanks to its international nature the Internet has become a fertile territory for malevolent forces to operate. Regarding this, North Macedonia as well as every other country, following their main goals, should make sure that their citizens have their rights guaranteed and protected.

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

Personal information in North Macedonia is protected by the Law on Protection of Personal Data.⁹⁸⁴ The main purpose of the Law, among others, is the harmonization of the local legislation with EU legislation commonly known as the General Data Protection Regulation or 'GDPR', as well as the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data of the Council of Europe. Harmonization of legislation in personal data

⁹⁸³ Law for Civil Liability for Insult and Defamation, Official journal of Republic of North Macedonia no. 143/2012.

⁹⁸⁴ Law for Protection of Personal Data, Official journal of Republic of North Macedonia no. 42/2020.

protection has been one of the government's priority activities since 2002. The draft of a new law was made in 2018 for alignment with the EU GDPR and the final version was made in 2020.

In the Law on Protection of Personal Data a 'personal data' is defined as any information relating to an individual or legal entity that can be identified. A Person that can be identified is a person whose identity can be determined directly or indirectly, especially based on the personal identification number of the citizen or based on one or more characteristics specific to his physical, physiological, mental, economic, cultural or social identity.

According to personal data processing principles, personal data is processed if: processed legally And in a transparent manner concerning the data subject, collected for specific, explicit, and legitimate purposes, and not processed in an incompatible manner with those purposes. They are adequate, relevant, and limited to only what is necessary, kept in a form which permits identification of data subjects for no longer than is necessary and are processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage using appropriate technical or organisational measures.⁹⁸⁵

Measures that are implemented to ensure the security of processing are: the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, the ability to restore the availability to access to personal data on time in the event of physical or technical incidents, a process for regularly testing and ensuring the security of the processing. The controller and processor are supposed to take steps to ensure that any individual acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller unless he or she is required to do so by law.⁹⁸⁶ In case of a violation of personal data, the controller should without any delay, not later than 72 hours after becoming aware of it, notify the Agency about the personal data violation, unless it is unlikely to result in a risk to the rights and freedoms of the person. If the Agency is not notified within 72 hours, it should be accompanied by reasons for the delay. The controller and the processor can assign the protection to an entitled person if: the processing is carried out by a state administration body, except for courts acting in their judicial capacity, the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a bigger scale, the activities of the controller or the processor consist of processing on a large scale of special categories of data under Article 13 of the Personal data protection Law⁹⁸⁷ and personal data relating to criminal convictions and offences referred to in Article 14 of this Law. The controller or the processor are obligated to publish the contact details of the entitled person and inform the Agency about them. Personal data is also protected with the Regulation for Personal data processing.⁹⁸⁸ According to this regulation main values while protecting personal data are trustworthiness, integrity, availability, authentication, and

⁹⁸⁵ Guide on technology and privacy, February 2018 - Nina Ugrinovska (Directorate for Personal Data Protection.

⁹⁸⁶ Law for Protection of Personal Data, Official journal of Republic of North Macedonia no. 42/2020.

⁹⁸⁷ *ibid.*

⁹⁸⁸ Regulation on Personal Data Processing, 45/2001, EDPS

irrevocability. Other than the Law on Personal data protection, this issue is protected with: the regulation about the form and content of the forms for recognizing the transfer of personal data to other countries and way of keeping the records, regulation for the manner of performing inspection supervision, regulation on technical and organizational measures for providing secrecy and protection of personal data processing, regulation on the content and form of the act for the way of performing video surveillance and the manual on the manner of performing external control.

Transferring data. Entities may transfer personal data subject to processing if the conditions such as the level of protection, the respect of human rights, the existence of one or more independent supervisory authority are fulfilled. Transferring personal data to third countries or international organizations may be conducted only if the Data protection act considers the third country or international organization to provide adequate levels of protection. Although the Data Protection Law itself does not require special, prior approval by the Data Protection Act (Transfer Approval) if an adequacy decision issued by the Act for the (importing) third country or world organization exists or the below safeguards are provided (on condition that enforceable data subject rights and effective legal remedies for data subjects are available), up until this point in time, the Act has had a conservative approach and from its content we can conclude that even in such cases a Transfer Approval has to be obtained.

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?

3.1 Cooperation between private and public sector: relevant laws on data protection and legal apparatus for any violation

When it comes to cooperation between the public and private sectors, specifically on personal data protection, employers and employees are often the subject of discussions on the application of personal data protection laws. Whether or not employee privacy is protected by law, admiration for it is considered an added value in a company's work culture. The employer must process the personal data of the employees in accordance with the Law on Labour Relations (for example, with the article 35 in this law, is regulated the Obligation for the employee to keep a business secret, which means that any information that the employee finds out in his / her workplace and that information or data is considered as business secret, he / her must keep to him / herself and can not be used for his / her personal usage or benefit), the Law on Wages and Contributions and other laws on the basis of which it is established and operates. This, however, does not release him from the obligation to balance legal obligations and real needs. The employer must know who he is hiring, so he initially collects personal data contained in the CV (curriculum vitae) of the job candidates. He/she is then obliged to process data that are part of the employee's personal file and of course, must process personal data necessary for the calculation and payment of salary. Very often, video surveillance is installed in the official premises, for which there are special provisions in the Law on Personal Data Protection

(hereinafter in this research paper this Law will be referred with the abbreviation LPDP). Also, in the Law on Labour Relations mentioned above in this paragraph, the article 44 specifically regulates personal data of the employees (this article will be explained in detail in the following 3.2 section) and that personal data can only be used for the work needs of the employer, no difference if that employer is whole firm or just one person. Precisely, the employer can perform video surveillance in official or business premises if it is necessary for protection of life or health of people, protection of property, protection of life and health of employees directly to the nature of work or providing control over entering and leaving office or business premises. The employer must inform the employees about performing video surveillance in official or business premises. In many companies, certain processing of personal data is done on the basis of law, which gives employees the opportunity to exercise their rights. Whether in the public or private sector, all employers are the main controllers of their primary personal data collections and remain responsible for meeting the standards for technical and organizational data protection measures, including rules about access to their personal data.⁹⁸⁹ This legal system works for both sides of the working contracts, but only if those contracts are respected and esteemed: the employees can be protected by various laws for unwanted or illegal usage of their personal data and the employers can be secured with the same legal apparatus for any violation or breach of their business informations regarding to the section of business secrets.

3.2 Personal data exchange

The Law on Labor Relations has a particular article⁹⁹⁰ that regulates the protection of employees 'personal data, according to which employees' personal data can be collected, processed, used and submitted to third parties only if it is determined by this or another law or if it is necessary for the realization of the rights and obligations from the employment relationship or in relation to the employment relationship. Concerning the exchange of personal data of employees between state institutions, personal data of employees can be subject to exchange between certain state institutions only if there is a clear legal basis or if it is necessary to exercise other rights and obligations of the employer or the employee. In this regard, the Employment Agency, the Pension and Disability Insurance Fund, the Health Fund and the temporary employment agencies have the right to exchange certain categories of personal data on employees in the Republic of Macedonia, in accordance with the provisions of the LPDP. If it is a matter of publishing personal data on the Internet, the employer must obtain the express consent of the employees (personal data subjects) so that he can publish the personal data on the Internet or other internal networks of the employer. The controller should provide appropriate technical measures for confidentiality and protection of personal data processing, as follows: unique username, password created by each authorized person, composed of a combination of at least eight alphanumeric characters (of which at least one capital letter) and special characters, username and password that allows the authorized person to access the information system as a whole, individual applications and / or individual collections of personal data needed to perform

⁹⁸⁹ This article can be accessed on the following link: <https://www.dzlp.mk/node/2380>.

⁹⁹⁰ Law on Labor Relations, article 44, Official Journal of North Macedonia no. 62/2005.

his work, automated logout from the information system after a certain period of inactivity (not longer than 15 minutes), automated rejection of the information system after three unsuccessful login and antivirus protection attempts. In addition to technical measures, the controller should provide appropriate organizational measures for confidentiality and protection of personal data processing, such as measures for physical security of the premises and information and communication equipment where personal data are collected, processed and stored.

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

Is the right to data privacy defined in your legal system? If not, is it a part of another right protected by national law? Can the data subject restrict or object the data processing? What are the circumstances and exceptions to this option?

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 respect and protection of the privacy of personal and family life, dignity and reputation is guaranteed to every citizen.⁹⁹¹

Citizens have guaranteed protection from violation of their personal integrity which arises from the registration of their information through data processing.

4.1 The right to privacy in national and international framework in North Macedonia

In our country, the right to privacy is contained in many legal regulations and ratified conventions, where one of the most appropriate and precise definitions of protection of privacy can be found in the Universal Declaration of Human Rights⁹⁹² in Article 12 which stipulates that: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his or her honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. The explanation about the meaning of protection of privacy can also be found in the European Convention on Human Rights from 1950 contained in Article 8 which guarantees the right to respect for private and family life: Everyone has the right to respect for his private and family life, home and family and the correspondence. Public authorities must not interfere in the exercise of this right, unless such interference is provided by law and if it is a measure in the interest of state and public security, the economic well-being of the country, the protection of order and the prevention of crime, the protection of health and morals, or the protection of the rights and freedoms of others, in a democratic society.⁹⁹³

4.2 Circumstances for restriction in the usage of personal data

⁹⁹¹ Article 25 page 5 of the Constitution of the Republic of North Macedonia

⁹⁹² The abbreviated version of this Convention can be accessed on the following link:

<http://hrlibrary.umn.edu/edumat/hreduseries/hereandnow/Part-5/7_udhr-full.htm> accessed 11 February 2021.

⁹⁹³ European Convention on Human Rights, article 8, page 11, available at

<https://www.echr.coe.int/documents/convention_eng.pdf> accessed 11 February 2021.

As for the right to restrict the use of personal data, they can be used only in situations when:⁹⁹⁴

- The personal data subject has given permission for processing of his personal data for one or more specific purposes,
- Processing is required to fulfil the contract where the personal data subject is one of the contracting parties, or to take action at the request of the entity of personal data before its accession to the contract,
- The processing is necessary for fulfilling the legal obligation of the controller,
- The processing is necessary for the protection of the essential interests of the subject of personal data or to another natural person,
- The processing is necessary for performing works of public interest or when performing public authorization of the controller determined by law and
- Processing is required for the purposes of the legitimate interests of the controller or of another third party, unless such interests do not prevail over interests or fundamental rights and freedoms of the personal data subject who is seeking protection of personal data, especially when the personal data subject is a child.

4.3 Legal personal data protection

The LPDP stipulates the right of the subject for information regarding the identity of the controller, the purposes of processing personal data, users of personal data, legitimate interests about the processing the personal data, the obligation to provide answers to questions regarding the requests, possible consequences for unanswered answers and the existence of access to the controller for modification of personal data.⁹⁹⁵ All this is done with the prior consent of the entity that owns the personal data. The main body that acts on the misdemeanours in the field of personal data is the Personal Data Protection Agency and the subjects can submit a written request⁹⁹⁶ to the controller who is responsible for processing their data, ask for an insight into the data, and if necessary, change the data . The controller who processes the data, is obliged within 30 days to inform the entities that have requested inspection or change of whether and which their personal data is processed, for the purposes and legal basis of the processing of personal data, for the purpose and legal basis due to which their personal data are made available for use to other users, for the source of personal data, when they are collected and updated and for existing reasons for automatic data processing.⁹⁹⁷ If the entity re-submits the same or similar request for inspection of personal data, and in the meantime no changes have occurred, the controller (authority) has no obligation to respond to it. There is an exception to this rule: if more than six months have passed since the response of the controller from the day of submission for the previous request and if in the period of deciding about that particular demand, there has been no other requests or demands form the same entity, the controller

⁹⁹⁴ Law on Personal Data Protection, article 10, page 6, Official journal of Republic of North Macedonia no. 42/2020.

⁹⁹⁵ *ibid*, art 17-19.

⁹⁹⁶ The example about the structure of the request can be accessed on the following link:

<<https://dzlp.mk/mk/prizlnlp>> accessed 11 February 2021.

⁹⁹⁷ This article may be accessed at: <<https://dzlp.mk/mk/uvidzbr>> accessed 11 February 2021.

(authority) can still consider that no new significant changes have occurred. Also, when personal data are processed exclusively for scientific research or statistical purposes, the controller has no obligation to act upon the request for inspection. For supplementing, amending or deleting the personal data of the entity, the subject can submit a request only if the personal data are incomplete, inaccurate or out of date and if their processing is not in accordance with law and in case the controller determines that the personal data are incomplete, inaccurate or out of date, he is obliged to add, change or delete them and within 30 days from the day of submitting the request to notify in writing the entities that submitted the requests.⁹⁹⁸ Furthermore, when it comes to legal remedies, the subjects have the right to file a lawsuit to a competent court for damages in a court procedure against the controller of personal data collection, if he used them unauthorized, i.e. provided personal data for use or in any other way. The subjects can file, at any time, request for compensation of damages due to violation of the right to personal data protection against the controller, regardless of whether a violation of the right has been previously determined by the Personal Data Protection Agency or not.

4.4 Supervision over personal data protection

The Personal Data Protection Agency is also the supervisory body when it comes to supervision over personal data protection. This function is performed by supervisors for personal data protection, who also must have an official identification card given by the Agency. The supervisor can:

- look over general and individual acts, files, documents, computer files, information and other evidence in scope according to the subject of supervision or his / her request;
- inspects documents for personal identification according to the LPDP;
- can take control of the areas in which personal data is processing;
- can ask the controller for the usage of personal data and the purposes of it;
- provides evidence according to the subject of supervision and the needs for it etc.⁹⁹⁹

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

5.1. The most effective protection of databases in North Macedonian's legislation is judicial review. It is provided by the courts. There is situation where competence administrative body, in fact Personal Data Protection Agency does not provide enough effective review of protection data bases. It is so because court decisions have higher law. And also courts are charges to give the highest and effective protection of violated human rights. During conduct the review courts are obliged to respect key principles of constitutionality and legality , independence, impartiality and effective. They must to judge by law and to adherence on principle of trial within a reasonable time.

⁹⁹⁸ Law on Personal Data Protection, article 20 and 21.

⁹⁹⁹ ibis, article 105.

This procedure of review is initiated by a lawsuit pursuant to provisions of North Macedonian's Law of Civil Procedure. Judicial review of protection databases is regulated at Law of Regulated Data Protection from Articles 98-101

5.2. Judicial review on databases conducted by the courts is needed to be most effective in the context of their protection. It is then that the Agency conducts judgment for protection of data with aims. Law of effective protection on databases is mentioned at Art 98 of North Macedonian LRDP.¹⁰⁰⁰ Each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them, without prejudice to any other administrative or non-judicial remedy.

Without prejudice to any other administrative or non—judicial remedy, every data subject has the right to effective judicial protection, when the Agency in accordance with the competencies determined in Articles 65 and 66 of this Law has not acted upon the request or has not informed the personal data subject within three months for the outcome of the procedure upon the submitted request according to Article 97 of this Law.

In other words this judicial review occurs as a result of the Agency's falling to act at its competences and assignments certain at art 65. Or also Agency after submitted request don't offer sufficient protection, or review of data breaches. According to art 99 of Law, the data subject also has the right to an effective judicial remedy against a controller or processor. So, without prejudice to any available administrative or non-judicial remedy, including the right to submit a request to the Agency in accordance with Article 97 of Law, every data subject shall have the right to effective judicial protections when it considers that his or her rights personal data are used contrary to Law.

5.3. According to Art 99 of Law,¹⁰⁰¹ data subject also has the right to an effective judicial remedy. Each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them, without prejudice to any other administrative or non-judicial remedy. So there are value legal remedies those are regulated by Art 286¹⁰⁰², 337-341¹⁰⁰³ and 372-399.¹⁰⁰⁴ Legal remedy at civil procedure against holded court decisions can be regular or extraordinary. Regular remedies are appeal and objection.

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

When processing the data bases, it is possible to encounter some acts of different treatment toward certain persons on various grounds. This may appear discriminatory. Protection from discrimination during the processing databases is guaranteed at *Article 5 of LPDP* of North Macedonia.¹⁰⁰⁵ Protection of personal data shall be guaranteed to any natural person free of discrimination based on nationality, race, skin colour, religious belief, ethnic background, gender,

¹⁰⁰⁰ *ibid*, art 95.

¹⁰⁰¹ *ibid*, art 99.

¹⁰⁰² *ibid*, art 286.

¹⁰⁰³ *ibid*, art 337-341.

¹⁰⁰⁴ *ibid*, art 372-399.

¹⁰⁰⁵ *ibid*, art 5.

language, political or other beliefs, material status, origin by birth, education, social background, citizenship, place or type of residence, or any other personal characteristics of that person.

Different types of legal assets against discrimination of individuals are available such as criminal, civil, administrative nature or combined.

The most effective review against discrimination during data processing is judicial. Every individual who believes that a form of discrimination occurred during the processing of his or her data may apply to the primary court. Court holds this case according to rules that apply for civil procedure.¹⁰⁰⁶ It means that there is this procedure regarding civil courts. But at this point with claims seeking compensation there become competent primary courts with extended jurisdiction.¹⁰⁰⁷ If it is about dispute over claims value over 50.000, 00 EUR denar counter value. According to art 35 of Law on Civil Procedure on North Macedonia,¹⁰⁰⁸ local jurisdiction just as courts with basic competence in fact may to be competences court where discriminated person has residence. Where one of the sides at anti-discrimination judicial process is a legal entity than may competence is also basic court with extended jurisdiction.¹⁰⁰⁹

According to Anti-discrimination Law there are several types of claims against discrimination, just as basic claim (art.34),¹⁰¹⁰ actio popularis (art.35) and mutual action. With basic claims on discrimination may to seek 1) to determine that has violence of plaintiff's rights, 2) to prohibit taking actions those are harmful, ie it violates or may to break legal provisions, 3) to borrow defendant to take some actions, 4) to compensate damage done, and 5) to publish the dispositive of judgment where is determined discrimination. This seeks may to stand out with other requests if those are subject of civil procedure, and for that decide civil court.¹⁰¹¹ Then so called actio popullaris than may to apply by associations, syndicates, foundations and other non-formal groups whose activity contains from protection of discrimination if normally represents for many similar or ident cases. The complaint referred with this claim may be put forward in order to: 1) establish that the defendant has committed discrimination against the group whose interests are represented by the plaintiff, i.e. that the action the defendant has taken or overlooked may directly lead to discrimination against the group; 2) forbid activities that discriminate the group whose interests are represented by the plaintiff; 3) oblige the defendant to take actions that eliminate the discrimination or its consequences; and 4) publish in the media the operative part of the judgment establishing the discrimination in an accessible format at the expense of the defendant.¹⁰¹²

¹⁰⁰⁶ It refer to all valid provisions of Law of Civil Procedure of North Macedonia (Official Gazete No.79/05, 110/08, 83/09, 116/10, 124/15).

¹⁰⁰⁷ Anti-Discrimination Law, Ph.D. Lazar Jovevski, Ph.D. Zaneta Popovska, Organisation for Security and Cooperation with Europe, Skopje 2015.

¹⁰⁰⁸ art.35, Law on Civil Procedure of North Macedonia (Official Gazete No.79/05, 110/08, 83/09, 116/10, 124/15).

¹⁰⁰⁹ Anti-Discrimination Law, Ph.D. Lazar Jovevski, Ph.D. Zaneta Popovska, Organisation for Security and Co-operate with Europe, Skopje 2015.

¹⁰¹⁰ art.34, Law of Anti-Discrimination (Official Gazete No.258/20).

¹⁰¹¹ *ibid.*

¹⁰¹² *ibid* art 35.

The burden of proof is on the claimant's side. He is obliged to give facts and evidence that confirm discrimination.

At this court procedure third parties are possible to appear. It is often when most people are discriminated against by other grounds during data processed so than they apply with mutual assets, supported from one non-formal group or union, or organization. They simply seek. They can claim to have been discriminated against, to correlate with some organizations, groups, unions. For those parties are valid provisions on Law on Civil Procedure.

At the practice of Agency for Protection of Personal Data it is possible to make a certain algorithm bias. In fact those contain from non-processing of personal data or public announcement of sensitive and confidential data, or low level of safety of data, and unintended uses. This contributes the same individual to face big problems, like non-possibility to have access to some services, exercise of rights, and also discriminatory behaviour. Algorithm bias occurs as systematic and reliable errors at computer system where are stored personal data. Their consequences are also "systematic and unfair discrimination". Algorithmic bias has been cited in cases ranging from election outcomes to the spread of online hate speech. It has also arisen in criminal justice, healthcare, and hiring, compounding existing racial, economic, and gender biases. Which is quite a practice at north macedonian's institutions to marginalized populations.

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?

North Macedonia does not have specific regulations regarding big data, artificial intelligence, Internet of Things. Encryption is mentioned in several Macedonian laws. Primarily is the Law on Personal Data Protection, entirely aligned with the General Data Protection Regulation of the European Union ratified in 2020. Macedonia has an obligation to align its national legislation with the EU framework as it is a candidate country. Encryption is regulated in the Law on Personal Data Protection in several places.¹⁰¹³ First, under lawfulness of processing, it is mentioned that the controller shall take into account the existence of appropriate safeguards which may include encryption. Secondly, it is considered in the security of processing (security of personal data).

Finally, encryption is mentioned in the Communication of a personal data breach to the data subject.¹⁰¹⁴ The communication to the data subject shall not be required if the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as the encryption. Encryption of personal data is one of the data processors rights and responsibilities. Data processors must implement appropriate technical and organizational

¹⁰¹³ Law for Protection of Personal Data, Official journal of Republic of North Macedonia no. 42/2020.

¹⁰¹⁴ *ibid.*

security measures to protect personal data from accidental or unlawful destruction or loss. Encryption of personal data is considered as one of the possible measures.¹⁰¹⁵

Although these issues do not have specific regulations in our country, many companies participate in projects that could help the improvement of artificial intelligence, big data, the internet of things, and other advanced digital technologies and lead to placing them into our legal framework. Worth mentioning is The Chamber of Commerce for Information and Communication Technologies – MASIT.¹⁰¹⁶ MASIT represents the Macedonian Information and Communication Industry and promotes the business interests of ICT companies in order to promote and develop the ICT industry and business environment. This Chamber represents operating a wide range of ICT products and services in Macedonia and since its establishment in 2000, as a nonprofit and voluntary institution, has provided its member companies with access to information, education, legal advice, and promotion at domestic, regional, and international levels, with the aim of advancing and developing the ICT industry. MASIT cooperates regionally and internationally with other organizations and associations. It cooperates with all ICT Associations in the SEE region and is a member of the Balkan and Black Sea Cluster Network. On an international level MASIT has been a member of the World Information Technology and Services Alliance - WILSA since May 2005.¹⁰¹⁷ The vision of this Chamber is the growth of Macedonian ICT businesses as well as the development of ICT-related Legislation. MASIT participates in numerous projects and conferences that aspire to help the development and usage of artificial intelligence and other kinds of advanced digital technology as well as initiate to include them in a legal framework in North Macedonia. At the 16th Annual MASIT Conference called “Data as an asset” although the particularly important and crucial topic was the data, discussions included advanced digital technology such as big data, artificial intelligence, and the Internet of Things.

The top ten companies of this kind located in Macedonia are: Hyperlink InfoSystem, Devsy, Haselt, Axeltra, Netcetera, 3P Development, Cosmic Development, ITgma, CodeWell and CodeIt Solution. All of these companies include Artificial Intelligence in their everyday work. For example, they use AI, they develop software using AI or they simply dedicate their work to progressing AI.¹⁰¹⁸

North Macedonia does not have a specific legal framework for Big Data, Artificial Intelligence, and other ADT. However, the country, the companies, non-governmental organizations, and other private actors consistently expand the manners in which they can assist the development of these issues, as well as create a way in which providing regulations concerning them would become inevitable.

¹⁰¹⁵ *ibid.*

¹⁰¹⁶ <https://masit.org.mk/en/> - MASIT - Chamber of Commerce Website.

¹⁰¹⁷ *ibid.*

¹⁰¹⁸ <https://topsoftwarecompanies.co/macedonia-republic-of/ai-development/agencies/macedonia> - Top Software companies Website.

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

Decryption of messages is allowed under the Law of Criminal Procedure of The Republic of North Macedonia¹⁰¹⁹ and Decree for interoperability standards of Macedonian information magistral and rules of safety on informatically systems.¹⁰²⁰ Decryption of messages like an encryption is conducted by the respective telecommunication operator. The need to exist encryption and pseudonymisation of message contents, and also their decryption lies to safety some level of security of internal communication. That is a way to come closer to detect the actual situation. In doing so, the principles of legality and inviolability of privacy should be preserved when is decrypting some form of private communications. It is part of special investigation measures regulated by Criminal Procedure Law¹⁰²¹. During the performance of measures all human rights must be protected¹⁰²². Parts of conversations that contain confident content should not be disclosed. In the interest of investigation, the content of decrypted messages may to deliver to same institution. According to art 141 par 2 this personal datas may to used at other criminal proceedings, in accordance with law, or international policies Or criminal cooperation just as subject of criminal investigation is directly connected with other subject.¹⁰²³

In other cases competence institutions have the right to seek insight into the computer system where conduct private communication with apply on special measures. Special investigation measures on its default may to used for prescribed crimes act according to art 253 of Law of Criminal Procedure.¹⁰²⁴ Those measures may again prefer persons who are convicted for conduct some crime and other persons according to art 255 of Law.¹⁰²⁵ It also refers to a person who uses messages that need to decrypted, or make some copies, transfer etc. According to art 184 par 2 of North Macedonian Law of Criminal Proceeding competence institutions are obliged to combat destruction or exchange of basis from messages.¹⁰²⁶ The person who will not act according to orders of competence institutions of persons to deliver messages for decryption aims will be sanctioned. If the person who have messages that correlate with crimes that later need to be decrypted didn't deliver them then competence institutions may confiscate without a needed warrant according to art 96 of Law of Criminal Proceeding.¹⁰²⁷ Messages with high

¹⁰¹⁹ Code of Criminal Procedure of The Republic of North Macedonia (Official Gazette No.150/10, 100/12, 142/16, 193/16, 198/18).

¹⁰²⁰ Decree for interoperability standards of Macedonian information magistral and rules of safety on informatica systems (Official Gazette No.36/06).

¹⁰²¹ It refers to measuring intrusion into accomplished phone calls and other communications, art 252 par 1 point 6, Code of Criminal Procedure of The Republic of North Macedonia (Official Gazette No.150/10, 100/12, 142/16, 193/16, 198/18).

¹⁰²² It refer also of articles 262 (notice of concerned person), 264 (protection data bases), Code of Criminal Procedure of The Republic of North Macedonia (Official Gazette No.150/10, 100/12, 142/16, 193/16, 198/18).

¹⁰²³ This also applied to contains of private decrypted messages, art 141 par 2, Code of Criminal Procedure of The Republic of North Macedonia (Official Gazette No.150/10, 100/12, 142/16, 193/16, 198/18).

¹⁰²⁴ art. 253, Code of Criminal Procedure of The Republic of North Macedonia (Official Gazette No.150/10, 100/12, 142/16, 193/16, 198/18).

¹⁰²⁵ *ibid* art.255\.

¹⁰²⁶ *ibid* art 184.

¹⁰²⁷ *ibid* art 96.

confidentiality contains are not subject to their decryption. These decrypted messages may be surrendered to suspected, or accused person whose messages are, or their defense council, to find contra proofs that will fall accuse. Proofs that contained from decrypted messages contain are performed within evidentiary hiring.

As stated above decryption is performed under special software. For its enter is necessary special identifications. Those form as special identification cards, some symbols (username, numbers, signs), electronic signature or other forms of authentication.¹⁰²⁸

This body safety just some form of level protection under decryption and system maintenance, safety of communication, maintain regular transfer system etc. Decryption like an encryption is conduct with uses some technical form of bases. Every act of encryption or decryption need to be certified. And controllers who perform encryption need to have a special certificate for quality.¹⁰²⁹

The competence body for encryption, i.e. same operator for communication is obliged for the process of encryption, also and for decryption to notice Agency for Personal Data Protection.

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

Nowadays, the modern life of living and operating is more focused on digitalization than ever before. No matter how disruptive the technology might be, the application of the same is more cost efficient and leads us to gaining more by giving less. However, digitalization as such is challenging from a lot of perspectives and it makes it highly difficult to be tracked by someone who is now knowledgeable in the 'digital world'.

The North Macedonian authorities are operating with a lot of online tools designed for several purposes including but not limited to interactions with natural persons, that is citizens to publish verdicts publicly available to everyone on official websites of the authorities and etc. On the other hand, providers of services are designing online tools for interaction with their clients on daily basis in which they share a large volume of document that contain personal data. All modern trends are leading us to the key conclusion that more digitalization requires more protective measures for protection of the human rights, that is personal data.

9.1. General public's interest or personal data protection?

While on one hand we have the protection of human rights and on the other hand we are having the broader interest of the general public it is really difficult to be determined which importance prevails over the other. In this line, the authorities have been struggling with the Constitutional Court over one initiative for abolishment of several provisions related to disclosure of personal information for natural persons that have committed a criminal offence related to sexual freedom and morality committed against children. Namely, for the purposes of harmonization with the EU Law, North Macedonia has ratified the Protocols to the Convention on protection

¹⁰²⁸ <https://www.it.mk>

¹⁰²⁹ art.3, Decree for Necessary Equipment and system for keeping certificates and qualified certificates (Official Gazete No.36/06).

of the rights of the child,¹⁰³⁰ further to which it has undertaken measures for prevention of prostitution, pornography and other harmful acts towards children. One of these measures was the registry for people that have committed a criminal offence related to sexual freedom and morality committed against children (hereinafter referred to in as: the “Registry”).¹⁰³¹ A special law was adopted for the purposes of establishing the Registry.¹⁰³² The Registry contains the information for every individual that has committed such crime:

- name and surname,
- date of birth,
- address of residence,
- a criminal offense for which he/she has been convicted,
- duration of the fine,
- date of commencement of serving the sentence,
- date of termination of serving the sentence,
- changes during the serving of the sentence,
- date of release from serving a prison sentence,
- date of deletion from the register,
- photography; and
- note (if something additional needs to be disclosed).¹⁰³³

Considering that neither the Convention, nor any other state in the neighboring countries had such a registry this action draw the attention to the public. Further to this, Article 5 paragraph (2) and (3) that prescribed that the content of the Registry will be publicly available was challenged to be incompliant with the Article 18 of the Constitution of the country that prescribes that the protection, security and secrecy of the personal data is guaranteed to the citizens. However, while there were separate opinions in the Constitutional court itself and in lack of required majority for nullification of the paragraphs (2) and (3) of Article 5, the article remained in force.¹⁰³⁴

9.2. Court decisions and their publications online

¹⁰³⁰ Law on ratification of the Convention of the rights of the child, Official journal of the Socialist Republic of Yugoslavia, no. 150/1990 – Official journal of Republic of Macedonia, 1993; Law on ratification of the Facultative Protocol to the Convention for protection of the rights of the child for trade with children, prostitution and pornography, Official journal of Republic of Macedonia no. 44/2003, 3 July 2003; and Law on ratification of the Facultative Protocol to the Convention for protection of the rights of the child for the participation of children in armed conflicts, Official journal of Republic of Macedonia no. 44/2003, 3 July 2003.

¹⁰³¹ The registry may be accessed on the following link: <<http://www.registarnapedofili.mk/>>.

¹⁰³² Law on special register for persons that have been convicted with a final verdict for criminal offences for sexual abuse of minors and pornography, Official journal of Republic of Macedonia no. 11/2012 and 112/2014.

¹⁰³³ Article 4 of the Law on special register for persons that have been convicted with a final verdict for criminal offences for sexual abuse of minors and pornography, Official journal of Republic of Macedonia no. 11/2012 and 112/2014.

¹⁰³⁴ The separate opinion of the Constitutional Court may be found on the following link: <<http://ustavensud.mk/?p=14872>>.

Based on the Law on Management in the Movement of the cases in the courts¹⁰³⁵ the courts are obliged to publish the final decisions in the official website for publication of the same. While performing the publishing the court is entitled to disclose only the name and surname of the parties involved in the procedure and anonymize their address of residence, personal unique identification number and the personal data of all witnesses and injured parties. Based on the published final decisions following the adoption of this regulation, that is following 24.05.2020, it can be concluded that the courts are aligning their behavior and are compliant with the prescribed requirements in the above-mentioned law.¹⁰³⁶

9.3. Publications and practical experience from the Agency for personal data protection

The provisions of the new Law on Personal Data Protection prescribe that the Agency for protection of the personal data may publish online on its' website a decision, opinion or guideline adopted for a particular case from the practice. The Agency is obliged to anonymize and pseudonymizes such decision/ opinion/ guideline in order to protect the personal data of the involved parties in the particular case.¹⁰³⁷ So far, no publications have been performed in order to check the compliance of the regulatory body. The Agency has adopted a Strategy for the period 2017-2022 in which one of the main focuses that it wants to improve is the protection of the personal data in the modern era that is the digital economy, smart- living, e- government concepts and other related concepts that the societies are facing nowadays due to the rapid development of the digital technology.¹⁰³⁸

Based on the last issued Report for the operation of the Directorate for protection of personal data for 2019, 60% of the total cases initiated in front of the respective institution have been related to violation of protection of personal data online, that is more specifically on the social media (Facebook, Instagram, Snapchat, YouTube, Twitter, Tinder, xHamster and Yahoo). The nature of the cases has been related to matters that the Directorate should deal with and also some related to criminal matters that are out of the scope of the regulatory body. Further to this, the Directorate has concluded a Memorandum for cooperation with the Ministry of Internal Affairs for the purposes of cooperation and providing a full support to the citizens whose personal data has been violated in a harmful way.

The Agency for protection of personal data is a stakeholder in the protection of personal data that has a significant impact not only in the protection of the personal data but in educating the general public on their rights and the responsibilities of the processors. Only by knowing your rights you would be able to detect the violation of the same. Driven by this principle the Agency

¹⁰³⁵ Article 9 of the Law on Management in the Movement of the cases in the courts, Official journal of Republic of Macedonia no. 42/2020.

¹⁰³⁶ The following link contains access to some court decisions published following the adoption of the regulation: http://sud.mk/wps/portal/central/sud/odlukilut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfljo8zizdxNTAwsvA183ANCzQ0cfV0MPEIsYwsjMz0w_EpcDc304-iQD9IAUi_AQ7gaADVj0cBQfujCFkRhc8MkBcigW4wRyiw93ADKgh1NTR1tAg0MnEx1w8GmZGZW5CTmZxZ4pufkpgjH1ISVJqqX5AbGhphkGVakK6oCADGEdsn/p0/IZ7_6G4408K0LOHF70AUE15A8Q24D7=CZ6_6G4408K0LGPU70AMD0HT9J2826=LA0=Ejavadoc.action!seArchAction==/#Z7_6G4408K0LOHF70AUE15A8Q24D7.

¹⁰³⁷ Article 66 paragraph (7) and (8) of the Law on Personal Data Protection, Official journal of Republic of North Macedonia no. 42/2020.

¹⁰³⁸ The Strategy may be accessed on the following link: https://dzlp.mk/sites/default/files/dzlp_strategija_mk.pdf.

has tried to educate the general public by publications of several guidebooks/ materials on their official website.¹⁰³⁹ In addition to this, the Agency has also made the reporting of the violation of the protection of personal data more easier than in the past. Namely, individuals may report any abuse of their personal data either in paper or online. The online application is simple and easy to perform. The software also provides an option for attaching supporting documentation to the application which makes the whole process more time efficient and easy.¹⁰⁴⁰

Another interesting case that has raised the awareness for the importance of compliance of the institutions with the personal data protection was related to the system of the State Election Commission. Namely, following a large number of complaints directed to the Agency for personal data protection, the latter has performed an audit in the State Election Commission on 15.07.2020. In essence, the State Election Commission has been attaching and publishing personal data on Google Drive by using CloudFlare services and in that way has transferred personal data outside of the country. The State Election Commission has violated several provisions of the personal data protection regulation by failing to test and check the compliance of the technical features of the software for processing of personal data prior to commencement of using the same. Moreover, the State Election Commission has failed to undertake required measures for notifying/ obtaining approval for sharing of personal data on virtual data rooms outside of the territory of North Macedonia. In such a way, the Agency for Personal Data Protection had no other option by to issue guidelines and provide a specific deadline for correction of the behavior of the institution.¹⁰⁴¹

On a separate note, there has been a gap in the operation of the Directorate for Personal Data Protection from the period in which the Head of the regulatory body has resigned from the position until the election of the new one. During this period (from May- December 2019) the Directorate was not functioning properly and this has had a huge impact on the violation of the personal data during that period due to the incapability of the regulatory body to perform normally its' daily activities.

9.4. Private sector and personal data protection

While on one hand we are having the regulatory bodies that are part of the governmental engine that drives the protection of the personal rights, we are also having the private sector that needs to be compliant with the prescribed regulation for protection of personal data. Considering that the providers of services to natural persons, that is individuals are obliged to hold an authorization for processing of personal data of a certain individual it is highly important for them to be compliant with the regulation. We are all aware of the importance of the marketing, subscription alerts, promotion from service providers/sellers of goods to reach their targeted groups and offer their services/products. If in the past this was not subject to approval of the

¹⁰³⁹ Some general guidelines/ publications may be accessed on the following link:

<<https://dzlp.mk/mk/publications>>.

¹⁰⁴⁰ The online reporting of violation of personal data may be performed by accessing the following link:

<<https://dzlp.mk/node/3274>>.

¹⁰⁴¹ A short article related to the audit in the State Election Commission may be found on the following link:

<<https://mia.mk/vonrednata-supervizi-a-na-azlp-vo-dik-utvrđi-pove-e-povredi-na-propisite-za-zashtita-na-lichnite-podatoci/>>.

individuals, nowadays it has become a must and the private companies are “following this trend” and have adopted their internal regulations in such a manner that a special approval from the customer should be obtained for the same to be contacted in case of special offers that the company has to offer to him/ her.¹⁰⁴²

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?

In summary, personal data should stay personal to the large extent given the necessity of its protection. All stakeholders should understand the importance of personal information in order to protect it. Only by knowing the rights and responsibilities, each stakeholder would be able to perform its obligations or seek for protection of its rights. It is important to remember that by protecting personal data we also protect the fundamental rights and freedoms of every individual related to that data. While protecting personal data we ensure that their rights and freedoms aren't violated.

The general rule for incompliance applies in all areas and leads to adverse effects. While on one hand incorrect processing of personal data might lead to a situation where a person is overlooked for a job opportunity or losing their current job, on the other hand showing diligent care and promoting personal data protection may lead to positive outcomes for everyone.

10.1 From adoption to compliance

North Macedonia to a large extent has adopted the EU regulation for protection of personal data. Having the right and proper measures for protecting the personal data set in legally binding rules in several laws is the first step in the whole process. However, even having the best regulation without practicing of the law and auditing the implementation of the same leads nowhere.

The Council of Europe for 2020 in its last report comes to the conclusion that there are a lot of challenges that are yet to be faced in the future. While on one hand, the Council recognizes the improvement of the country in the adoption of the new regulation for protection of personal data, on the other hand it also stresses out concerns of the capabilities of the regulatory body that is entitled with the power to check the compliance of the main stakeholders. As indicated above, the regulatory body has not been able to perform its obligations during the period from May-December 2019 due to the lack of a new head of the regulatory body. The head of the regulatory body is the driving force in the same and in lack of such for a long period of time there is a lack of a “watch dog” that would take care for the implementation of the regulation. Having a stable, sustainable regulatory body is of key importance. The authorities should make sure that no such case happens again in the future. Moreover, there should be a transitional period in which the former head of the regulatory body would hand- over the function to the

¹⁰⁴² A sample of such specific approvals for processing of personal data for the purposes of provisions of marketing services, that is offers in case of special promotions and etc. may be found on the following link: <https://www.setec.mk/SetecClubCard/images/CCardIzjava.pdf>.

new one and would guide him/ her in the process of becoming an independent actor in the whole process.

The development of the regulation in the following years will need to follow the speed of the digitalization and find ways how to cope with the harmful acts and incomppliance of the stakeholders with the regulation related to the protection of personal data.

Conclusion

The protection of personal data, as stated above, in accordance with the definitions of the Universal Declaration of Human Rights and the European Convention on Human Rights and Freedoms, can be most effectively and quickly achieved through notification by the entity that considers his or her right has been violated, ie by submitting a request to the Agency and by submitting a lawsuit to the controller whom the entity considers to be responsible for processing his personal data, if he has not acted previously on the request submitted by the entity. There is currently no specific definition of the right to privacy of any kind of data according to our legislation and in our legal system, but according to the international framework that our country has accepted and ratified, the right to privacy is explained above in this paper according to the two definitions of the Universal Declaration of Human Rights and the European Convention on Human Rights. There is currently no specific definition of the right to privacy of any kind of data according to our legislation and in our legal system, but according to the international framework that our country has accepted and ratified, the right to privacy is explained above in this paper in the content of the two definitions of the Universal Declaration of Human Rights and the European Convention on Human Rights and Freedoms. While the Law on Personal Data Protection regulates on a high level, the definitions of personal data, which are part of personal data and information, further, this law also regulates legal remedies and the ways of reporting the violation of protection of personal data, as well as the rights of entities to restrict the use of their personal data.

Table of legislation

Provision in [native] language	Corresponding translation in English
Кривичен законик, член 318 Тој што со намера да го загрози уставниот поредок или безбедноста на Република Македонија, јавно или со ширење списи повикува или поттикнува на непосредно извршување или го поддржува извршувањето на делата од членовите 307 до 317, ќе се казни со затвор од три месеци до пет години.	Criminal Code, Article 318 One who intends to endanger the constitutional order or the security of The Republic of Macedonia, publicly or by disseminating writings, invites or encourages immediate execution or supports execution of offenses under Articles 307 to 317, shall be punished by imprisonment of three months to five years.
Член 18 од Уставот на Република Северна Македонија Се гарантираат сигурноста и тајноста на личните податоци. На граѓаните им се гарантира заштита од повреда на личниот интегритет што произлегува од регистрирањето на информации за нив преку обработка на податоците	Article 18 of the Constitution of the Republic of Northern Macedonia The security and confidentiality of personal data are guaranteed. The citizens are guaranteed protection against breach of personal integrity arising from registering information about them through data processing
Член 25 од Уставот на Република Северна Македонија На секој граѓанин му се гарантира почитување и заштита на приватноста на неговиот личен и семеен живот, на достоинството и угледот.	Article 25 of the Constitution of the Republic of Northern Macedonia Every citizen is guaranteed respect and protection of his privacy, personal and family life, dignity and reputation.
7. „Контролор“ е физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело, кое самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци, а кога целите и начинот на обработка на личните податоци се утврдени со закон, со истиот закон се определуваат контролорот или	"Controller" is a legal person, a body of state power, a state body or a legal entity established by the state to exercise public authority, an agency or another body, which independently or together with others determines the goals and the manner of processing of personal data, and when the purposes and manner of processing of personal data data are determined by law, the controller is determined by the same law or

посебните критериуми за негово определување;	the special criteria for its determination;
Член 37, Закон за заштита на личните податоци (Сл. весник на Република Северна Македонија 42/2020) (1) Во случај на нарушување на безбедноста на личните податоци, контролорот веднаш и не подоцна од 72 часа откако дознал за истото е должен да ја извести Агенцијата за нарушувањето на безбедноста на личните податоци, освен ако не постои веројатност нарушувањето на безбедноста на личните податоци да создаде ризик за правата и слободите на физичките лица. Кога известувањето до Агенцијата не е поднесено во рок од 72 часа, заедно со известувањето треба да биде доставено и образложение за причините за доцнењето. (2) Обработувачот е должен да го извести контролорот веднаш, откако дознал за нарушување на безбедноста на личните податоци. (3) Известувањето од ставот (1) на овој член, мора да го содржи најмалку следното: (а) опис на природата на нарушувањето на безбедноста на личните податоци, вклучувајќи, категориите и приближниот број на засегнати субјекти на личните податоци, како и категориите и приближниот број на засегнати евидентирани лични податоци; (б) наведување на името, презимето и контакт податоци на офицерот за заштита на личните податоци или на друго лице за контакт, од кое може да се добијат повеќе информации; (в) опис на можните последици од нарушувањето на безбедноста на личните податоци;	Article 34, Law on Personal Data Protection Article 37, Law on Personal Data Protection (Official Gazette of the Republic of Northern Macedonia 42/2020) (1) In case of violation of the security of personal data, the controller immediately and not later than 72 hours after learning about it is obliged to inform the Agency for the violation of personal data security, unless breach of personal data security is likely to create a risk to the rights and freedoms of individuals. When the notification to the Agency is not submitted within 72 hours, together with the notification should An explanation of the reasons for the delay should be submitted. (2) The processor is obliged to inform the controller immediately, after learning about the after learning of a breach of personal data security. (3) The notification referred to in paragraph (1) of this Article must contain at least the following: (a) a description of the nature of the breach of personal data security, including the categories and approximate number of personal data subjects concerned, as well as the categories and approximate number of records recorded; (b) an indication of the name, surname and contact details of the personal data protection officer or other contact person from whom more information may be obtained; (c) a description of the possible consequences of the breach of personal data security; violation of the security of personal data. (4) The information may be provided gradually without further unnecessary delay,

(г) опис на преземените или предложените мерки од страна на контролорот за справување со нарушувањето на безбедноста на личните податоци, вклучувајќи соодветни мерки за намалување на можните негативни ефекти. (4) Информациите може постепено да се обезбедат без понатамошно непотребно одлагање, само доколку не било можно целосно или дел од информациите да се поднесат истовремено. (5) Контролорот ги документира сите нарушувања на безбедноста на личните податоци, вклучувајќи ги фактите поврзани со нарушувањето на безбедноста на личните податоци, нивните последици и преземените активности за справување со нарушувањето, а со цел да и овозможи на Агенцијата да ја провери усогласеноста со овој член.	only if it was not possible to submit all or part of the information at the same time. (5) The controller shall document all violations of the personal data security, including the facts related to the violation of the personal data security, their consequences and the undertaken activities for dealing with the violation, in order to enable the Agency to check the compliance with this member.
Law on Labor Relations, Article 44 Protection of the employee's personal data. (1) Личните податоци на работниците можат да се собираат, обработуваат, употребуваат и доставуваат на трети лица само ако е тоа определено со овој или друг закон или ако е тоа потребно заради остварување на правата и обврските од работниот однос или во врска со работниот однос. (2) Личните податоци на работниците може да ги собира, обработува, употребува и доставува на трети лица само работодавачот или работникот, кого работодавачот за тоа посебно го овластил. (3) Личните податоци на работниците, за чие собирање не постои повеќе законска	Law on Labor Relations, article 44, Official Journal of North Macedonia no. 62/2005 (1) The personal data of the employees may be collected, processed, used and submitted to third parties only if it is determined by this or another law or if it is necessary for the realization of the rights and obligations from the employment relationship or in relation to the employment relationship. (2) The personal data of the employees can be collected, processed, used and submitted to third parties only by the employer or the employee, whom the employer has specially authorized for that. (3) The personal data of the workers, for the collection of which there is no longer a legal basis, must be immediately deleted and ceased to be used.

основа, мораат веднаш да се избришат и да престанат да се употребуваат.	
Article 10 Законитост на обработката на личните податоци (1) Обработката на личните податоци е законита, само ако и до оној степен доколку е исполнет најмалку еден од следните услови: - субјектот на лични податоци дал согласност за обработка на неговите лични податоци за една или повеќе конкретни цели, - обработката е потребна за исполнување на договор каде субјектот на лични податоци е договорна страна, или за да се преземат активности на барање на субјектот на лични податоци пред неговото пристапување кон договорот, - обработката е потребна за исполнување на законска обврска на контролорот, - обработката е потребна за заштита на суштинските интереси на субјектот на лични податоци или на друго физичко лице, - обработката е потребна за извршување на работи од јавен интерес или при вршење на јавно овластување на контролорот утврдено со закон, - обработката е потребна за целите на легитимните интереси на контролорот или на трето лице, освен кога таквите интереси не преовладуваат над интересите или основните права и слободи на субјектот на лични податоци коишто бараат заштита на личните податоци, особено кога субјектот на личните податоци е дете. (2) Одредбите од ставот (1) алинеја 6 на овој член нема да се применува за обработка на личните податоци од страна на органите на државната власт при спроведување на нивните надлежности. (3) Правниот основ за обработка на личните податоци наведен во ставот (1)	Law on Personal Data Protection, article 10, page 6, Official journal of Republic of North Macedonia no. 42/2020 Legality of personal data processing (1) The processing of personal data is legal, only if and to the extent that at least one of the following conditions is met: - the personal data subject has given consent for processing of his personal data for one or more specific purposes, fulfilling an agreement where the personal data subject is a contracting party, or to take action at the request of the personal data subject before its accession to the agreement, - the processing is necessary for fulfilling the legal obligation of the controller, - the processing is necessary for protection of the essential interests of the personal data subject or of another natural person, - the processing is necessary for performing activities of public interest or when performing public authorization of controller determined by law, - the processing is necessary for the purposes of the legitimate interests of the controller or a third party, except when such interests do not prevail over the interests or fundamental rights and freedoms of the personal data subject seeking protection of personal data, especially when the subject personal data is a child. (2) The provisions of paragraph (1) line 6 of this Article shall not apply to the processing of personal data by the state authorities during the exercise of their competencies. (3) The legal basis for personal data processing referred to in paragraph (1) lines 3 and 5 of this Article shall be determined by law. The law obligatorily provides provisions

алинеи 3 и 5 на овој член се утврдува со закон. Во законот задолжително се предвидуваат одредби за: условите кои ја одредуваат законитоста на обработката од страна на контролорот, целите на обработката, категориите на лични податоци кои се предмет на обработката, категориите на субјекти на личните податоци; субјекти на кои може да бидат откриени личните податоци, како и целите за кои се откриваат личните податоци, ограничувањата во однос на целите на обработка, периодот на чување, операциите и постапките за обработка, вклучувајќи и мерки за обезбедување на законска и правична обработка, а со Службен весник на РСМ, бр. 42 од 16.2.2020 година 7 од 70 цел да се исполни целта од јавниот интерес и да биде пропорционално на извршување на легитимната цел. Законот мора да содржи и процена на влијанието на заштитата на личните податоци за случаите предвидени во членот 39 од овој закон.

(4) Ако личните податоци се обработуваат за друга цел различна од целта за која првично биле собрани, при што обработката не се врши врз основа на согласност на субјектот на личните податоци или врз основа на закон, кој е неопходна и пропорционална мерка за заштита на целите утврдени во членот 27 став (1) од овој закон тогаш контролорот за да утврди дали обработката за други цели е во согласност со првичната цел за која биле собрани личните податоци, е должен меѓу другото да ги земе предвид: - секоја поврзаност помеѓу целите заради кои се собираат личните податоци и целите за предвидената понатамошна обработка, - контекстот во кој биле собрани личните податоци, особено во поглед на односите

for: the conditions that determine the legality of the processing by the controller, the objectives of the processing, the categories of personal data that are subject to processing, the categories of personal data subjects; entities to which personal data may be disclosed, as well as the purposes for which personal data are disclosed, restrictions regarding the purposes of processing, storage period, operations and processing procedures, including measures to ensure legal and equitable processing, and with the Official Gazette of RSM, no. 42 of 16.2.2020 7 of 70 goal to fulfill the goal of public interest and to be proportional to the performance of the legitimate goal. The law must also contain an assessment of the impact of personal data protection on the cases provided for in Article 39 of this Law.

(4) If the personal data are processed for a purpose other than the purpose for which they were originally collected, where the processing is not performed on the basis of consent of the personal data subject or on the basis of law, which is necessary and proportionate measure for protection of the objectives set out in Article 27 paragraph (1) of this Law, then the controller in order to determine whether the processing for other purposes is in accordance with the initial purpose for which the personal data were collected, is obliged to take into account, inter alia: which personal data are collected and the purposes for the envisaged further processing, - the context in which the personal data were collected, especially in the relations between the personal data subjects and the controller, - the nature of the personal data, and especially whether special categories of personal data are processed in accordance with Article 13 of this Law or personal data related to criminal

помеѓу субјектите на лични податоци и контролорот, - природата на личните податоци, а особено дали се обработуваат посебни категории на лични податоци согласно со членот 13 од овој закон или се обработуваат лични податоци кои се однесуваат на казнени осуди и казнени дела согласно со членот 14 од овој закон, - можните последици од предвидената понатамошна обработка за субјектите на лични податоци, - постоењето на соодветни заштитни мерки кои може да вклучуваат криптирање или псевдонимизација	convictions and criminal acts are processed in accordance with Article 14 of this Law, - the possible consequences of the envisaged further processing for the personal data subjects, - the existence of appropriate protection measures that may include encryption or pseudonymization
Article 17 (1) Кога личните податоци се собираат од субјектот на личните податоци, контролорот во моментот на собирањето на личните податоци, на субјектот на личните податоци му ги обезбедува следните информации: 1) идентитетот и контакт податоците на контролорот и податоци за неговиот овластен претставник во Република Северна Македонија; 2) контакт податоци за офицерот за заштита на личните податоци; 3) целите на обработката за коишто личните податоци се наменети, како и правната основа за обработката; 4) легитимните интереси што ги спроведува контролорот или трето лице, кога обработката се врши врз основа на членот 10 став (1) алинеја 6 од овој закон; 5) корисниците или категориите на корисници на личните податоци, доколку ги има; 6) каде што е применливо, фактот дека контролорот има намера да пренесе лични податоци во трета	Law on Personal Data Protection, article 17-19, page 11-13, Official journal of Republic of North Macedonia no. 42/2020 regarding the relations between the personal data subjects and the controller, - the nature of the personal data, and especially whether special categories of personal data are processed in accordance with Article 13 of this Law or personal data related to criminal convictions and criminal acts are processed in accordance with Article 14 of this Law, - the possible consequences of the envisaged further processing for the personal data subjects, - the existence of appropriate protection measures that may include encryption or pseudonymization 4) the legitimate interests pursued by the controller or a third party, when the processing is performed on the basis of Article 10 paragraph (1) line 6 of this Law; 5) users or categories of users of personal data, if any; 6) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization; as well as in case of transfer of personal data in accordance with Article 50 or Article 51 or Article 53 paragraph (1) second subparagraph

земја или меѓународна организација, како и во случај на пренос на лични податоци согласно со членот 50 или членот 51 или членот 53 став (1) втор потстав од овој закон, повикување на соодветните или прифатените заштитни мерки и начинот за добивање на копија од нив или информации каде истите се достапни. (2) Покрај информациите од ставот (1) на овој член, контролорот во моментот на собирањето на личните податоци, на субјектот на личните податоци му ги дава следните дополнителни информации кои се неопходни за обезбедување на правична и транспарентна обработка: 1) временскиот период за кој ќе се чуваат личните податоци, а ако тоа е невозможно, критериумите што се користат за одредување на тој период; 2) постоењето на право да се бара од страна на контролорот пристап, исправка или бришење на личните податоци или ограничување на обработката на личните податоци кои се однесуваат на субјектот на личните податоци, или право на приговор за обработката, како и право на преносливост на податоците;	of this Law, reference to the appropriate or accepted protection measures and the manner of obtaining a copy of them or information where they are available . (2) In addition to the information referred to in paragraph(1) of this Article, the controller at the moment of collecting the personal data, gives to the personal data subject the following additional information that are necessary for ensuring fair and transparent processing: 1) the time period for which the personal data will be stored, and if that is not possible, the criteria used to determine that period;
Член 43, Закон за заштита на личните податоци (Сл. весник на Република Северна Македонија 42/2020) (1) Офицерот за заштита на личните податоци ги врши најмалку следните работи: (а) ги информира и советува контролорот или обработувачот и вработените кои	The functions of the personal data protection officer are defined in article 43 of LPDP, page 29, Official journal of Republic of North Macedonia no. 42/2020 1) The personal data protection officer performs at least the following activities: (a) inform and advise the controller or processor and the staff performing processing

вршат обработка соодветно на нивните обврски според одредбите од овој закон; (б) ја следи усогласеноста со овој закон, со други засегнати закони кои се однесуваат на заштитата на личните податоци во Република Северна Македонија, како и со политиките на контролорот или обработувачот во однос на заштитата на личните податоци, вклучувајќи распределување на одговорности, подигнување на свеста и обучување на вработените кои што учествуваат во операциите на обработка, како и вршење на ревизии за заштита на личните податоци; (в) каде што е потребно, дава совети во однос на процената на влијанието на заштитата на личните податоци и го следи извршувањето на процената во согласност со членот 39 од овој закон; (г) соработува со Агенцијата; (д) дејствува како контакт точка за Агенцијата во однос на прашањата поврзани со обработката, вклучувајќи ја претходната консултација од членот 40 од овој закон, како и советување според потребите за сите други прашања. (2) При извршувањето на своите работи, офицерот за заштита на личните податоци ги зема предвид ризиците поврзани со операциите на обработката, како и природата, обемот, контекстот и целите на обработката.	in accordance with their obligations under the provisions of this Law; (b) monitor compliance with this Law, other relevant laws relating to the protection of personal data in the Republic of Northern Macedonia, as well as the policies of the controller or processor regarding the protection of personal data, including the allocation of responsibilities, awareness and training of employees participating in processing operations, as well as conducting audits for personal data protection; c) where necessary, provide advice regarding the impact assessment of personal data protection and monitor the execution of the assessment in accordance with Article 39 of this Law; (d) cooperate with the Agency; (e) act as a contact point for the Agency on matters relating to processing, including prior consultation referred to in Article 40 of this Law, as well as advising as necessary on all other matters. (2) In performing his / her duties, the personal data protection officer shall take into account the risks related to the processing operations, as well as the nature, scope, context and objectives of the processing.
Член 105, Закон за заштита на личните податоци (Сл. весник на Република Северна Македонија 42/2020) При вршење на супервизијата, супервизорот може да: - проверува општи и поединечни акти, датотеки, документи, компјутерски досиеја,	Law on Personal Data Protection, article 105, page 61, Official journal of Republic of North Macedonia no. 42/2020 In performing the supervision, the supervisor may: - checks general and individual acts, files, documents, computer files, information and

информации и други докази во обем според предметот на супервизијата, како и да побара и задржи копии од истите во хартиена или електронска форма без надоместок, - врши контрола во деловните или службените простории и други објекти каде што се врши обработка на личните податоци и бара увид во нивната обработка, - врши увид во документи за лична идентификација на лица поради потврдување на нивниот идентитет во согласност со закон, - бара од контролорот, односно обработувачот писмено или усно објаснување во врска со прашања од делокругот на супервизијата, - бара експертска анализа и мислење кога е тоа потребно за супервизијата, - употребува технички средства за фотографирање како и обезбедува видео записи кои можат да бидат искористени во супервизијата, - ја испитува опремата со која се врши обработка на личните податоци и опремата каде што се чуваат личните податоци, како и испитување на информацискиот систем и информатичката инфраструктура во рамки на кои се врши обработка на личните податоци, со овластен претставник на контролорот, односно обработувачот, - ги користи комуникациските уреди на контролорот, односно обработувачот заради исполнување на целите на супервизијата и - обезбедува други потребни докази според предметот на супервизијата.	other evidence in volume according to the subject of supervision, as well as to request and keep copies of them in paper or electronic form free of charge, acts, files, documents, computer files, information and other evidence in volume according to the subject of supervision, as well as to request and keep copies of them in paper or electronic form free of charge, - performs control in the business or official premises and other objects where the processing of the personal data is performed and requests insight in their processing, - inspects personal identification documents of persons for the purpose of confirming their identity in accordance with law, - requests from the controller, ie the processor a written or oral explanation regarding issues within the scope of supervision, - requires expert analysis and opinion when necessary for supervision, - uses technical means for photography as well as provides videos that can be used in the supervision, - examines the equipment with which the personal data processing is performed and the equipment where the personal data are stored, as well as the examination of the information system and the information infrastructure within which the personal data processing is performed, with an authorized representative of the controller, ie the processor, - uses the communication devices of the controller, ie the processor in order to fulfill the objectives of the supervision and - provides other necessary evidence according to the subject of supervision.

Закон за парнична постапка (Сл. весник на Република Македонија бр. 79/05, 110/08, 83/09, 116/10, 124/15):

Член 98

(1) Тужбата, одговорот на тужбата, правните лекови и другите изјави, предлози и соопштениеја што се даваат надвор од расправата се поднесуваат писмено, или по електронски пат до приемното одделение на надлежниот суд (поднесоци).

(2) Поднесоците задолжително треба да содржат адвокатски печат, освен оние кои се составени отстрана на полномошници определени во член 81 став (1) алинеи 2 и 3 од овој закон.

(3) Поднесоците мораат да бидат разбирливи и мораат да го содржат сето она што е потребно за да може да се постапи по нив. Тие особено треба да содржат означување на судот, име и презиме поткрепени со доказ за лична идентификација, живеалиште, односно престојувалиште на странките, односно фирмата и седиштето на правното лице запишани во Централниот регистар на Република Македонија или друг регистар поткрепени со доказ од соодветниот регистар, нивните законски застапници и полномошници, ако ги имаат, предмет на спорот, вредноста на спорот, содржина на изјавата и потпис на подносителот, односно електронски потпис, е-мил адреса и контакт телефон.

(4) Поднесоците поднесени од адвокати, државен орган односно орган на државна управа, единици на локалната самоуправа, правни лица и лица кои вршат јавни овластувања покрај податоците од ставот (3) на овој член треба да содржат и податоци за

Law on Litigation Procedure of North Macedonia (Official Gazette No.79/05, 110/08, 83/09, 116/10, 124/15)

Article 98

(1) The lawsuit, the response to the lawsuit, the legal remedies and other statements, proposals and announcements that are given outside the hearing shall be submitted in writing, or electronically to the reception department of the competent court (submissions).

(2) The submissions must contain a lawyer seal, except those that are composed by proxies determined in Article 81 paragraph (1) lines 2 and 3 of this Law.

(3) The submissions must be understandable and must contain everything that is necessary in order. In particular, they should contain a court designation, name and surname supported by proof of personal identification, place of residence of the parties, ie company and seat of the legal entity registered in the Central Register of the Republic of Macedonia or other register supported by evidence from the relevant register, their legal representatives and proxies, if any, the subject of the dispute, the value of the dispute, the content of the statement and the signature of the applicant, ie electronic signature, e-mail address and contact telephone number.

(4) The submissions submitted by lawyers, state body, ie state administration body, local self-government units, legal entities and persons exercising public authorizations, in addition to the data from paragraph (3) of this Article, should also contain data for electronic mailbox for delivery of written registered in accordance with the law.

електронско сандаче за достава на писмената регистрирано согласно со закон. (5) Странката во поднесокот е должна да го наведе својот единствен матичен број на граѓанинот, односно единствен матичен број на субјектот на уписот (ЕМБС) за правните лица. (6) Ако изјавата содржи некое барање, странката треба во поднесокот да ги наведе фактите врз кои се заснова барањето, како и докази кога тоа е потребно. (7) Изјавата што се дава со поднесокот може, наместо со поднесок, да се даде усно на записник, односно тонски запис кај парничниот суд.	(5) The party in the submission is obliged to state its unique personal identification number of the citizen, ie unique registration number of the registration subject (EMBS) for legal entities. (6) If the statement contains a request, the party shall state in the submission the facts on which the request is based, as well as evidence when necessary. (7) The statement given with the submission may, instead of a submission, be given orally to the minutes, ie audio recording at the litigation court.
Член 35, Закон за парнична постапка (Сл. весник на Република Македонија 79/05,110/08,83/09,116/10,124/15) (1) Во прв степен споровите ги суди совет или судија поединец. (2) Кога суди во прв степен, советот е составен од еден судија како претседател на советот и двајца судии поротници.	art.35, Law on Civil Procedure of North Macedonia (Official Gazette No.79/05, 110/08, 83/09, 116/10, 124/15) (1) In the first instance, disputes are adjudicated by a council or an individual judge. (2) When adjudicating in the first instance, the chamber is composed of one judge as president of the chamber and two lay judges.
Член 252 ст. 1, точка 6, Закон за Кривична постапка (Сл. весник на Република Македонија бр. 150/10,100/12, 142/16,193/16, 198/18) (1) Кога е веројатно дека ќе се обезбедат податоци и докази неопходни за успешно водење на кривичната постапка, како и податоци за лице кое е предмет на распишана меѓународна потерница кои на друг начин не можат да се соберат, може да се преземат следниве посебни истражни мерки: 1) следење и снимање на телефонските и другите електронски комуникации во постапка утврдена со посебен закон;	It refer to measure intrusion into accomplished phone calls and other communications, art 252 par 1 point 6, Code of Criminal Procedure of The Republic of North Macedonia (Official Gazette No.150/10, 100/12, 142/16, 193/16, 198/18) 1) When it is probable that the data and evidence necessary for the successful conduct of the criminal proceedings will be provided, as well as data on a person who is the subject of an international arrest warrant which cannot otherwise be collected, the following special investigative measures may be taken :

2) следење и снимање во дом, затворен или заграден простор што му припаѓа на тој дом или деловен простор означен како приватен или во возило и влез во тие простории заради создавање на услови за следење на комуникации; 3) тајно следење и снимање на лица и предмети со технички средства надвор од домот или деловен простор означен како приватен; 4) таен увид и пребарување во компјутерски систем; 5) автоматско, или на друг начин, пребарување и споредување на личните податоци; 6) увид во остварени телефонски и други електронски комуникации, 7) симулиран откуп на предмети; 8) симулирано давање и примање поткуп; 9) контролирана испорака и превоз на лица и предмети и одложување на приведување или одземање предмети; 10) користење на лица со прикриен идентитет за снимање, следење и собирање на информации или податоци и инфилтрирање во организирани криминални групи; 11) отворање симулирана банкарска сметка и 12) симулирано регистрирање на правни лица или користење на постојни правни лица за собирање на податоци и создавање услови за инфилтрирање. (2) Во случај кога не се располага со сознание за идентитетот на сторителот на кривичното дело, посебните истражни мерки од ставот (1) на овој член може да се определат и спрема предметот на кривичното дело.	1) monitoring and recording of telephone and other electronic communications in a procedure determined by a special law; 2) monitoring and recording in a home, enclosed or enclosed space belonging to that home or business premises marked as private or in a vehicle and entering those premises in order to create conditions for monitoring communications; 3) secret surveillance and recording of persons and objects with technical means outside the home or business premises marked as private; 4) secret inspection and search in a computer system; 5) automatic, or otherwise, search and comparison of personal data; 6) insight into realized telephone and other electronic communications, 7) simulated purchase of items; 8) simulated giving and receiving bribes; 9) controlled delivery and transportation of persons and objects and delay of apprehension or seizure of objects; 10) use of persons with concealed identities to record, monitor and collect information or data and infiltrate organized criminal groups; 11) opening a simulated bank account and 12) simulated registration of legal entities or use of existing legal entities for data collection and creation of conditions for infiltration. (2) In case when the information on the identity of the perpetrator of the crime is not available, the special investigative measures referred to in paragraph (1) of this Article may be determined in relation to the subject of the crime.

Член 262 Известување на засегнатото лице По прекинување на посебните истражни мерки, ако тоа не штети на постапката, по барање на засегнатото лице, јавниот обвинител ќе му ја достави писмената наредба. Засегнатото лице барањето може да го достави и до судот Член 264 Заштита на податоци во врска со посебните истражни мерки Лице кое на кој и да било начин дознае податоци што се однесуваат или произлегуваат од примената на посебните истражни мерки е должно да ги чува како службена тајна	It refer also of articles 262 (notice of concerned person), 264 (protection data bases), Code of Criminal Procedure of The Republic of North Macedonia (Official Gazete No.150/10, 100/12, 142/16, 193/16, 198/18) Article 262 Notification to the person concerned Upon termination of the special investigative measures, if it does not harm the procedure, at the request of the person concerned, the public prosecutor shall deliver the writ command. The person concerned may also submit the request to the court Article 264 Data protection in relation to special investigative measures A person who in any way finds out information relating to or arising from the application of special investigative measures is obliged to keep them as an official secret.
Член 141 Давање на личните податоци на корисници (1) Личните податоци собрани за потребите на кривичната постапка може да се даваат на користење на државни органи и други правни и физички лица само ако тоа е дозволено со закон. (2) Личните податоци од ставот (1) на овој член можат да се користат, во согласност со закон, во други кривични постапки, во постапка на меѓународна соработка во кривична материја и меѓународна полициска соработка, а во други судски постапки може да се користат само ако предметот во другата судска постапка е директно поврзан со предметот на кривичната постапка. (3) Личните податоци собрани исклучиво врз основа на утврдување на идентитетот,	This also applied to contains of private decrypted messages, art 141 par 2, Code of Criminal Procedure of The Republic of North Macedonia (Official Gazete No.150/10, 100/12, 142/16, 193/16, 198/18) Article 141 Providing personal data to users (1) The personal data collected for the needs of the criminal procedure may be allow the use of state bodies and other legal and natural persons only if it is allowed by law. \ (2) The personal data referred to in paragraph (1) of this Article may be used in in accordance with the law, in other criminal proceedings, in international proceedings cooperation in criminal matters and international police cooperation, and in others

телесен преглед или молекуларно-генетска анализа, по завршувањето на кривичната постапка можат да се користат, во согласност со закон, само заради откривање или спречување на кривични дела.	court proceedings may be used only if the case in another court procedure is directly related to the subject of the criminal
Член 3 (1) Ако поинаку не е договорено, одредбите од овој закон со исклучок на одредбите од членовите 4 и 12 не важат за затворени системи кои во целост се уредуваат со писмени спогодби меѓу познат број на договорни странки. (2) Правните или физичките лица можат односите во врска со податоците во електронски облик, електронските пораки и електронскиот потпис да ги уредат поинаку отколку што е определено со овој закон, ако од одделна одредба на овој закон или од нејзината смисла не произлегува нешто друго.	art.3, Decree for Neccesary Equipment and system for keeping cerificates and qualified certificates (Official Gazete No.36/06) Article 3 (1) Unless otherwise agreed, the provisions of this Law with the exception of the provisions of Articles 4 and 12 do not apply to closed systems that are fully governed by written agreements between known numbers of the contracting parties. (2) Legal or natural persons may have relations regarding the data in electronic form, edit emails and signature differently than specified herein law, unless something else arises from a separate provision of this law or its meaning.
ОД 2012 Член 4 Регистарот ги содржи следниве податоци за лица осудени со правосилна пресуда за кривичните дела од членот 3 од овој закон: - име и презиме, - датум на раѓање, - адреса на живеење или престојувалиште, - кривично дело за кое е правосилно осуден, - висина на казната, - датум на започнување на издржување на казната, - датум на прекин на издржување на казната, - промени во текот на издржување на казната,	Article 4 of the Law on special register for persons that have been convicted with a final verdict for criminal offences for sexual abuse of minors and pornography, Official journal of Republic of Macedonia no. 11/2012 and 112/2014. Article 4 The Register contains the following data on persons convicted by a final judgment for the criminal offenses referred to in Article 3 of this Law: - name and surname, - date of birth, - address of residence or stay, - a criminal offense for which he has been convicted, - amount of the fine,

- датум на отпуштање на издржување на казна затвор, - датум на бришење од регистарот, - фотографија и - забелешка. ОД 2014 Член 4 По членот 6 се додаваат два нови член 6-а и 6-б кои гласат: „Член 6-а Управата за извршување на санкции за лицата осудени со правосилна пресуда за кривичните дела од членот 3 од овој закон е должна во рок од 15 работни дена од денот на започнување на издржување на казна затвор, да достави до ЈУ Завод за социјални дејности копија од пресудата со која лицето е осудено за кривично дело, како и писмено известување со следните податоци: - име и презиме, - датум на раѓање, - адреса на живеење или престој, - кривично дело за кое е правосилно осуден, - висина на казната, - датум на започнување на издржување на казната, - датум на прекин на издржување на казната, - промени во текот на издржување на казната, и - датум на отпуштање на издржување на казна затвор. Член 6-б	- date of commencement of serving the sentence, - date of termination of serving the sentence, - date of commencement of serving the sentence, - date of termination of serving the sentence, - changes during the serving of the sentence, and - date of release from serving a prison sentence. Article 6-b The Ministry of Interior, for the person convicted with a final verdict for the criminal offenses from Article 3 of this Law, is obliged within 15 days from the day of submitting a written request to the PI Office for Social Activities to submit a photo from the date of commencement of support of the prison sentence and a photograph from the date of release from serving the prison sentence.

Министерството за внатрешни работи, за лицето осудено со правосилна пресуда за кривичните дела од членот 3 од овој закон, должно е во рок од 15 дена од денот на доставувањето на писмено барање на ЈУ Завод за социјални дејности да достави фотографија од датумот на започнување на издржување на казната затвор и фотографија од датумот на отпуштање на издржување на казната затвор. Фотографијата е во боја, со големина 3,5 x 4,5 см, и се менува на секои десет години.“	
Објавување на правосилни судски одлуки на веб-страницата на судот Член 9 (1) Овластениот судски службеник на првостепениот суд е должен во рок од седум дена од денот на правосилноста на судската одлука, односно од денот на доставување на одлуката од страна на повисокиот суд, да ја објави на веб-страницата на судот со име и презиме на странките, односно називот на правното лице, при што се анонимизира адресата на живеалиште, односно престојувалиште или седиштето на странките, единствениот матичен број на граѓанинот или единствениот матичен број на субјектот на упис и личните податоци на сведоците и општетените во постапката. (2) Овластениот судски службеник на повисокиот суд е должен во рок од седум дена од денот на верификацијата на правосилната судска одлука да ја објави на веб-страницата на судот. (3) Автоматизираниот систем генерира податоци за правосилни судски одлуки кои се објавуваат на веб-страницата на судот. (4) Во случаите кога јавноста е исклучена согласно со Уставот на Република Северна	Article 9 of the Law on Management in the Movement of the cases in the courts, Official journal of Republic of Macedonia no. 42/2020. Article 9 (1) The authorized court clerk of the first instance court is obliged to publish it on the website of the court with name and surname within seven days from the day the court decision enters into force, i.e. from the day of delivery of the decision by the higher court. of the parties, ie the name of the legal entity, whereby the address of residence, ie residence or seat of the parties, the unique identification number of the citizen or the unique identification number of the subject of registration and the personal data of the witnesses and the The authorized court clerk of the higher court is obliged to publish the final court decision on the court's website within seven days from the day of the verification. (3) The automated system generates data for final court decisions that are published on the website of the court. (4) In cases when the public is excluded in accordance with the Constitution of the

Македонија, законот и ратификуваните меѓународни договори во согласност со Уставот на Република Северна Македонија, судските одлуки без образложение се објавуваат на веб-страницата на судот. (5) Објавените кривични судски одлуки на веб-страницата на судот се бришат врз основа на донесено решение за бришење на правните последици од осудата, а другите судски одлуки се бришат по истекот на пет години од денот на нивното објавување. (6) Софтверското решение за објавување на судските одлуки на веб-страницата на судот содржи можност за нивно печатење, без да може да се врши менување, копирање и обработка на текстот на објавениот документ. (7) Начинот на објавување и пребарување на судските одлуки на веб-страницата на судот се уредува со упатство на Работното тело за стандардизација на постапките при користење на автоматизираниот систем во судовите.	Republic of Northern Macedonia, the law and the ratified international agreements in accordance with the Constitution of the Republic of Northern Macedonia, damaged in the procedure court decisions are published on the court's website without explanation. (5) The published criminal court decisions on the website of the court shall be deleted on the basis of a decision for deleting the legal consequences of the conviction, and the other court decisions shall be deleted after the expiration of five years from the day of their publication. (7) The manner of publishing and searching the court decisions on the website of the court shall be regulated by an instruction of the Working Body for standardization of the procedures when using the automated system in the courts.

Bibliography

English titles

Books

Guide on technology and privacy, February 2018 - Nina Ugrinovska (Directorate for Personal Data Protection)

Anti-Discrimination Law, Ph.D. Lazar Jovevski, Ph.D. Zaneta Popovska, Organisation for Security and Co-operate with Europe, Skopje 2015

Law and Information Technology, Goce Naumovski, Dragi Raskovski, Law Faculty Iustinianus Primus, university St.Chyrl and Metodius, 2014

Digital resources

<https://mk.voanews.com/a/miki-licni-podatoci-/4669467.htmltr>

<https://www.dzlp.mk/>

<http://ustavensud.mk/?p=14872>

https://metamorphosis.org.mk/wp-content/uploads/2019/08/Privacy-protection-and-media_mk.pdf.

<https://topsoftwarecompanies.co/macedonia-republic-of/ai-development/agencies/macedonia>

North Macedonian titles

Books

Водич за технологија и приватност, февруари 2018 година - Нина Угриновска (Дирекција за заштита на лични податоци)

Закон против дискриминација, д-р. Д-р Лазар Јовевски Занета Поповска, Организација за безбедност и соработка со Европа, Скопје 2015 година

Право и информатичка технологија, Гоце Наумовски, Драги Расковски, Правен факултет Јустинијан Први, универзитет „Свети Кирил и Методиј“, 2014

Digital resources

<https://www.dzlp.mk/>

<http://ustavensud.mk/?p=14872>

https://metamorphosis.org.mk/wp-content/uploads/2019/08/Privacy-protection-and-media_mk.pdf.

<https://topsoftwarecompanies.co/macedonia-republic-of/ai-development/agencies/macedonia>



The European Law Students' Association