ELSA LEGAL RESEARCH GROUPS

The European Law Students' Association

INTERNATIONAL LEGAL RESEARCH GROUP
ON HUMAN RIGHTS & TECHNOLOGY
VOL III

The European Law Students' Association
IRELAND

The European Law Students' Association
NORWAY

The European Law Students' Association
POLAND

The European Law Students' Association
TÜRKIYE

The European Law Students' Association
UKRAINE

International Legal Research Group on Human Rights and Technology

Vol. III

Reporting Countries:

ELSA Ireland

ELSA Norway

ELSA Poland

ELSA Turkey

ELSA Ukraine

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 Editor

Velina Stoyanova

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

Jodie McStay

National Academic Supervisors

Liam Sunner

Linguistic Editors

Emily Coffey

Technical Editors

Eithne Kavanagh

Jodie McStay

Researchers and Authors

Áine Harkin

Ciara O'Regan

Diarmuid Corcoran

Eithne Kavanagh

Hannah Arthurs

Katharina Neumann

Katie Ward

Lauren Dunne

Michael Ryan

Natasha Richardson

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 **11**

ELSA Ireland **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? 16

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 of data protection breaches? 22

5. Does the review constitute effective protection of data privacy? 26

6. What is the process of judicial review of anti-discrimination cases? 28

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? 31

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations? 34

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online? 36

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? 40

Conclusion 41

Table of legislation 43

Bibliography 72

ELSA NORWAY **80**

Introduction 81

1. Which human rights issues do Advanced Digital Technologies pose in your country? 81

2. How is personal information protected in your national legislation? 83

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? 87

4. What is the process of judicial review of cases data protection breaches? 90

5. Does the review constitute effective protection of data privacy? 92

6. What is the process of judicial review of anti-discrimination cases? 95

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? 99

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations? 102

9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online? 104

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? 107

Conclusion 109

Table of legislation 111

Bibliography 112

ELSA Poland **121**

Introduction 122

1. Which human rights issues do Advanced Digital Technologies pose in your country? 122

2. How is personal information protected in your national legislation? 123

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? 126
4. What is the process of judicial review of cases of data protection breaches? 132
5. Does the review constitute effective protection of data privacy? 139
6. What is the process of judicial review of anti-discrimination cases? 144
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? 147
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations? 153
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online? 154
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? 158
Conclusion 162
Table of legislation 163
Bibliography 172
ELSA TURKEY 175
Introduction 176
1. Which human rights issues do Advanced Digital Technologies pose in your country? 177
2. How is personal information protected in your national legislation? 179
3. To what extent is the data protection self-regulated by the private sector in your country? How do public and private sectors cooperate in this regard? 186
4. What is the process of judicial review of cases of data protection breaches? 187
5. Does the review constitute effective protection of data privacy? 189
6. What is the process of judicial review of anti-discrimination cases? 193
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? 195
8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations? 198
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online? 201
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? 204
Conclusion 206
Table of legislation 207
Bibliography 240
ELSA UKRAINE 247
Introduction 248
1. Which human rights issues do Advanced Digital Technologies pose in your country? 248
2. How is personal information protected in your national legislation? 255
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? 259
4. What is the process of judicial review of cases data protection breaches? 262
5. Does the review constitute effective protection of data privacy? 265
6. What is the process of judicial review of anti-discrimination cases? 269
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? 271

8. Does your country's legislation require encrypted personal messages to be decrypted and accessible for criminal investigations? 275
9. Has your country reached an adequate balance between allowing digital advancements and protecting human rights online? 278
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? 284
Conclusion 287
Table of legislation 290
Bibliography 336

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 Ireland

Contributors

National Coordinator

Jodie McStay

National Academic Coordinator

Liam Sunner

Director for Legal Research

Orla Murnaghan

National Researchers

Áine Harkin

Ciara O'Regan

Diarmuid Corcoran

Eithne Kavanagh

Hannah Arthurs

Katharina Neumann

Katie Ward

Lauren Dunne

Michael Ryan

Natasha Richardson

National Linguistic Editor

Emily Coffey

National Technical Editor

Eithne Kavanagh

Jodie McStay

National Academic Supervisor

Liam Sunner

Introduction

The aim of our National Research Group is to examine the Irish legal stance on Technology and Human Rights. In particular, this will focus on how a balance between the two positions can be achieved under national legislation. There are a range of aspects that need to be taken into consideration in order to get a comprehensive look at how this balance is achieved. This will be conducted through a critical analysis of both public and private regulations, while also addressing the issues in relation to the General Data Protection Regulation (GDPR) and other areas related to data protection. A particular focus will centre on the effectiveness of the remedies in place to deal with data and privacy breaches. Overall, we will discover how Ireland balances technological advances and human rights. This research will conclude with what changes (if any) need to be made to the national legislation as it currently stands.

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

Human Rights are the basic rights and freedoms that are afforded to each and every individual in the world regardless of gender, race or religion.[1] These rights are viewed as paramount, and therefore should be actively protected against any form of discrimination. International Law broadly defines basic human rights as the right to life, liberty, freedom of expression and opinion. This is extended across the civil, political, economic, and social landscapes. Every government must ensure legislative protections are in place to protect and promote the human rights of all their citizens.[2] According to the Human Rights Council, technology poses 'enormous potential and profound implications' in relation to human rights.[3] Technology, and in particular, its rapid advancement is seen as one of the most powerful tools when dealing with human rights, but like everything, it comes with its advantages and disadvantages. On one hand, technology, such as artificial intelligence, can vastly improve lives. On the other hand, the development of such technology, when paired with information of individuals, has a significant potential to impact human rights of not only the user but other members of the community.[4] Thus, the rapid growth of technology has given rise to issues surrounding the strength and adequacy of regulations and protections within the various legal systems. A comprehensive report drafted by the Council of Europe in 2019 outlines the challenges and issues that advanced technology

[1] Equality and Human Rights Commission, 'What are Human Rights?' (Human Rights, 19 June 2019) <https://www.equalityhumanrights.com/en/human-rights/what-are-human-rights> accessed 28 February 2021.

[2] United Nations, 'Human Rights' (What are human rights) https://www.un.org/en/global-issues/human-rights accessed 31 May 2021.

[3] Human Rights Council, Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights (2020) <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf> accessed 1 March 2021.

[4] Open Global Rights, 'How can technology be a powerful force in support of human rights?' (Technology and Human Rights, April 2018) <https://www.openglobalrights.org/technology/> accessed 1 March 2021.

poses in relation to the protection and vindication of human rights.[5] For example, the right to a fair trial, as protected by Article 6 of the European Convention on Human Rights (ECHR), has the potential to be compromised following developments and broad implementation in automated decision-making systems within legal systems. Another key area for conflict relates to the protections afforded the freedoms in relation to information, opinions and expression. In conjunction of these ever-evolving advancements in technology, comes new advantages. For example, with the creation and advancement of the various algorithms that control, change and categorise information availability online, comes with it new mechanisms in preventing hate-speech, bullying, and discrimination online. However, with every advantage comes the possibility of conflict and misuse. As such, it is essential that legal systems move with these changes to ensure it can provide adequate and effective protection to these new circumstances.

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

Irish Law protects personal information in multiple ways, including constitutional protections for information and privacy and European fundamental rights protections under the European Convention on Human Rights and Charter on Fundamental Rights under the EU. There are also protections provided for in legislation passed due to EU data law, and also specific privacy provisions in a number of laws. The Irish Constitution protects personal information through Article 40.3.2,[6] and Article 43,[7] the right to privacy and the right to the inviolability of the dwelling respectively. While the Irish Constitution does not have an expressed right to privacy in the text, it exists as a right derived from others.[8] Foundations for these rights include a link to expressed rights, rights stemming from the 'democratic nature of the state,' or a combination of the two.[9] Clauses which lead to the existence of such a right include personal autonomy, free association and protection of private property.[10] Privacy was first recognised as a derived right in McGee v Attorney General,[11] concerning a case where a married woman wished to import contraception into Ireland from the UK.[12] While the privacy right in the case was restricted to married couples, this was later extended to include an individual's right to privacy.[13] This was found to be derived from Article 40.3.2 of the Constitution,[14] which reads '[t]he State shall, in

[5] Council of Europe DGI (2-19) 05, 'A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework' <https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168096bdab> accessed 31 May 2021.
[6] Bunreacht na hÉireann (Irish Constitution), Article 40.3.2.
[7] ibid, art 43.
[8] Rónán Kennedy and Maria Helen Murphy, *Information and Communications Technology Law in Ireland* (2017), pp 137.
[9] *Friends of the Irish Environment v The Government of Ireland* [2020] IESC 49, para 31.
[10] Denis Kelleher, *Privacy and Data Protection Law in Ireland* (2nd edn, Bloomsbury 2016), pp 7.
[11] *McGee v Attorney General* [1974] IR 284.
[12] Oran Doyle and Tom Hickey, *Constitutional Law: Text, Cases and Materials* (2nd edn, Clarus Press 2019), pp 35-36.
[13] Kelleher (n 10), pp 8.
[14] Jeane Kelly & Aoife Treacy, 'Republic of Ireland' in Monika Kuschewsky, Van Bael & Bellis, *Data Protection & Privacy: Jurisdictional comparisons* (Thomas Reuters 1st edn 2012), pp 443.

particular, by its laws protect as best it may from unjust attack and, in the case of injustice done, vindicate the life, person, good name, and property rights of every citizen.'[15] The Irish Courts have also interpreted the Constitution as giving a right to privacy under Article 40.5.[16] It reads, 'the dwelling of every citizen is inviolable and shall not be forcibly entered save in accordance with law.'[17] Justice Hogan in Sullivan v Boylan held that Article 40.5 'protects the rights of the residents of a dwelling to security, protection against all-comers and privacy which are all necessary features of the inviolability of the dwelling.'[18] The facts of the case are instructive, the plaintiff was subject to a campaign of vicious harassment by a debt collector of the defendant, which Justice Hogan described as 'contemptible, irresponsible and outrageous.'[19] The Court held that this was in breach of the plaintiff's constitutional rights of personhood and the inviolability of the dwelling, and awarded damages on that basis. The inviolability of the dwelling was later cited by Justice Hogan in Schrems v Data Protection Commissioner.[20] Here the plaintiff was seeking a judicial review of the Data Protection Commissioner's decision not to investigate the plaintiff's allegation, arising out of Edward Snowden's NSA leaks, that there were no protections for data in America, and as, 'European Facebook user's data was transferred to the US by Facebook Ireland under the EU-US 'Safe Harbour' framework, that his and other users' rights were being violated.'[21] In obiter comments, Justice Hogan wrote of Article 40.5 and its influence on the constitutional order, 'it is very difficult to see how the mass and undifferentiated accessing by State authorities of personal data generated perhaps especially within the home...would pass any proportionality test or could survive constitutional scrutiny.'[22] Mulligan suggested that, traditionally, Article 40.5 operated to exclude people from the home without lawful authority.[23] In Schrems however, the right was found to provide protection for 'information in the home.'[24] Furthermore, Mulligan suggested that the analysis by Justice Hogan has added an informational privacy aspect to the right, which supplements its long established spatial element.[25] The relevance of the right of privacy to data protection is that the two are intimately connected, with Kennedy and Murphy noting, 'in some ways, data protection could be seen as a subsection of privacy law.'[26] While they note that in EU Law privacy and data protection are distinct legal rights,[27] in Irish Law privacy has been held to encompass personal information. A breach of privacy has been described by Justice Charleton as, 'the unwelcome intrusion of others into aspects of living

[15] Irish Constitution (n 6), Article 40.3.2.
[16] ibid, Article 40.5.
[17] ibid.
[18] *Sullivan v Boylan (no 2)* [2013] IEHC 104.
[19] ibid.
[20] *Schrems v Data Protection Commissioner* [2014] IEHC 310.
[21] Doyle and Tom Hickey (n 12), pp 427.
[22] ibid, pp 52.
[23] Andrea Mulligan, '*Case Comment: Constitutional Aspects of International Data Transfer and Mass Surveillance*' 2016 Irish Jurist 207.
[24] ibid.
[25] ibid.
[26] Kennedy and Murphy (n 8), pp 99.
[27] ibid.

that are particularly personal to the individual or into information shared in confidence.'[28] The Law Reform Commission wrote in its report on privacy that, 'at its core lies the desire of the individual to maintain control over information, possessions and conduct of a personal kind, and . . . to deny or control access thereto by others.'[29] The Irish Courts have recognised horizontal applicability of constitutional rights, meaning that those whose right to privacy have been violated can seek redress against private parties in the courts.[30] Remedies include monetary damages and injunctions for breaches of the right.[31] Two possible routes for determining breach of privacy discussed by McMahon and Binchy are, whether the breach is highly offensive to a reasonable person's ordinary sensibilities, or if the plaintiff had a reasonable expectation of privacy.[32] It will be interesting to see where the Irish Courts take their jurisprudence if a case revolving around the disregard for Constitutional protections for personal information is taken. Privacy is also considered a right under the European Convention on Human Rights (ECHR). Article 8 recognises a general right to private and family life. It is important to note that while the state is bound by the ECHR under International Law, this is not the case in domestic Irish Law.[33] Under the European Convention on Human Rights Act 2003,[34] all legislation interpreted by Irish Courts must be done in accordance with the convention. Furthermore, it requires that, 'every organ of the State shall perform its functions in a manner compatible with the State's obligations under the Convention provisions.'[35] The ECHR rights also play a role in the EU's legal order, meaning that EU Law applied in Ireland takes the ECHR into account.[36] Privacy is also protected within the EU by the Charter of Fundamental Rights, which includes provisions protecting privacy for individuals and families generally and personal data protection in particular, under Articles 7 and 8 respectively.[37] The Lisbon Treaty of 2009 requires that, 'the EU and its institutions must act in accordance with the EU Charter and Member States must comply with the Charter when implementing EU Law.'[38] The main legislation which gives rise to rights to data protection are the Data Protection Acts of 1988,[39] 2003,[40] and 2018.[41] The 1988 Act was passed to, 'give effect to the Council of Europe's Convention of 29 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data.'[42] This was later amended in the 2003 Act, which was passed to implement Directive 95/46/EC to protect individual's

[28] *EMI v DPC* [2012] IEHC 264.
[29] Law Reform Commission, *Report on Privacy* (LRC 1998), pp 24.
[30] Bryan McMahon and William Binchy, *The Law of Torts* (4th edn, Butterworths 2013), pp 1436.
[31] ibid.
[32] *Report on Privacy*, pp 1437-1443.
[33] Kennedy and Murphy (n 8), pp 138.
[34] European Convention on Human Rights Act 2003, s 2(1).
[35] ibid, s 3(1).
[36] Kelleher (n 10), pp 32.
[37] Kennedy and Murphy (n 8), pp 144.
[38] ibid.
[39] Data Protection Act 1988.
[40] Data Protection (Amendment) Act 2003.
[41] Data Protection Act 2018.
[42] Kelly and Treacy, pp 441.

data.[43] Under EU Regulation 2016/679, more commonly known as GDPR, the Oireachtas was required to pass the Data Protection Act 2018[44] to meet its obligation under the regulation.[45] Secondary legislation dealing with data protection include the ePrivacy Directive, derived from Directive 2002/58/EC.[46] Outside of the Data Protection Acts, there is legislation that contains privacy rights in specific situations, including *inter alia* the Mental Health Act 2001,[47] the Employment Equality Act 1998,[48] and the Adoption Act 2008.[49] The Oireachtas has not made a statutory right to privacy.[50] There have been previous attempts to pass a Privacy Bill with the intent of making breach of privacy a tort in Irish Law.[51] However this was dropped as the government pursuing the legislation lost office and no subsequent government has brought the legislation before the Dáil. While not the law in Ireland, it is of note that the legislation proposed included a provision that a disclosure of personal data under the aforementioned 1988 or 2003 Data Protection Acts would not constitute a violation of privacy.[52]

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 forms a vital part of the general protection of privacy as stated in Article 8 of The European Convention on Human Rights. GDPR ensures that an individual's privacy rights are protected when their data is processed, managed or stored by companies. The Data Protection Act was signed into law to give practical effect to GDPR in the Irish jurisdiction.[53] The processing of data is beneficial for both the private and public sector. The use of personal data by the private sector is for commercial benefit because data can be monetised and the company can use the data themselves or sell it on to other companies.[54] In contrast, the public sector tends to use data analysis to understand societal needs and improve existing processes in order to enhance government performance. There are three forms of regulation in relation to data protection: government regulation, self–regulation and co-regulation. Self-regulation is 'the possibility for economic operators,

[43] ibid.
[44] Data Protection Act 2018 (n 41).
[45] Sharon McLaughlin, '*Ireland: A brief Overview of the Implementation of the GDPR*' (2018) 4 Eur Data Prot L Rev 227.
[46] Kelly and Treacy, pp 441.
[47] Mental Health Act 2001, s 4(3).
[48] Employment Equality Act 1998, s 27(1)(a)(i).
[49] Adoption Act 2010, s 88.
[50] Kelleher, pp 27.
[51] Report on Privacy (n 29), pp 1444.
[52] ibid, pp 1446.
[53] Eoin Cannon, 'Data Protection Act 2018' (2018) 23(3) The Bar Review 79.
[54] Rebecca Kelly, Gerald Swaby 'Consumer Protection Rights and "Free" Digital Content' (2017) 23(7) Computer and Telecommunications Law Review 165-170.

social partners, non-governmental organisations or associations to adopt common guidelines amongst themselves'.[55] It has been argued that self-regulation has many benefits associated with it, including the fact that it is cheaper than government regulation, since companies can individually adapt to their own needs and thus be more efficient in the implementation of their own regulations.[56] Industry self-regulation of consumer data protection has been proposed as a flexible alternative to traditional government regulation.[57] When properly managed, self-regulation by the private sector can adapt quicker and more appropriately to innovations than government regulation.[58] In Ireland, the private sector does not have a *carte blanche* when regulating data. The GDPR and Data Protection Act 2018 provide for high standards of data protection and significantly affect how organisations collect, use and manage personal data that they collect.[59] Co-regulation encompasses initiatives in which the government and industry share responsibility for drafting and enforcing regulatory standards.[60] It is neither pure government regulation, nor pure industry self-regulation, but rather a hybrid of the two.[61] In Ireland, under the GDPR and the Data Protection Act 2018, there are statutory requirements outlined that must be adhered to by the private sector. Organisations follow this set of rules when drafting the documentation in order to show compliance with the legislation. Public regulation and enforcement are undertaken by national data protection supervisory authorities with the power to impose administrative fines.[62] In Ireland this authority is the Data Protection Commissioner (DPC). The DPC monitors the lawfulness of processing personal data by organisations.[63] Consequently, this model of data protection is not pure self-regulation since the DPC retains an important role in reviewing and supervising an organisation's co-operation and compliance with legislation. Additionally, it is not a pure government regulation since the individual organisations, not the regulators, draft the detailed rules and standards that will govern their members in relation to data protection. Therefore, in

[55] Ana Isabel Segovia Domingo and Nathalie Desmet Villar, "Self-Regulation in Data Protection" [2018] BBVA Research <https://www.bbvaresearch.com/wp-content/uploads/2018/10/Watch_Self-regulation-and-data-protection-1.pdf> accessed 12 March 2021.
[56] ibid.
[57] Siona Listokin, 'Industry Self-Regulation of Consumer Data Privacy and Security' (2016) 32(1) John Marshall Journal of Information Technology 15-41.
[58] ibid.
[59] Gordon Wade, 'The Insurability of Fines and Sanctions Under the GDPR' (2018), 36(18) Irish Law Times 280.
[60] Dennis D Hirsch 'The Law and Policy of Online Privacy: Regulation, Self – Regulation or Co – Regulation?' (2011) 34 Seattle University Law Review 439-480.
[61] ibid.
[62] Eoin O'Dell 'Compensation for Breach of the General Data Protection Regulation' (2017) 40(1) Dublin University Law Journal 99.
[63] Data Protection Act 2018 (n 41), s 12(2).

Ireland, the approach taken towards data protection is a co-regulatory model. The GDPR emphasises the need for organisations to be accountable in their data processing operations and to keep a record of their processing practices.[64] This means that detailed internal data protection policies and procedures must be adopted to illustrate the processor's processing practices and to document any decision making reasoning relating to personal data.[65] An organisation must also be able to show the security measures in place in the event of a breach.[66] Article 30(2) of the GDPR requires processors to keep an up to date record of all processing activities carried out on behalf of a controller.[67] Firms must maintain records if their processing occurs on a regular basis or if their processing includes special categories of sensitive data described in Article 9 GDPR.[68] Security measures are also provided for in the Data Protection Act 2018 as Section 72 requires that a controller shall ensure that the measures provide a level of security appropriate to the harm that might result from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the data concerned.[69] Under the Data Protection Act 2018, all data must be processed lawfully and fairly and the processing shall not be excessive in relation to the purposes for which it is processed.[70] In Ireland, an organisation must have an explicit and legitimate reason for the processing of an individual's data and it cannot be done arbitrarily. A key element of the GDPR is a 'risk-based' approach to data protection. In Ireland, there is no standard content that a data protection policy must have. However, it should include high-level principles and rules for the firm regarding data processing and it is also essential to be aware of the mandatory periods of data retention. In the event of a breach, a firm should carry out an immediate risk assessment, as time is of the essence with certain breaches needing to be reported to the DPC within 72 hours.[71] While an organisation has discretion in the method chosen to draft documents and policies showing compliance with the relevant legislation, there remains strict criteria that they are bound by, showing that this is a co-regulatory system. It is vital that both the private and public sector comply with their obligations as controllers. Section 141 of the Data Protection Act gives details of the fines that can be imposed by the DPC in relation to

[64] Laura Dietschy 'GDPR Series: New Obligations on Data Processors' (2018) 18(4) Privacy and Data Protection, pp 6-8.
[65] ibid.
[66] ibid.
[67] Data Protection Act 2018 (n 41), pp 7-8.
[68] Sarah Shyy 'The GDPR's Lose - Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business' (2019), 20 UC Davis Business Law Journal 156.
[69] Data Protection Act 2018 (n 41), s 72.
[70] Data Protection Act 2018 (n 41), s 71.
[71] General Data Protection Regulation 2018, Article 33.

breaches of data privacy law.[72] In imposing fines, the DPC shall act in accordance with Article 83 of the GDPR which outlines that fines of up to €20 million or 4% of worldwide turnover, whichever is higher, may be imposed.[73] Article 83 is instructive in outlining what factors should be taken into account in determining the seriousness of the breach of data protection and the level of fine to be imposed.[74] It was suggested that the public sector be exempted from paying such fines in the event of a breach.[75] However, concerns were expressed by the DPC regarding these exemptions as higher standards are arguably demanded from public sector bodies.[76] As a result of these concerns, the DPC can impose administrative fines of up to €1 million on public bodies that are not in competition with private sector bodies.[77] Additionally, data subjects can, pursuant to Article 82 GDPR, claim compensation from controllers or processors for damage suffered from infringements of the GDPR.[78] Therefore, compliance with the GDPR is ensured through a combination of public and private enforcement that blends public fines with private damages.[79] To conclude, individual organisations draft the documentation containing the detailed rules and standards that will govern their members in relation to data protection. However, in Ireland, both public and private sector organisations are ultimately bound by the GDPR and Data Protection Act 2018. Additionally, the DPC reviews documentation and ensures compliance with legislation and this limits the extent to which data protection is self - regulated by the private sector in Ireland. It is essential that organisations cooperate and fully comply with the legislation and statutory requirements to avoid fines for breaches of their obligations.

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

The main piece of legislation that governs data protection in Ireland is the Data Protection Act 2018, which was introduced as part of transposing the GDPR and ePrivacy Regulations.[80] Personal data is defined within the act and relates to data of a living individual, who is or can be identified from the data in question.[81] The law governs all situations where personal data is processed except where it is processed by an individual

[72] Data Protection Act 2018 (n 41), s 141.
[73] Report on Privacy (n 29), pp 79-80.
[74] Report on Privacy (n 29).
[75] ibid.
[76] ibid.
[77] ibid.
[78] Hirsch (n 61).
[79] ibid.
[80] S.I No. 336/2011 European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011.
[81] ibid (n 79), s 2(2).

for a 'purely personal or household' activity with no connection to any professional or commercial activity.[82] Once a data protection breach is suspected and has not been resolved by the DPC, a mechanism that can be triggered, whereby the breach can be reviewed by the judiciary which is encapsulated within the legislation.[83] It is also an offence for unauthorised disclosure by a processor and if found to have knowingly or recklessly disclosed data unlawfully they may be liable for a fine or imprisonment. [84]

4.1 The right to data privacy has defined in Ireland

Data privacy is not explicitly defined in the Irish legal system, it is however recognised as falling under the remit of privacy, which is found in the Constitution, case law, and in legislation. The right to privacy was recognised in the Courts in a series of cases Norris, In Re a Ward of Court (No. 2), and Fleming, which through an interpretation of the Irish Constitution established privacy as a fundamental unenumerated right.[85] Additionally, as mentioned above, the right to privacy is addressed in relation to Article 7 and 8 of the Charter of Fundamental Rights of the European Union.

4.2 Restriction and objection to data processing

For an organisation to lawfully process personal data, they have to be able to show it is for a lawful purpose. Under GDPR, these reasons are consent, to carry out a contract, in order to meet a legal obligation, where processing the data is necessary to protect the vital interests of a person, where processing the personal data is necessary for the performance of a task carried out in public interest, and finally in the legitimate interests of a company/organisation (except where those interests contradict or harm the interests or rights and freedoms of the individual).[86] It is important that a controller is aware of the legal basis under which they are processing data. The GDPR regulation also states that a person has a right to object to the processing of information when in connection with tasks that are:

1. In the public interest;
2. Under official authority;
3. In the legitimate interests of others.

---

[82] An Coimisiún um Chosaint Sonraí (Data Protection Commission) 'Commonly Asked Questions about the Basics of Data Protection' (version updated July 2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190710%20Data%20Protection%20Basics.pdf> accessed 19 February 2021.

[83] S.I No. 526/2008 European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008.

[84] Data Protection Act 2018 (n 41), s 144.

[85] See *Norris v Attorney General* [1984] IR 36, *In Re a Ward of Court (No.2)* [1996] 2 IR 79, *Fleming v Ireland* [2013] IEHC 2; [2013] 2 IR 417.

[86] Article 6(1) 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).

In relation to direct marketing, a person can object to processing at any time and the data controller must stop processing the data immediately. In order to have data processing stopped, the data subject must make a complaint to the data controller, specifying the grounds of the objection. The controller must either cease processing or respond to the data subject with a legitimate reason as to why the processing of such data must continue. Website owners and third-party services must obtain consent to allow cookies to process data, unless 'that cookie or technology is strictly necessary to provide the user with the service which they have requested'.[87] There is a restriction on the right of the data subject to object to data processing when such processing is for election purposes and processing by the Referendum Commission.[88] The data subject is not able to object to processing when it is deemed to be in pursuit of important objectives of general public interests, as stated in Article 60 of the Data Protection Act.[89] These general interests include, but are not limited to, safeguarding cabinet confidentiality,[90] tax administration,[91] and 'the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties'.[92] However, any restriction must be necessary and proportionate.[93] Another specific area wherein the data subject's right to restrict processing is altered is in relation to the processing of data for scientific or historical research purposes or statistical purposes. If the restriction requested by the data subject is likely to render impossible, or seriously impair, the achievement of those purposes, their request can be denied.

4.3 Process for notification of a breach

As per the Data Protection Act 2018,[94] a data breach is one that involves a person (or body) who, without authority of the controller or processor, obtains personal data and discloses the data or information to another person.[95] When a data processor becomes aware of a personal data breach, they are required to make the controller (on whose behalf the data was being processed) aware of the breach in writing and without undue delay.[96] The processor must also notify the DPC of the breach within 72 hours of becoming aware thereof. A 'data controller' means a person who either alone or without others controls and uses the personal data. However, this does not apply when 'taking into account the nature of the personal data and the scope, context and purposes of the processing, the personal data is unlikely to result in a risk to the rights and freedoms of data subjects.'[97] Where there has been a breach and the controller deems there is a high risk to the rights and freedoms of the data subject, they must notify whomever the breach relates to without undue delay.

[87] ibid (n 81), pp 8.
[88] Data Protection Act 2018, s 59.
[89] ibid, s 60.
[90] ibid, s 60(3)(a)(i).
[91] ibid, s 60(3)(a)(iii).
[92] ibid, s 60(3)(a)(ii).
[93] ibid, s 60(3)(a).
[94] ibid.
[95] ibid, s 144.
[96] ibid, s 85.
[97] ibid, s 86(3).

The notification must be in clear, plain language, describe the nature of the personal data and the breach, as well as at least, the effects of the breach, and the measures that have been taken to mitigate any adverse effects of the breach.[98] The Data Protection Act 2018 also explicitly states a right to effective judicial remedy, whereby on hearing the case the Court has the ability to annul the decision, substitute its own determination or dismiss the appeal. This process is available to the controller, the data subject and the DPC. However, if either the data subject or controller feels that the DPC is not complying with a complaint, they may also apply for a court order.[99] Such cases may be heard in the Circuit Court or the High Court, however, if any issue of law arises, the case may be brought to the High Court or Court of Appeal.[100] There are certain incidents where the data subject does not need to be notified and these are contained in Section 87 of the Data Protection Act 2018.[101] In general a data subject must be notified 'where a personal data breach has occurred, that is likely to result in a high risk to the rights and freedoms of a data subject', subject to subsection (2),(4) and (7).[102] In such instances, the controller must notify, without due delay, the data subject unless, they have implemented an appropriate technological and organisational protection measure that would render the data unintelligible to any unauthorised person.[103] Also if the controller has taken measures since a personal data breach that means that the risk to rights and freedoms of the data subject are no longer likely to materialise they do not have to notify the data subject.[104] If there was a situation where a notification was to involve a disproportionate effort from the controller, they do not need to notify the data subject directly but can notify by ways of a public communication or similar method. If this method is taken by the controller, they must ensure that the informing of the data breach is done in an equally effective manner to directly notify.[105] If the controller proceeds with a public communication, they must also notify the Data Commission and if the Commission deem the communication unsatisfactory can advise the controller to contract the data subject through other means.[106] The Data Protection Act 2018 explicitly states the controller may only restrict the right of a data subject to be notified 'where to do so constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and legitimate interests of the data subject'.[107] Where the decision is made by the controller it is important that all decisions made are not made in any arbitrary way. The decision process must be authentic and have the ability to be scrutinised to ensure a consistent application of the law and ensure the rights and freedoms of the data subject are respected and ensure the continued effectiveness of safeguards.

[98] ibid, s 86 - s 87.
[99] ibid, s 150.
[100] ibid.
[101] ibid.
[102] ibid, s 87(1).
[103] ibid, s 87(2)(a).
[104] ibid, s 87(2)(b).
[105] ibid, s 87(4).
[106] ibid, s 87(6).
[107] ibid, s 87(7).

4.4 Conclusion

While Article 8 of the Charter of Fundamental Rights of the European Union, does not specify that judicial oversight is explicitly needed in regard to the oversight of data protection, it has been interpreted that the principle of legality must have safeguards built in.[108] The Irish judiciary takes a strong view of judicial oversight, especially where there is the potential for breach of a fundamental right, an example of this can be found in Damache.[109] The legislation that has been enacted here in Ireland reflects the protections that were put in place, in particular as a response to the concerns enunciated in the Grand Chamber in the Digital Rights case,[110] as well as to bring Ireland in line with its EU counterparts.

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

5.1 The process of the review and the bodies conducting this process.

Section 117(1) of the Data Protection Act 2018 states that a data subject who considers their data protection rights to have been infringed can bring a 'data protection action' against the data controller or processor who is alleged to have infringed these rights. Concurrent jurisdiction lies with the Circuit Court and the High Court to determine these data protection actions.[111] As this is an action founded in tort,[112] it has been suggested the rules of negligence should apply to these cases of data breaches.[113] Therefore, the data subject must prove that the data controller or processor has breached its obligations under the GDPR and that this breach has actually and legally infringed the data subjects' rights.[114] The data subject must also establish the four elements of the tort of negligence to have a successful case. Therefore, there must be a duty of care, breach of the standard of care, causation and damage.[115] This is evident from Collins v FBD Insurance plc,[116] where Justice Feeney stated that in order to claim for a breach of duty of care, 'it is necessary for a claimant to establish that there has been a breach, that there has been damage and that breach caused such damage'.[117] The data controller and processor's duty of care to data subjects is set out in various provisions contained in the GDPR and Data Protection Act 2018. Therefore, a breach of one of these provisions would arguably be a breach of their duty of care to the data subject. In terms of the standard of care owed to the data subject, the data controller or processor must have been found to have 'infringed' the data subjects'

[108] See in particular *Klass v Germany,* application 5029/71, 6 September 1978; *Malone v. United Kingdom,* application 8691/79, 2 August 1984; *Weber and Saravia v Germany*, application 54934/00, 29 June 2006; and *Kennedy v United Kingdom*, application 26839/05, 18 May 2010.
[109] *Damache v DPP* [2011] IEHC 197 (High Court); [2012] IESC 11 (Supreme Court).
[110] Joined Case C-293/12 and C-594/12 *Digital Rights Ireland Ltd and Seitlinger and Others* (2014) ECJ.
[111] Data Protection Act 2018 (n 41), s 117(3).
[112] ibid, s 117(2).
[113] Trevor Murphy, 'The Justiciability of Data Protection Laws in Ireland: A New Dawn of Civil Litigation?' (2020) 27(11) CLP 238, pp 242.
[114] ibid.
[115] Piracy Report (n 29), para 5-02.
[116] *Collins v FBD Insurance plc* [2013] IEHC 137.
[117] ibid, para 4.4 (Feeney J).

rights. Therefore, the data subject would have to prove the data controller or processor fell below the standard of care required by the Data Protection Act 2018 for the data subject to claim any remedies.[118] It is suggested that section 117(4) wording of the data subject receiving damages 'as a result of the infringement' of their rights, suggests causation must be proved.[119] Therefore, the data controller or processor must have both factually and legally caused the breach of the data subjects' rights.

5.2 The remedies for data protection breaches

There are three types of remedies available under the Data Protection Act 2018. The first is the data controller or processor can be sanctioned for data breaches.[120] Although a large fine could be detrimental to a small company, it is arguable the sanctions being produced are not enough punishment for larger organisations. For example, Twitter was fined €450,000 by the Data Protection Commission in December 2020 for GDPR breaches. Commentators have stated that this fine is meagre and will not dissuade Twitter from having further data protection breaches.[121] The second remedy is an injunction to prevent the processing of data.[122] This injunction can either be interim, interlocutory or an injunction of indefinite duration.[123] Justice Eagar in the High Court granted an interim injunction to a mother against eBay, when her child's image was being used without her knowledge and consent by the website to advertise a seller's product.[124] The final remedy is compensation for the damage suffered by the data subject due to the breach.[125] The Data Protection Act 2018 states that the damage can either be material or non-material damage.[126] Non-material damage in particular is a contentious issue, as there is a lack of case law in the area and non-material damage is difficult to ascertain. The seminal case on this issue is Collins v FBD Insurance plc.[127] However, this case took place in 2013, meaning it precedes the Data Protection Act 2018 and GDPR. The plaintiff in this case was granted €15,000 in damages by the Circuit Court due to several breaches of the plaintiff's personal data by FBD. However, FBD appealed the case to the High Court, where the Circuit Court's decision was overturned by Justice Feeney. He stated that the plaintiff could not establish any 'actual damage' and He stated that generally, damages cannot be recovered for distress, damage to reputation or upset, unless "extreme distress results in actual damage

[118] Murphy (n 113), pp 245.
[119] ibid.
[120] Data Protection Act 2018 (n 41), s 141.
[121] Will Goodbody, 'Twitter fined €450,000 by Data Protection Commission for data breach' (RTÉ Business News, 15 December 2020) <https://www.rte.ie/news/business/2020/1215/1184537-twitter-fined-by-data-protection-commission> accessed 27 February 2021.
[122] Data Protection Act 2018 (n 41), s 117(4)(a).
[123] ibid, s 117(10).
[124] 'Mother secures order to stop use of child's image on eBay' *The Irish Times* (Dublin, 20 April 2020) <https://www.irishtimes.com/news/crime-and-law/courts/high-court/mother-secures-order-to-stop-use-of-child-s-image-on-ebay-1.4233304?mode=amp> accessed 27 February 2021.
[125] Data Protection Act 2018 (n 41), s 117(4)(b).
[126] ibid, s 117(10).
[127] *Collins v FBD Insurance plc* [2013] IEHC 137.

such as a recognisable psychiatric injury"..[128] Eoin O'Dell comments that Justice Feeney failed to realise that distress is actual damage, and calls for this position to be abandoned completely.[129] However, this case was subsequently upheld in Duggan v Commissioner of An Garda Síochána.[130] Nevertheless, this case also predates the Data Protection Act 2018 and GDPR. It is unclear whether future decisions will continue to use the approach set out by Justice Feeney in Collins,[131] or if they will set a new precedent, in line with the definition of damage in the Data Protection Act 2018 as being both 'material' and 'non-material'.[132]

5.3 Is this process effective in protecting data privacy?

It is arguable that there are flaws in this process. Although injunctions appear to be an effective remedy for breaches of data protection, there are certainly issues in relation to sanctions and non-material damage. Companies need to be sanctioned effectively to discourage them from conducting further breaches of data protection. Sanctions that have little to no impact on companies will not maintain data privacy and personal data will continue to be exposed. In terms of non-material damage, there is undoubtedly more development needed in this area of Irish Law. However, continuing to follow the approach set out by Justice Feeney in Collins[133] will not maintain data privacy, as the purpose of damages is to put the data subject back in the position, they would have been had the breach not occurred.[134] A breach of personal data is a breach of the constitutional right to privacy.[135] Therefore, the Courts should make use of the remedies available to compensate for this. It is hoped Justice Feeney's position will be abandoned in light of the Data Protection Act 2018 and GDPR.

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

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

Since its inception, Bunreacht na hÉireann has explicitly recognised the equal status of all persons under Article 40.1, which states that '[a]ll citizens shall, as human persons, be held equal before the law.' However, certain academics, including Doyle, contend that Article 40.1 lacks a strong comprehensive meaning and that any interpretation which restricts itself solely to the text would not provide for a 'convincing account of equality.'[136] Despite such

---

[128] ibid, para 4.3 (Feeney J).
[129] Eoin O'Dell, 'Ireland: Damages for Data Protection Breaches, 1: Why Collins v FBD Insurance is wrong (again)' (Informs' Blog, 19 December 2019) <https://inforrm.org/2019/12/19/ireland-damages-for-data-protection-breaches-1-why-collins-v-fbd-insurance-is-wrong-again-eoin-odell> accessed 27 February 2021.
[130] *Duggan v Commissioner of An Garda Síochána* [2017] IEHC 565.
[131] *Collins v FBD Insurance plc* [2013] IEHC 137.
[132] Kennedy and Murphy (n 8), s 117(10).
[133] *Collins v FBD Insurance plc* [2013] IEHC 137.
[134] Murphy (n 113), pp 246.
[135] Irish Constitution (n 6), Article 40.3.
[136] Oran Doyle, 'Constitutional Equality in Ireland: A Critical Account' Trinity College Dublin, Ireland School of Law 2004, pp 39.

arguments, Article 40.1 succeeds in placing the principle of equality and non-discrimination on a strong constitutional footing in Ireland. The constitutional recognition of equality is complimented by an array of anti-discrimination legislation, including the Equal Status Acts 2000-2004, which defines discrimination under section 31(a) as a situation where a 'person is treated less favourably than another person is, has been or would be treated.' The Act serves as a fundamental piece of legislation, prohibiting discrimination in the provision of goods and services, accommodation, advertising and education.[137] The Employment Equality Acts 1998-2015 also serve as important pieces of equality and anti-discrimination legislation, prohibiting discrimination in the workplace across nine grounds. The European Convention on Human Rights Act 2003 is another reformatory piece of equality legislation which gives effect to the ECHR in Irish law. While the Act will certainly enable the judiciary to read legislation in accordance with the Convention, it does not, as Egan argues, secure an independent cause of action or remedy for the litigant,[138] a substantial obstacle. The Irish Human Rights and Equality Commission Act 2014 (2014 Act) provides for the establishment of the Irish Human Rights and Equality Commission (the Commission) for the purposes of Directive 2014/54/EU of the European Parliament.[139] The 2014 Act defines 'discrimination' pursuant to the meaning under section 6 of the 1998 Act and section 3(1) and 4(1) of the 2000 Act. The Commission established under the 2014 Act is responsible for the review of reported cases of discrimination. Its array of functions, including the protection and promotion of human rights and equality, are listed under section 10 of the 2014 Act. Under Section 10 (2)(e), the Commission is empowered to apply to the High Court or Supreme Court for liberty to appear before the High Court or Supreme Court as *amicus curiae* in proceedings that involve the human rights or equality rights of any person. The Commission is also empowered under S.10(2)(m) to carry out equality reviews and prepare action plans or to invite others to do so where appropriate. Under S35(1), the Commission is empowered, through its own judgement or if requested by the Minister for Justice and Equality, to conduct an inquiry if it is considered by the Commission that (a) there is, in any body (whether public or otherwise) institution, sector of society, or geographical area, evidence of (i) a serious violation of human rights or equality of treatment obligations in respect of a person or a class of persons, or (ii) a systemic failure to comply with human rights or equality of treatment obligations, and (b) the matter is of grave public concern, and (c) it is in the circumstances necessary and appropriate so to do. Section 35(2) of the 2014 Act establishes that an inquiry may be undertaken by one or more than one member of the Commission. Section 35(3) provides that prior to conducting an inquiry, the Commission shall, as soon as may be, prepare terms of reference for the inquiry and an outline of the procedures to be followed for the

[137] Irish Human Rights and Equality Commission, 'Equal Status Act' https://www.ihrec.ie/guides-and-tools/human-rights-and-equality-in-the-provision-of-good-and-services/what-does-the-law-say/equal-status-acts/ accessed 31 May 2021.

[138] Egan, 'The European Convention on Human Rights Act 2003: A Missed Opportunity for Domestic Human Rights Litigation' (2003) 25 DULJ, pp 246.

[139] 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.

inquiry. Section 35(4) sets out that the Commission shall arrange for a copy of the terms of reference and outline of procedures referred to in subsection (3) to be laid before each House of the Oireachtas. Section 35(5) states that the Commission shall arrange for a notice of those terms and that outline to be published; (a) in at least one newspaper circulating in the State, (b) in such other manner as the Commission considers appropriate. Section 35(6) establishes that in conducting an inquiry the Commission shall to the greatest possible extent consistent with its duties under this Act: (a) seek the voluntary cooperation of persons whose evidence is desired for the purposes of the inquiry, and (b) facilitate such cooperation. Section 35(7) provides that the Commission shall conduct its inquiry as expeditiously as is consistent with its duties under this Act.

6.2 Does the review constitute effective protection against discrimination?

Human rights commissions have succeeded in asserting themselves as pillars of international human rights law, shifting from their once 'esoteric' nature as Dickson concludes.[140] Section 35 of the 2014 Act, as highlighted above, empowers the Commission to conduct inquiries and as the then Minister for Justice Equality and Defence Mr Alan Shatter stated the Act was modelled on that contained in the Commission of Investigations Act 2004 to ensure that the power vested in the Commission is a real one. Following analysis, it appears that the invocation of Section 36, which provides for the publication of an equality and human rights compliance notice following or in the course of an inquiry, has the potential to ensure high levels of conformity. He further stated that the notice explicitly specifies the nature of the discrimination employed and provides a detailed plan to eliminate the discriminatory practices which are to be implemented within a specific time frame.[141] The publication of the compliance notices has the potential to have a significant deterrent effect. The detailed plan and time frames provided by the Commission succeed in putting pressure on bodies in contravention of human rights or equality of treatment obligations to conform. Furthermore, Section 39, which enables the Commission to apply to the Circuit Court for an injunction against a person who does not comply with a human rights and equality compliance notice, succeeds in dismantling the contention that the Commission's light touch powers of enforcement are ineffective. Dickson further notes that the Commission's power to institute proceedings in its own name consolidates the Commission's *locus standi* regarding the protection of rights.[142] To this end, the Commission's inquiry procedure serves as a generally effective means to protect against discrimination and the promotion of human rights and equality.

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

---

[140] Brice Dickson, 'Ireland's Human Rights Commission' 36 Irish Jurist (NS), pp 265.
[141] Department of Justice, Dáil Éireann Irish Human Rights and Equality Commission Bill 2014 Second Stage Speech 8 April 2014 Alan Shatter, TD, Minister for Justice, Equality and Defence - The Department of Justice <http://www.justice.ie/en/JELR/Pages/SP14000097> accessed 31 May 2021.
[142] Dickson (n 140).

The UK Government's Industrial Strategy has described Artificial Intelligence (AI) as 'Technologies with the ability to perform tasks that would otherwise require human intelligence, such as visual perception, speech recognition, and language translation.'[143] AI has experienced exponential growth and is employed by a wide array of sectors in their decision-making process due to its apparent capacity to engage in 'efficient' and 'objective' decision-making.[144] However, as Kim propounds, while AI is inherently more efficient, it simultaneously has the capacity to engage in discrimination on the basis of sex, race or other discriminatory grounds, engaging in classification bias when, for example, employers use data algorithms to filter applications.[145] From an Irish standpoint, section 60(l)(ii) provides for the protection of 'members of the public against discrimination or unfair treatment in the provision of goods or services to them.' Section 89 of the Act further addresses rights in relation to automated decision-making and states that, 'subject to subsection (2), a decision that produces an adverse legal effect for a data subject or significantly affects a data subject shall not be based solely on automated processing, including profiling, of personal data that relate to him or her.' Subsection 2 provides that subsection 1 shall not apply where (a) the taking of a decision based solely on State and the law so authorising contains appropriate safeguards for the rights and freedoms of the data subject, including the right of the data subject to make representations to the controller in relation to the decision, and (b) the controller has taken adequate steps to safeguard the legitimate interests of the data subject. Section 89 (3) provides for the prohibition of profiling that results in discrimination against an individual on the basis of a special category of personal data. To this end, Irish legislation provides for some degree of protection against the technical aspects that result in discrimination. The AI space is a continuously developing sector and it will be pivotal that Irish legislation has the capacity to adapt to this ever-evolving technology to ensure sufficient protection against 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?

Ireland has consistently remained at the forefront of technological innovation and continues to rank highly in both the uptake and use of advanced digital technologies among the EU Member States.[146] Indeed, Ireland has steadily ranked in the top ten EU

[143] Department for Business, Energy and Industrial Strategy, 'Industrial Strategy: Building a Britain fit for the future' (HM Government 2017) 37 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf> accessed 14 March 2021.
[144] Naomi Foale, 'Back to the Future: How Well Equipped Is Irish Employment Equality Law to Adapt to Artificial Intelligence?' (2020) 23 Trinity CL Rev 170.
[145] Pauline T Kim, 'Data-Driven Discrimination at Work' (2017) 58 William and Mary Law Review 857, pp 866.
[146] National Cyber Security Centre, 'National Cyber Security Strategy 2019-2024' (2019) 8 <https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf> accessed 31 May 2021.

Member States for internet usage by both individual citizens and enterprises alike.[147] However, specific national regulation concerning Advanced Digital Technologies remains sparse. This is in part due to the Irish Government's recognition of the competence by which the EU acts to introduce comprehensive regulations in the area of Advanced Digital Technologies. Such regulations are transposed into national legislation in line with EU requirements. This is achieved by the Irish legislature's secondary (delegated) legislation in the form of a statutory instrument (SI).[148] The Right to Privacy and Data Protection is primarily regulated under the Data Protection Acts 1988, 2003, and 2018. The Data Protection Act 2018 transposed the GDPR into Irish Law. This is supplemented in Irish domestic law by the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011[149] (the 'E-Privacy Regulations'), which transposes the EU Directive 2009/136/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services.[150] Advanced Digital Technologies such as Big Data are in part regulated by the E-Privacy regulations. Where Big Data can be considered to amount to personal data, providers of publicly available services or communication networks are required to take both appropriate technical and organisational steps to ensure the security of the data through the use of encryption or other means. Furthermore, any interception or surveillance of communications and data over a publicly accessible electronic communications service is prohibited under the E-privacy regulations. Further measures were introduced by the EU in the Security of Network and Information Systems Directive 2016/1148 (NISD).[151] NISD is based on Article 114 of the Treaty on the Functioning of the European Union (TFEU) and seeks to ensure the continuity of services to allow the Union's economy and society to function properly.[152] The transposition of the NISD into Irish Law was facilitated by the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (the NISD Regulations).[153] Advanced Digital Technologies are in part subject to rules under the NISD Regulations whereby operators of essential services and digital services are mandated to take appropriate

[147] European Commission, 'Digital Economy and Society Index (DESI) 2020' (2020) 63 <https://ec.europa.eu/digital-single-market/endigital-economy-and-society-index-desi> date accessed 24 May 2021.
[148] Raymond Byrne and others, *The Irish Legal System* (Seventh edition, Bloomsbury Professional 2020) para 13.03-13.04.
[149] General Data Protection Regulation 2018 (n 71).
[150] 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.
[151] Directive 2016/1148 EU 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.
[152] European Commission, 'Report from the Commission to the European Parliament and the Council Assessing the Consistency of the Approaches Taken by Member States in the Identification of Operators of Essential Services in Accordance with Article 23(1) of Directive 2016/1148/EU on Security of Network and Information Systems COM/2019/546 Final' (2019).
[153] S.I. No. 360/2018 - European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018.

measures to prevent and minimise incidents, and any impact thereof which affects the security of the network and information systems used in the provision of essential and digital services. The NISD Regulations are supplemented by the Commission Implementing Regulation 2018/151 which provides for, inter alia, further elements to be taken into account in the identification of measures to ensure the security of network and information systems.[154] In 2011, the Irish Government introduced the Computer Security Incident Response Team (CSIRT-IE) as part of the then Irish Department of Communications, Energy and Natural Resources.[155] This was subsequently followed by the establishment of the Irish National Cyber Security Centre (NCSC) in 2013. As of 2015, the NCSC is a State Agency within the Irish Department of the Environment, Climate and Communications (DECC). The NCSC provides expertise in cybersecurity to and facilitates safeguarding for the security of systems and information for both the Irish Government, private industry and consumers.[156] At a policy level, a National Digital Strategy for Ireland was published by the DECC in 2013.[157] The Irish Government has recently completed a public consultation in anticipation of adopting an updated National Digital Strategy, which is currently being drafted.[158] Furthermore, from the publication of a 2018 White Paper by the Irish Department of Public Expenditure and Reform, it appears that Ireland is on track to become a European leader in the regulation of Advanced Digital Technologies, with the goal of establishing Ireland as a 'best practice hub'.[159] Finally, the DECC is currently taking the lead in developing legislation that will transpose the European Electronic Communications Code Directive 2018/1972 (EECC) into Irish Law.[160] The EECC entered into force in December 2018 and was due to be transposed into the domestic law of Member States by 21 December 2020. However, as of February 2021, only Greece, Hungary and Finland have completed transposition into national legislation.[161] While infringement proceedings have been brought by the European Commission against 24

[154] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact C/2018/0471.
[155] 'NCSC: National Cyber Security Centre' <https://www.ncsc.gov.ie/> accessed 24 February 2021.
[156] 'NCSC: About Us' <https://www.ncsc.gov.ie/about/> accessed 24 February 2021.
[157] Department of Communications, Energy & Natural Resources, 'Doing More with Digital: National Digital Strategy for Ireland' (2013) <https://assets.gov.ie/27518/7081cec170e34c39b75cbec799401b82.pdf> accessed 24 May 2021.
[158] Department of the Environment, Climate and Communications, 'National Digital Strategy' <https://www.gov.ie/en/publication/f4a16b-national-digital-strategy> accessed 24 February 2021.
[159] Department of Public Expenditure and Reform, 'Enabling Digital Ireland: A Summary Report on Ireland's Ambition to Be a Leader in the Provision of Digital Government Services' (2018) <https://pulse.microsoft.com/uploads/prod/2018/08/Enabling-Digital-Ireland-Whitepaper.pdf> accessed 24 May 2021, SEE ALSO ibid (n159) pp 29.
[160] Directive 2018/1972 EU of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.
[161] 'Commission Opens Infringement Procedures against 24 MS' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_206> accessed 24 February 2021.

Member States for failure to transpose the EECC by the deadline,[162] the DECC has published a draft implementing legislation to be enacted later in 2021.[163]

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

Multiple academics, legal professionals, government bodies and international institutions have recognised the rapidly evolving nature of cybersecurity, and as such, the importance of 'security protections that safeguard the confidentiality, integrity and availability of information for both individuals and organisations'.[164] However, the rapid advancement of technologies has presented opportunities for criminals and terrorists to conceal incriminating evidence through encrypting communications and stored data.[165] As such, this has developed obstacles for law enforcement authorities in intercepting encrypted personal communications, rendering them beyond the remit of criminal investigation.[166] Consequently, this prevents law enforcement authorities from obtaining vital evidence and intelligence for criminal investigations and conviction.[167] Currently, at a national level, there is no specific legal framework governing the accessibility to encrypted personal messages for criminal investigations, or the failure to disclose keys to encrypted materials to law enforcement agencies. However, there are specific Garda statutory powers available to law enforcement for key disclosure or information decryption.[168] The most prominent powers fall under the Criminal Justice (Theft and Fraud Offences) Act 2001 (2001 Act), that may become relevant in criminal investigations. Section 48 of the 2001 Act governs authority of law enforcement in relation to search warrants whereby members of the Garda Síochána may require persons to give any password necessary to operate such information 'in a form in which it can be removed and in which it is, or can be made, visible and legible.'[169] Section 52 includes powers to require persons to produce evidence and decrypt such evidential information, in the event that 'there are reasonable grounds for suspecting that the material constitutes evidence of or relating to the commission of the offence'.[170] However, academics have considered the narrow limitations of these statutory powers that require

[162] ibid.
[163] Department of the Environment, Climate and Communications, 'European Electronic Communications Code (EECC)' <https://www.gov.ie/en/publication/339a9-european-electronic-communications-code-eecc/> accessed 24 February 2021, SEE ALSO End-User Rights text of draft Statutory Instrument transposing the European Electronic Communications Code <https://assets.gov.ie/77304/24998a57-3f1e-4bdb-9a72-f7bfec561bac.pdf> accessed 24 February 2021.
[164] Eoghan Casey, 'Practical Approaches to Recovering Encrypted Digital Evidence', (2002) Vol 1(3) International Journal of Digital Evidence.
[165] ibid.
[166] Samuel Elliot, 'The Right to Encryption? An Examination of Cryptography Law and Jurisprudence in the UK', Trinity College Law Review <https://trinitycollegelawreview.org/right-to-encryption/> accessed February 2021.
[167] Dorothy E. Denning, 'Hiding Crimes in Cyberspace', (1999) Vol 2(3) Information, Communication and Society.
[168] Criminal Justice (Theft and Fraud Offences) Act, 2001, Proceeds of Crime (Amendment) Act 2005.
[169] Criminal Justice (Theft and Fraud Offences) Act, 2001, s 48.
[170] ibid section 52, para. 2-3.

such persons to be on the premises of investigation,[171] or in 'possession or control' of the incriminating evidence.[172] Consequently, these legal powers have prompted senior representatives of An Garda Síochána to appeal for specific national legislation governing access to incriminating encrypted data for criminal investigations.[173] In 2020, Garda Commissioner Drew Harris appealed for legislation governing access to keys to encrypted personal communications, and for the criminalisation of withholding keys.[174] Commissioner Harris detailed the importance of the proposed powers in cases of serious criminal cases, such as child abuse and human trafficking. Commissioner Harris further denounced the judicial backlog of child abuse imagery as an 'operational and reputational risk' to the organisation and stated that the proposed legislation would hasten criminal process.[175] Similarly, at the European Union level, there is no requirement that keys to encrypted materials be disclosed to law enforcement authorities.[176] However, there are currently measures in place governing access to encrypted communications. For example, the non-binding 2001 Resolution on Law Enforcement Operational Needs with Respect to Public Telecommunication Networks and Services,[177] which considers the operational needs of law enforcement authorities,[178] specifically 'in the development and implementation of any measures concerning legally authorized forms of interception of telecommunications.'[179] The Resolution calls on Member States to adopt national legislation governing the decryption of encrypted materials, 'if network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications *en clair*.'[180] While these measures are not binding on Member States, the Garda Cyber Crime Bureau can avail of the advanced 'decryption platform' launched by Europol in December 2020 in close collaboration with European Commission's Joint Research Centre.[181] This platform 'marks a milestone in the fight

[171] ibid, s 48.
[172] ibid, s 52.
[173] Cormac O Keefe, 'Gardaí call to access digital devices to tackle online child abuse imagery', The Irish Examiner (10 February 2020) <https://www.irishexaminer.com/news/arid-30980947.html> accessed 26 February 2021.
[174] ibid.
[175] ibid.
[176] The Law Library of Congress, 'Government Access to Encrypted Communications', <https://www.loc.gov/law/help/encrypted-communications/gov-access.pdf> accessed 25 February 2021.
[177] Council of the European Union, Council Resolution on Law Enforcement Operational Needs with Respect to Public Telecommunication Networks and Services, June 20, 2001.
[178] ibid.
[179] Council of the European Union, Council Resolution on Law Enforcement Operational Needs with Respect to Public Telecommunication Networks and Services, June 20, 2001, at *Annex*. <https://www.statewatch.org/media/documents/news/2001/sep/9194.pdf> accessed 25 February 2021.
[180] ibid, para 3.3.
[181] 'Europol and the European Commission Inaugurate New Decryption Platform to Tackle the Challenge of Encrypted Material for Law Enforcement Investigations', Europol (18 December 2020) <https://www.europol.europa.eu/newsroom/news/europol-and-european-…rm-to-tackle-challenge-of-encrypted-material-for-law-enforcement> accessed February 25, 2021.

against organised crime and terrorism' in Europe that recognises fundamental human rights without limiting or weakening encryption for citizens.[182]

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

Despite ambitious efforts in recent years towards stimulating digital advancement, Ireland has historically failed to vindicate the human right to privacy in the context of data protection.[183] Home to the European headquarters of internet giants such as Facebook, Google, and Apple, it is particularly incumbent on Ireland to address these legislative and administrative gaps. The Irish Government has repeatedly asserted its intention to become a best-in-class leader in the digitization of the public sector, utilising new technologies to securely store the personal information of data subjects. However, doubts persist as to the technical and regulatory capabilities of the DPC, which have been widely criticized on the world stage, both before the EU courts and by international counterparts. The NGO Digital Rights Ireland had previously challenged Ireland's implementation of the Data Retention Directive,[184] which provided for the retention of personal communications data for law enforcement purposes. The plaintiffs contended that this was contrary to the rights to privacy, travel and freedom of expression as guaranteed by the Irish Constitution. The matter was eventually referred to the CJEU.[185] The Directive was invalidated on the grounds that it interfered with the right to privacy and to data protection guaranteed by the EU Charter of Fundamental Rights.[186] It was the Schrems cases,[187] however that had the most significant impact on data management in Irish and European Law. It is no secret that Ireland's Foreign Direct Investment Strategy is particularly welcoming to technology multinational corporations,[188] nor that this has previously come into conflict with ensuring these companies comply with European data protection law. Between 2011 and 2013, Austrian national Max Schrems lodged 23 complaints against Facebook Ireland with the Data Protection Commission. These complaints largely revolved around Facebook's excessive collection and processing of user data, contrary to Irish[189] and EU law[190.] Since 2010, Facebook users outside North America are under terms-of-service contracts with Facebook Ireland Ltd, rather than Facebook Inc. in California. This effectively placed the

---

[182] ibid.
[183] An in-depth discussion of the legal basis of a right to privacy in Irish law, and the relationship of this right to data protection, can be found in Question 2, at 1.
[184] Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105.
[185] Joined Case C-293/12 and C-594/12 *Digital Rights Ireland Ltd and Seitlinger and Others* (2014) ECJ.
[186] Article 7 & 8, EU Charter of Fundamental Rights 2000.
[187] Case 311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2018] ECLI 559.
[188] Jack Conway, 'Big Tech Picks Ireland as Data Centre Hub' (FDI Intelligence, 17 August 2020) <https://www.fdiintelligence.com/article/78473> accessed 12 March 2021.
[189] Data Protection Act 1988 s 2(1)(c)(iii), replaced by the Data Protection Act 2018.
[190] Council Directive 1995/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281, predecessor to the GDPR.

DPC in the position of regulating Facebook as processor and controller of the data of millions of EU citizens.[191] Mr Schrems' final complaint in 2013 followed Edward Snowden's revelations regarding the routine global telecommunications monitoring by the US National Security Agency. It alleged that this surveillance programme proved that there was not an effective level of data protection within the US, and called on the DPC to order a halt to the transfer of data from Facebook Ireland to America.[192] The DPC initially dismissed Mr Schrems' complaint as 'frivolous and vexatious',[193] citing an earlier decision of the European Commission, which confirmed the US complied with the 'Safe Harbour' privacy requirements for the transfer of data from a Member State to outside the EU.[194] The matter was referred to the European Court of Justice (ECJ) for preliminary ruling, where it was determined that a Commission decision cannot reduce the powers available to national supervisory authorities under the Data Protection Directive.[195] The ECJ declared the Safe Harbour Principle inherently invalid, and that any legislation which permits public authorities to generally monitor electronic communications is to be considered repugnant to the fundamental right to respect for private life.[196] It subsequently forced the suspension of data transfer to the US by Facebook Ireland, compelling national data protection authorities to prevent the transfer of data made under standard contractual clauses, included in user Terms of Service Agreements.[197] The weakness of the Irish Data Protection Commission and regulatory framework has been subject to widespread criticism since Schrems I.[198] Peter Schaar, Germany's former Federal Commissioner for Data Protection and Freedom of Information, described Ireland as a convenient home for Big Tech, saying, 'of course Facebook would go to a country with the lowest levels of data protection. It's natural they would choose Ireland'.[199] Dr TJ McIntyre of Digital Rights Ireland, considers the DPC overly restrained by its legal obligation to seek an amicable resolution of every case before it takes formal action.[200] The lack of resources the Government has invested in the DPC were laid bare by these legal challenges. An audit of Facebook Ireland's compliance with data protection law was conducted in 2011. The DPC relied on pro-bono academic assistance, in the absence of in-house expertise.[201]

---

[191] TJ McIntyre, 'Regulating the Information Society: Data Protection and Ireland's Internet Industry' in David Farrell and Niamh Hardiman (eds), *The Oxford Handbook of Irish Politics* (Oxford University Press, forthcoming 2021).
[192] Doyle and Tom Hickey (n 12).
[193] European Convention on Human Rights Act 2003 (n 34).
[194] European Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ 2 215/7.
[195] Doyle and Tom Hickey (n 12).
[196] ibid, para 98.
[197] Case 311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2018] ECLI 559.
[198] McIntyre (n 191).
[199] Mark Scott, 'Irish Regulator Says Country Will Stay at Centre of Online Privacy Debate' *The New York Times* (New York, 23 June 2015) accessed 22 February 2021.
[200] ibid, pp 3.
[201] Data Protection Commission, *Annual Report 2011* (2011) pp 22 <https://www.dataprotection.ie/sites/default/files/uploads/2018-12/AnnualReport2011.pdf> accessed 01 June 2021.

Considering the Irish Government's well-publicized legislative steps towards increased digitization, a fit-for-purpose DPC will be crucial in vindicating the human rights of citizens online. In July 2018, the Office of the Government Chief Information Officer published a summary report which aimed to outline and strategize Ireland's ambition to become a world leader in the provision of digitized public services.[202] It was jointly produced with Microsoft Ireland and the Fletcher School of Law and Diplomacy, a department of Tufts University. The White Paper utilizes the Smart Society Benchmark, developed by the Fletcher School, to evaluate Ireland on its Digital Intelligence Index 2017, which measures the competitiveness of digital economies. Out of ninety countries, Ireland was ranked sixteenth in terms of the rapidity of the digitization of its economy. As of 2020, that ranking had increased to twelfth place.[203] A key factor in this advancement is the institutional support Ireland offers towards encouraging digital innovation; in this respect, Ireland is currently ranked fourth in the world. The Department of Public Expenditure engaged closely with the private sector in writing the report, in particular, the Applied Innovation Department of Microsoft, another company with European headquarters in Dublin. The foreword is co-authored by Government CIO Barry Lowry and the Managing Director of Microsoft Ireland, a clear expression of the government's inclination towards developing regulatory and fiscal conditions in line with technology companies' own assessments of their requirements. The report calls for the deployment of a legal and regulatory framework to support the introduction of technologies, such as a hyperscale public cloud for the provision of government services via the Internet.[204] It suggests a comprehensive strategy which outlines flexible security standards and technical measures, capable of adapting to ever-evolving technologies.[205] The Report describes Ireland's public services as under-digitized, but acknowledges this is partly due to the lack of an electronic public identification number at the time of writing. The subsequent launch of MyGovID, a secure online identification platform, which allows access to public services via the internet, is expected to significantly streamline the digitization of government services.[206] The Irish Government has already begun enacting legislation to support this strategy. The Digital Sharing and Governance Act 2019 will take effect upon the issuing of a commencement order by the Minister for Public Expenditure and Reform. It was heavily influenced by the eGovernment Strategy 2017-2020., which details how Ireland will work in tandem with the European Commission's commitment to governmental digital transformation within Member States.[207] The Digital Sharing and Governance Act 2019 will govern the management of personal data by the public sector, and how that data is

[202] Department of Public Expenditure and Reform, *Enabling Digital Ireland* (2018).
[203] Bhaskar Chakravorti, Ravi Shankar Chaturvedi, Christina Filipovic, and Griffin Brewer, 'Digital in the Time of Covid' (2020) Digital Intelligence Index pp 23 <https://sites.tufts.edu/digitalplanet/files/2020/12/digital-intelligence-index.pd> accessed 28 February 2021.
[204] McIntyre (n 191).
[205] ibid, pp 6.
[206] ibid, pp 28.
[207] Departure of Public Expenditure and Reform on 1 June 2017 at <https://www.gov.ie/en/publication/63a31-egovernment-strategy-20172020/> accessed 27 February 2021.

shared between government bodies. The objective is that citizens will only need to provide the State with their personal data once, where appropriate. It provides a statutory basis to allow public sector bodies to share data amongst themselves. The methods of data collection will continue to be governed by the GDPR, and the Data Protection Act 2018, which transposed it into Irish law. Under the terms of the GDPR, private entities may invoke a 'legitimate interest' in processing personal data as a requirement for delivering their services.[208] Public bodies, however, may only do so where a legal basis is provided by EU or domestic law. The requirements for disclosure of personal data between public bodies are lengthy, and predicated on necessity for the performance of a service or the verification of an individual's identity.[209] Data-sharing agreements between departments must be transparent; they must describe, among other details; the data which will be disclosed, and the purpose of sharing it; whether the disclosure relates to individuals or classes of data subjects; whether the disclosure is recurring, or on a one-time basis, and whether the data will be retained, and what security measures are in place to this effect.[210] The EU eGovernment Action Plan 2016-2020 established seven guiding principles for the digitisation of national governments, focusing on accessibility, sharing of data between public bodies, transparency, and cross-border operability. The final principle reinforces the importance of cybersecurity in order to safeguard citizens' aforementioned rights to data privacy and free communication. If digital public services are to be widely adopted, the public must trust that their government will vindicate these rights. Considering Ireland's poor track record in this respect, concentrated efforts may be required to encourage mass uptake. It seems Ireland is moving towards a greater regulatory emphasis on digital human rights within private industry, with an eye to digitizing the public sector in a manner that respects the data privacy of individuals. The DPC has assumed a more aggressive role as of late, issuing its first fines under the GDPR to two state agencies (the Health Service Executive and Tusla Child and Family Agency) for data breaches. In the private sector, Twitter was also subject to a fine of €450,000. However, despite a significant increase in funding since the inception of Schrems, Data Protection Commissioner Helen Dixon has pleaded for greater resource allocation, citing 'acute strain' and the pervasive international perception that there is a link between Ireland's lax data protection regulations and its foreign investment strategy. A greater material commitment to the national regulator will be required if Ireland is to lead the way in digital advancement.

[208] Article 6.1 of Council and Parliament Regulation (EU) 2016/679 of 27 April 2018 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 L 119. (GDPR).
[209] Michael Barrett, 'Share and Share Alike' (Law Society Gazette, 12 November 2020) <https://www.lawsociety.ie/gazette/in-depth/data-sharing/> accessed 27 February 2021.
[210] Data Sharing and Governance Act 2019, s 19.

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?

As a committed member of the EU most of Ireland's legislation with regards to Human Rights online is grounded in EU decisions, directives, and regulations. As a common law system, Ireland has exceptionally good legal prerequisites to shape the law in regard to human rights online and appropriately protect the rights of its citizens. This is because the common law system is more flexible in responding to societal needs due to reliance on precedent.

10.1 Will Irish law in regard to Human Rights Online develop within Legislation or Common Law?

Based on the foregoing analysis it is consistent to believe that Irish law will develop as both legislation and common law. With regard to the development of Irish legislation on human rights online, this development is likely to be EU-motivated.

10.1.1 Legislation

At the forefront of the protection of Human Rights generally and in particularly in the context of online activities, it can be assumed that the EU will put in place more substantial regulations and directives, because the issue is best handled across multiple jurisdictions. However, it follows from a recent statement of Commission president Ursula von der Leyen that the direction of EU legislation will change. Having focused on 'eCommerce' and 'neutrality' rules' which ensure that no operator can block, slow down, or prioritise certain traffic, the EU will now need to do more to ensure fair access to the most vital platforms for business, innovation and free expression, prevent disinformation and more heavily focus on the regulation of AI, ensuring rights against discrimination, to redress, for product safety.[211] Thus, it is convincing that future EU directives and regulations on the topic will push Ireland to advance its so far relatively poor protection in the sphere of AI and introduce legislation regarding big data, the internet of things and encryption which have so far been neglected in national legislation.

10.1.2 Common Law

[211] 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, and Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance), and European Commission Statement "Statement by President von der Leyen at the roundtable 'Internet, a new human right' after the intervention by Simona Levi" Brussels, 28 October 2020 <https://ec.europa.eu/commission/presscorner/detail/en/statement_20_200> accessed 28 February 2021.

The flexibility of the Irish Common Law provides an exceptionally good foundation to intensify the protection of human rights online. As the internet is developing and changing at an enormous pace, a pace that legislation is often unable to keep up with, precedent might be an exceptionally effective tool in the area at hand. It provides the opportunity to expand upon existing legislation and develop new legal principles that are more nuanced, time appropriate and address current issues. As the foregoing analysis demonstrates, Ireland's courts have been particularly active in the area of data protection, indicating that that precedent over legislation may likely be the focal means of advancing human rights online. In addition to GDPR, the constitutional right to privacy, recognized in Norris, Re a Ward of Court (No. 2), and Fleming,[212] establishing privacy through an interpretation of the Irish Constitution as a fundamental unenumerated right, might further provide a solid foundation for extensive case law regarding data protection breaches and the right to privacy online.[213] Although adjustment regarding remedies is needed, recognizing non-economic loss the same way as economic loss, as most damages from data protection breaches are of this nature, the recent jurisprudence regarding non-material damages indicates that a move towards a more comprehensive acknowledgement of loss is not unlikely. Thus, while the common law seems more prone to success in regard to protecting human rights online in the next five years, it is important to mention that change in the legal landscape is dependent upon cases with specific facts relevant to areas of contention being litigated before the courts. Such litigation would create the possibility for development of human rights online through the common law in Ireland, however, it must be noted that these outcomes, although possible, are not certain.

10.2 Conclusion

The above analysis indicates that while Ireland does fulfil the minimum requirements that the EU sets on the protection of Human Rights online, individually it does little proactively to go beyond those requirements. However, as the last remaining common law country in the EU, Ireland does have an advantage over other member states to incorporate flexible protection into Irish jurisprudence enabling more consistency to keep up with the fast-paced environment of the digital age. With this in mind, it is convincing that more cases with regard to Human Rights in the digital sphere might be brought to the Irish courts in the coming 5 years, changing the Irish and possibly European legal landscape by advancing new precedent to protect human rights online.

Conclusion

To conclude, under Irish Law, the situation surrounding technology and human rights is well-protected, but there is still room for more development. Ireland recognises the international right to personal information and has constitutionally protected this via Article 40 of Bunreacht na hEireann. However, it must be noted that the Oireachtas has

[212] ibid (n 85).
[213] Irish Constitution (n 6), Article 40.3.

not created a statutory right to privacy, there were efforts made by previous governments to make a breach of privacy under Irish Law a tort, but this has not prevailed as of yet. The public and private sectors in Ireland are regulated through the GDPR and Data Protection Act 2018. Both of which are governed by the Data Protection Commissioner, who is tasked to ensure compliance with the aforementioned legislation. Irish case Law has set out the strong role the judiciary has taken where a breach of a fundamental right occurs. The process of judicial review has ensured that the right to privacy of each citizen is protected and vindicated through public and private sector processes. But these processes are not faultless and stronger remedies and sanctions will need to be enacted. For the most part, there have been positive developments since the enactment of the GDPR and Data Protection Act 2018. Arguably, Irish Law does not reach beyond what is outlined as part of its EU membership. It does, however, have the potential to have exceptional legislative protections in relation to human rights, as we are the last remaining Common Law country within the European Union and therefore, have the advantage of being able to flexibly change Irish Jurisprudence. Ultimately, it is key that Irish national laws have the capacity to evolve as technology continues to develop. If this is ensured, Ireland has the potential to change not only national protection, but perhaps the European landscape in the area.

Table of legislation

Title of the legal act	Provision text in English language
Adoption Act 2008, s 88.	A court shall not make an order— (*a*) referred to in *section 86 (2)*, (*b*) for the discovery, inspection, production or copying of any book, document or record of the Authority (or of any extracts from any of them), or otherwise in relation to the giving or obtaining of information from any of them, unless the court is satisfied that it is in the best interests of any child concerned to make the order.
Article 6.1 of Council and Parliament Regulation (EU) 2016/679 of 27 April 2018 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 L 119.	1. (a) (b) (c) (d) (e) (f) kept 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').
Criminal Justice (Theft and Fraud Offences) Act, 200, s 52.	(1) This section applies to any offence under this Act which is punishable by imprisonment

	for a term of five years or by a more severe penalty. (2) A judge of the District Court, on hearing evidence on oath given by a member of the Garda Síochána, may, if he or she is satisfied that— (a) the Garda Síochána are investigating an offence to which this section applies, (b) a person has possession or control of particular material or material of a particular description, and (c) there are reasonable grounds for suspecting that the material constitutes evidence of or relating to the com- mission of the offence, order that the person shall— (i) produce the material to a member of the Garda Síochána for the member to take away, or (ii) give such a member access to it, either immediately or within such period as the order may specify. (3) Where the material consists of or includes information contained in a computer, the order shall have effect as an order to produce the information, or to give access to it, in a form in which it is visible and legible and in which it can be taken away. (4) An order under this section— (a) in so far as it may empower a member of the Garda Síochána to take away a document, or to be given access to it, shall also have effect as an order empowering the member to take away a copy of the document (and for that purpose the member may, if necessary, make a copy of the document), (b) shall not confer any right to production of, or access to, any document subject to legal privilege, and (c) shall have effect notwithstanding any other obligation as to secrecy or other restriction on disclosure of information imposed by statute or otherwise.

	(5) Any material taken away by a member of the Garda Síochána, under this section may be retained by the member for use as evidence in any criminal proceedings. (6) (a) Information contained in a document which was produced to a member of the Garda Síochána, or to which such a member was given access, in accordance with an order under this section shall be admissible in any criminal proceedings as evidence of any fact therein of which direct oral evidence would be admissible unless the information— (i) is privileged from disclosure in such proceedings, (ii) was supplied by a person who would not be compellable to give evidence at the instance of the prosecution, (iii) was compiled for the purposes or in contemplation of any— (I) criminal investigation, (II) investigation or inquiry carried out pursuant to or under any enactment, (III) civil or criminal proceedings, or (IV) proceedings of a disciplinary nature, or unless the requirements of the provisions mentioned in paragraph (b) are not complied with. (b) References in sections 7 (notice of documentary evidence to be served on accused), 8 (admission and weight of documentary evidence) and 9 (admissibility of evidence as to credibility of supplier of information) of the Criminal Evidence Act, 1992, to a document or information contained in it shall be construed as including references to a document mentioned in paragraph (a) and the information contained in it, and those provisions shall have effect accordingly with any necessary modifications.
Criminal Justice (Theft and Fraud Offences) Act, 2001, s 48.	(1) This section applies to an offence under any provision of this Act for which a person of full age and capacity and not previously convicted may be punished by imprisonment

	for a term of five years or by a more severe penalty and to an attempt to commit any such offence. (2) A judge of the District Court, on hearing evidence on oath given by a member of the Garda Síochána, may, if he or she is satisfied that there are reasonable grounds for suspecting that evidence of, or relating to the commission of, an offence to which this section applies is to be found in any place, issue a warrant for the search of that place and any persons found there. (3) A warrant under this section shall be expressed and shall operate to authorise a named member of the Garda Síochána, alone or accompanied by such other persons as may be necessary— (a) to enter, within 7 days from the date of issuing of the war- rant (if necessary by the use of reasonable force), the place named in the warrant, (b) to search it and any persons found there, (c) to examine, seize and retain any thing found there, or in the possession of a person present there at the time of the search, which the member reasonably believes to be evidence of or relating to the commission of an offence to which this section applies, and (d) to take any other steps which may appear to the member to be necessary for preserving any such thing and preventing interference with it. (4) The authority conferred by subsection (3)(c) to seize and retain any thing includes, in the case of a document or record, authority— (a) to make and retain a copy of the document or record, and (b) where necessary, to seize and, for as long as necessary, retain any computer or other storage medium in which any record is kept.

	(5) A member of the Garda Síochána acting under the authority of a warrant under this section may— (a) operate any computer at the place which is being searched or cause any such computer to be operated by a person accompanying the member for that purpose, and (b) require any person at that place who appears to the member to have lawful access to the information in any such computer— (i) to give to the member any password necessary to operate it, (ii) otherwise to enable the member to examine the information accessible by the computer in a form in which the information is visible and legible, or (iii) to produce the information in a form in which it can be removed and in which it is, or can be made, visible and legible. (6) Where a member of the Garda Síochána has entered premises in the execution of a warrant issued under this section, he may seize and retain any material, other than items subject to legal privilege, which is likely to be of substantial value (whether by itself or together with other material) to the investigation for the purpose of which the warrant was issued. (7) The power to issue a warrant under this section is in addition to and not in substitution for any other power to issue a warrant for the search of any place or person. (8) In this section, unless the context otherwise requires— "commission", in relation to an offence, includes an attempt to commit the offence; "computer at the place which is being searched" includes any other computer, whether at that place or at any other place, which is law- fully accessible by means of that computer; "place" includes a dwelling;

	"thing" includes an instrument (within the meaning of Part 4), a copy of such instrument, a document or a record.
Data Protection Act 1988 s 2(1)(c)(iii)	(iii) shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
Data Protection Act 2018, s 12(2).	The Commission shall monitor the lawfulness of processing of personal data in accordance with— (a) Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013[5] on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), and (b) Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013[6] establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast).
Data Protection Act 2018, s 71.	(1) A controller shall, as respects personal data for which it is responsible, comply with the following provisions: (a) the data shall be processed lawfully and fairly;

	(b) the data shall be collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes; (c) the data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed; (d) the data shall be accurate, and, where necessary, kept up to date, and every reasonable step shall be taken to ensure that data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; (e) the data shall be kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are processed; (f) the data shall be processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against— (i) unauthorised or unlawful processing, and (ii) accidental loss, destruction or damage. (2) The processing of personal data shall be lawful where, and to the extent that— (a) the processing is necessary for the performance of a function of a controller for a purpose specified in section 70(1)(a) and the function has a legal basis in the law of the European Union or the law of the State, or (b) the data subject has, subject to subsection (3), given his or her consent to the processing. (3) Where the processing of personal data is to be carried out on the basis of the consent of the data subject referred to in subsection (2)(b), the processing shall be lawful only where, and to the extent that— (a) having been informed of the intended purpose of the processing and the identity of the controller, the data subject gives his or her consent freely and explicitly, (b) the request for consent is expressed in clear and plain language, and where such

	consent is given in the context of a written statement that also concerns other matters, the request for consent is presented to the data subject in a manner that is clearly distinguishable from those other matters, and (c) the data subject may withdraw his or her consent at any time, and he or she shall be informed of this possibility prior to giving consent. (4) Where a data subject withdraws his or her consent to the processing of personal data pursuant to subsection (3)(c), the withdrawal of consent shall not affect the lawfulness of processing based on that consent prior to the consent being withdrawn. (5) Where a controller collects personal data for a purpose specified in section 70(1)(a), the controller or another controller may process the data for a purpose so specified other than the purpose for which the data were collected, in so far as— (a) the controller is authorised to process such personal data for such a purpose in accordance with the law of the European Union or the law of the State, and (b) the processing is necessary and proportionate to the purpose for which the data are being processed. (6) A controller may process personal data, whether the data were collected by the controller or another controller, for— (a) archiving purposes in the public interest, (b) scientific or historical research purposes, or (c) statistical purposes, provided that the said processing— (i) is for a purpose specified in section 70(1)(a), and (ii) is subject to appropriate safeguards for the rights and freedoms of data subjects. (7) A controller shall ensure, in relation to personal data for which it is responsible, that an appropriate time limit is established for— (a) the erasure of the data, or

	(b) the carrying out of periodic reviews of the need for the retention of the data. (8) Where a time limit is established in accordance with subsection (7), the controller shall ensure, by means of procedural measures, that the time limit is observed. (9) A processor, or any person acting under the authority of the controller or of the processor who has access to personal data, shall not process the data unless the processor or person is— (a) authorised to do so by the controller, or (b) required to do so by the law of the European Union or the law of the State, and then only to the extent so authorised or required, as the case may be. (10) A controller shall ensure that it is in a position to demonstrate that the processing of personal data for which it is responsible is in compliance with subsections (1) to (8) of this section.
Data Protection Act 2018, s 72.	(1) In determining appropriate technical or organisational measures for the purposes of section 71(1)(f), a controller shall ensure that the measures provide a level of security appropriate to the harm that might result from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the data concerned. (2) A controller or processor shall take all reasonable steps to ensure that— (a) persons employed by the controller or the processor, as the case may be, and (b) other persons at the place of work concerned, are aware of and comply with the relevant technical or organisational measures referred to in subsection (1).
Data Protection Act 2018, s 86(3).	Subsection (1) shall not apply where, taking into account the nature of the personal data and the scope, context and purposes of the processing, the personal data breach is

	unlikely to result in a risk to the rights and freedoms of data subjects.
Data Protection Act 2018, s 87.	(1) Subject to subsections (2), (4) and (7), where a personal data breach occurs that is likely to result in a high risk to the rights and freedoms of a data subject, the controller shall, without undue delay, notify the data subject to whom the breach relates. (2) Subsection (1) shall not apply where— (a) the controller has implemented appropriate technological and organisational protection measures that were applied to the personal data affected by the personal data breach, in particular where the said measures, including encryption, render the personal data unintelligible to any person who is not authorised to access it, or (b) the controller has taken measures in response to the personal data breach that ensure that the high risk to the rights and freedoms of a data subject from the breach is no longer likely to materialise. (3) A notification under subsection (1) shall— (a) describe, in clear and plain language, the nature of the personal data breach concerned, and (b) contain at least the information specified in paragraphs (b) to (d) of section 86(4). (4) Where a notification under subsection (1) would involve a disproportionate effort, the controller shall notify the data subjects concerned of the personal data breach by way of public communication or other similar measure that ensures the data subjects are informed of the personal data breach in an equally effective manner. (5) A notification under subsection (4) shall— (a) describe, in clear and plain language, the nature of the personal data breach concerned, and (b) contain such other information as is appropriate in all the circumstances.

	(6) Where— (a) a controller notifies the Commission under section 86 of a personal data breach, and (b) the controller has not notified the data subject to whom the personal data relate under subsection (1) or (4), as the case may be, of the personal data breach, the Commission may, having considered the likelihood of the data breach resulting in a high risk to the rights and freedoms of a data subject— (i) require the controller to notify the data subject under subsection (1) or (4), as the case may be, or (ii) determine that subsection (2) applies in relation to the personal data breach. (7) A controller may, in relation to the exercise of the right of a data subject to be notified under subsection (1) of a personal data breach, restrict the exercise of the said right where to do so constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and legitimate interests of the data subject, for a purpose specified in section 94(2). (8) Where a controller restricts the exercise of the right of a data subject under subsection (7), subsections (5), (6) and (7) of section 94 shall apply in respect of the said restriction, with all necessary modifications.
Data Protection Act 2018, s. 116.	(1) The Commission shall— (a) as soon as practicable after it makes a decision under section 111 or 112, give the controller or processor concerned a notice in writing setting out— (i) the decision and the reasons for it, and (ii) where applicable, the corrective power that the Commission has decided to exercise in respect of the controller or processor, and (b) in the case of a decision under section 112, and as soon as practicable after the

	giving of the notice under paragraph (a), give the complainant concerned a notice in writing setting out— (i) the decision and the reasons for it, and (ii) where applicable, the corrective power that the Commission has decided to exercise in respect of the controller or processor. (2) Subject to subsection (4), the Commission shall— (a) as soon as practicable after it adopts a decision under section 113(2)(b), give the controller or processor concerned a notice in writing setting out— (i) the decision and the reasons for it, and (ii) where applicable, the corrective power that the Commission has decided to exercise or, as the case may be, the action that it has decided to take, in respect of the controller or processor, and (b) in the case of a complaint lodged with the Commission, and as soon as practicable after the giving of the notice under paragraph (a), give the complainant concerned a notice in writing setting out— (i) the decision and the reasons for it, and (ii) where applicable, the corrective power that the Commission has decided to exercise or, as the case may be, the action that it has decided to take, in respect of the controller or processor. (3) The Commission shall, as soon as practicable after it adopts a decision under section 114, give— (a) the complainant concerned, and (b) the controller or processor concerned, a notice in writing informing them of the rejection or dismissal of the complaint or, as the case may be, the part of the complaint. (4) Where the Commission is the lead supervisory authority in relation to a complaint to which Article 60(9) applies, the

	Commission shall, as soon as practicable after it adopts its decision under Article 60(9)— (a) give the controller or processor concerned, at its main establishment or single establishment, a notice in writing setting out— (i) the decision and the reasons for it, and (ii) where applicable, the corrective power that the Commission has decided to exercise or, as the case may be, the action that it has decided to take in respect of the controller or processor, and (b) give the complainant concerned a notice in writing setting out— (i) the decision and the reasons for it, and (ii) where applicable, the corrective power that the Commission has decided to exercise or, as the case may be, the action that it has decided to take in respect of the controller or processor.
Data Protection Act 2018, s. 117.	(1) Subject to subsection (9), and without prejudice to any other remedy available to him or her, including his or her right to lodge a complaint, a data subject may, where he or she considers that his or her rights under a relevant enactment have been infringed as a result of the processing of his or her personal data in a manner that fails to comply with a relevant enactment, bring an action (in this section referred to as a "data protection action") against the controller or processor concerned. (2) A data protection action shall be deemed, for the purposes of every enactment and rule of law, to be an action founded on tort. (3) The Circuit Court shall, subject to subsections (5) and (6), concurrently with the High Court, have jurisdiction to hear and determine data protection actions. (4) The court hearing a data protection action shall have the power to grant to the plaintiff one or more than one of the following reliefs:

	(a) relief by way of injunction or declaration; or (b) compensation for damage suffered by the plaintiff as a result of the infringement of a relevant enactment. (5) The compensation recoverable in a data protection action in the Circuit Court shall not exceed the amount standing prescribed, for the time being by law, as the limit of that court's jurisdiction in tort. (6) The jurisdiction conferred on the Circuit Court by this section may be exercised by the judge of any circuit in which— (a) the controller or processor against whom the data protection action is taken has an establishment, or (b) the data subject has his or her habitual residence. (7) A data protection action may be brought on behalf of a data subject by a not-for-profit body, organisation or association to which Article 80(1) applies that has been mandated by the data subject to do so. (8) The court hearing a data protection action brought by a not-for-profit body, organisation or association under subsection (7) shall have the power to grant to the data subject on whose behalf the action is being brought one or more of the following reliefs: (a) relief by way of injunction or declaration; or (b) compensation for damage suffered by the plaintiff as a result of the infringement of the relevant enactment. (9) A data subject may not bring a data protection action against a controller or processor that is a public authority of another Member State acting in the exercise of its public powers. (10) In this section— "damage" includes material and non-material damage; "injunction" means— (a) an interim injunction,

	(b) an interlocutory injunction, or (c) an injunction of indefinite duration.
Data Protection Act 2018, s. 144.	144. (1) Personal data processed by a processor shall not be disclosed by the processor or by an employee or agent of the processor, without the prior authority of the controller on behalf of whom the data are processed. (2) A person who knowingly or recklessly contravenes subsection (1) shall be guilty of an offence and shall be liable— (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or (b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both. (3) Subsection (1) does not apply to a person who shows that the disclosing concerned was required or authorised by or under any enactment, rule of law or order of a court.
Data Protection Act 2018, s. 150.	(1) A controller or processor on which an information notice or enforcement notice or a notice under section 135(1) is served may, within 28 days from the date on which the notice is served, appeal against a requirement specified in the notice. (2) The court, on hearing an appeal under subsection (1), shall— (a) annul the requirement concerned, (b) substitute a different requirement for the requirement concerned, or (c) dismiss the appeal. (3) This subsection applies to an appeal brought under subsection (1)— (a) against a requirement specified in an information notice to which section 132(3) applies, or an enforcement notice to which section 133(6) applies, and (b) that is brought within the period specified in the notice concerned. (4) Notwithstanding any provision of this Act, the court, on hearing an appeal to which

	subsection (3) applies, may on application to it in that behalf, determine that non-compliance by the controller or processor concerned with a requirement specified in the notice, during the period ending with the determination or withdrawal of the appeal or during such other period as the court may determine, shall not constitute an offence. (5) A data subject or other person affected by a legally binding decision of the Commission under Chapter 2 or 3 may, within 28 days from the date on which notice of the decision is received by him or her, appeal against the decision. (6) The court, on hearing an appeal under subsection (5), shall— (a) annul the decision concerned, (b) substitute its own determination for the decision, or (c) dismiss the appeal. (7) Where the Commission, being the competent supervisory authority in respect of a complaint within the meaning of Chapter 2 or 3, does not comply with section 108(2) or, as the case may be, section 121(2), the complainant concerned may apply to the court for an order under subsection (8)(a). (8) The court, on hearing an application under subsection (7), shall— (a) order the Commission to comply with the provision concerned, or (b) dismiss the application. (9) The Circuit Court shall, concurrently with the High Court, have jurisdiction to hear and determine proceedings under this section. (10) The jurisdiction conferred on the Circuit Court by this section shall be exercised by the judge for the time being assigned to the circuit where— (a) in the case of an appeal under subsection (1), the controller or processor is established, (b) in the case of an appeal under subsection (5), the data subject or other person resides or is established, or

	(c) in the case of an application under subsection (7), the data subject resides, or, at the option of the controller, processor, data subject or person concerned, by a judge of the Circuit Court for the time being assigned to the Dublin circuit. (11) A decision of the Circuit Court or High Court, as the case may be, under this section shall be final save that an appeal shall lie to the High Court or Court of Appeal, as the case may be, on a point of law. (12) For the purposes of this section, a "legally binding decision" means a decision— (a) under paragraph (a) or (b) of section 109(5) or paragraph (a) or (b) of section 122(4), (b) under section 111(1)(a), 112(1), 113(2)(b), 114, 124(1)(a) or 125(1), or (c) to exercise a corrective power under Chapter 2 or 3.
Data Protection Act 2018, s. 59.	The right of a data subject to object at any time to the processing of personal data concerning him or her under Article 21 shall not apply to processing carried out— (a) in the course of electoral activities in the State by— (i) a political party, or (ii) a candidate for election to, or a holder of, elective political office in the State, and (b) by the Referendum Commission in the performance of its functions.
Data Protection Act 2018, s. 60.	(1) The rights and obligations provided for in Articles 12 to 22 and Article 34, and Article 5 in so far as any of its provisions correspond to the rights and obligations in Articles 12 to 22— (a) are restricted to the extent specified in subsection (3), and (b) may be restricted in regulations made under subsections (5) or (6).

	(2) Subsection (1) is without prejudice to any other enactment or rule of law which restricts the rights and obligations referred to in that subsection. (3) Subject to subsection (4), the rights and obligations referred to in subsection (1) are restricted to the extent that— (a) the restrictions are necessary and proportionate— (i) to safeguard cabinet confidentiality, parliamentary privilege, national security, defence and the international relations of the State, (ii) for the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties, (iii) for the administration of any tax, duty or other money due or owing to the State or a local authority in any case in which the non-application of the restrictions concerned would be likely to prejudice the aforementioned administration, (iv) in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure, (v) for the enforcement of civil law claims, including matters relating to any liability of a controller or processor in respect of damages, compensation or other liabilities or debts related to the claim, or (vi) for the purposes of estimating the amount of the liability of a controller on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the commercial interests of the controller in relation to the claim, (b) the personal data relating to the data subject consist of an expression of opinion about the data subject by another person

	given in confidence or on the understanding that it would be treated as confidential to a person who has a legitimate interest in receiving the information, or (c) the personal data concerned are kept— (i) by the Commission for the performance of its functions, (ii) by the Information Commissioner for the performance of his or her functions, or (iii) by the Comptroller and Auditor General for the performance of his or her functions. (4) The Minister may prescribe requirements to be complied with when the rights and obligations referred to in subsection (1) are restricted in accordance with subsection (3). (5) Subject to subsection (9), regulations may be made by a Minister of the Government where he or she considers it necessary for the protection of a data subject or the rights and freedoms of others restricting the rights and obligations referred to in subsection (1)— (a) (i) if the application of those rights and obligations would be likely to cause serious harm to the physical or mental health of the data subject, and (ii) to the extent to which, and for as long as, such application would be likely to cause such serious harm, and (b) in relation to personal data kept for, or obtained in the course of, the carrying out of social work by a public authority, public body, a voluntary organisation or other body. (6) Subject to subsection (9), regulations may be made restricting the rights and obligations referred to in subsection (1) where such restrictions are necessary for the purposes of safeguarding important objectives of general public interest and such regulations shall include, where appropriate, specific provisions required by Article 23(2). (7) Important objectives of general public interest referred to in subsection (6) include:

	(a) preventing threats to public security and public safety; (b) avoiding obstructions to any official or legal inquiry, investigation or process, including any out-of-court redress procedure, proceedings pending or due before a court, tribunal of inquiry or commission of investigation; (c) preventing, detecting, investigating and prosecuting breaches of discipline by, or the unfitness or incompetence of, persons who are or were authorised by law to carry on a profession or any other regulated activity and the imposition of sanctions for same; (d) preventing, detecting, investigating or prosecuting breaches of ethics for regulated professions; (e) taking any action for the purposes of considering and investigating a complaint made to a regulatory body in respect of a person carrying out a profession or other regulated activity where the profession or activity is regulated by that body and the imposition of sanctions on foot of such a complaint; (f) preventing, detecting, investigating or prosecuting, whether in the State or elsewhere, breaches of the law which are subject to civil or administrative sanctions and enforcing such sanctions; (g) the identification of assets which are derived from, or are suspected to derive from, criminal conduct and the taking of appropriate action to deprive or deny persons of those assets or the benefits of those assets and any investigation or preparatory work in relation to any related proceedings; (h) ensuring the effective operation of the immigration system, the system for granting persons international protection in the State and the system for the acquisition by persons of Irish citizenship, including by preventing, detecting and investigating abuses of those systems or breaches of the law relating to those systems;

	(i) safeguarding the economic or financial interests of the European Union or the State, including on monetary, budgetary and taxation matters; (j) safeguarding monetary policy, the smooth operation of payment systems, the resolution of regulated financial service providers (within the meaning of the Central Bank Act 1942), the operation of deposit- guarantee schemes, the protection of consumers and the effective regulation of financial service providers (within the meaning of the Central Bank Act 1942); (k) protecting members of the public against— (i) financial loss or detriment due to the dishonesty, malpractice or other improper conduct of, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate or other entities, (ii) financial loss or detriment due to the conduct of individuals who have been adjudicated bankrupt, or (iii) financial loss or detriment due to the conduct of individuals who have been involved in the management of a body corporate which has been the subject of a receivership, examinership or liquidation under the Act of 2014; (l) protecting— (i) the health, safety, dignity, well-being of individuals at work against risks arising out of or in connection with their employment, and (ii) members of the public against discrimination or unfair treatment in the provision of goods or services to them; (m) the keeping of public registers for reasons of general public interest, whether the registers are accessible to the public on a general or restricted basis; (n) safeguarding the integrity and security of examinations systems;

	(o) safeguarding public health, social security, social protection and humanitarian activities. (8) Where the rights and obligations referred to in subsection (1) are restricted in regulations made under subsection (6) on the basis of important objectives of general public interest of the State, other than the objectives referred to in subsection (7), the important objective or objectives of general public interest shall be identified in those regulations. (9) Subject to subsection (10), regulations may be made under subsection (5) or (6)— (a) by the Minister following consultation with such other Minister of the Government as he or she considers appropriate, or (b) by any other Minister of the Government following consultation with the Minister and such other Minister of the Government as he or she considers appropriate. (10) The Minister or any other Minister of the Government shall consult with the Commission before making regulations under subsection (5) or (6). (11) The Commission may, on being consulted under subsection (10), make observations in writing on any matter which is of significant concern to it in relation to the proposed regulations and, if the Minister or any other Minister of the Government proposes to proceed to make the regulations notwithstanding that concern, that Minister shall, before making the regulations, give a written explanation as to why he or she is so proceeding to— (a) the Committee established jointly by Dáil Éireann and Seanad Éireann known as the Committee on Justice and Equality or any Committee established to replace that Committee, and (b) any other Committee (within the meaning of section 19(1)) which that Minister considers appropriate having regard to the subject matter of the regulations.

	(12) Regulations made under this section shall— (a) respect the essence of the right to data protection and protect the interests of the data subject, and (b) restrict the exercise of data subjects' rights only in so far as is necessary and proportionate to the aim sought to be achieved.
Data Protection Act 2018, s.85.	Where a processor becomes aware of a personal data breach, the processor shall notify the controller on whose behalf the data are being processed of the breach— (a) in writing, and (b) without undue delay.
Data Protection Act 2018, s141	(1) The Commission, in considering— (a) whether to make a decision to impose an administrative fine, and (b) where applicable, the amount of such a fine, shall act in accordance with this section and Article 83. (2) Where a controller to whom section 111(2)(b), 112(2)(b) or 133(9) applies is a controller by virtue of his or her being the subject of a designation under subsection (1) or (2) of section 3, a decision by the Commission to impose an administrative fine in respect of the infringement or failure concerned shall be a decision to impose an administrative fine on the appropriate authority that, or, as the case may be, the Minister who, made the designation, and not on the controller. (3) Where subsection (2) applies, a reference in sections 115(1)(a), 133(9)(b) and this Chapter to a controller shall be construed as a reference to the appropriate authority or Minister concerned. (4) Where the Commission decides to impose an administrative fine on a controller or processor that— (a) is a public authority or a public body, but

	(b) is not a public authority or a public body that acts as an undertaking within the meaning of the Competition Act 2002, the amount of the administrative fine concerned shall not exceed €1,000,000. (5) The Commission, as soon as practicable after— (a) a decision to impose an administrative fine is confirmed under section 142(3)(a) or 143(2), or (b) the court decides, under section 142(3)(b), to impose a different fine, shall give the controller or processor concerned a notice in writing, requiring the controller or processor to pay the amount of the fine concerned to the Commission within the period of 28 days commencing on the date of the notice. (6) A controller or processor shall comply with a requirement referred to in subsection (5). (7) All payments received by the Commission under this section shall be paid into or disposed of for the benefit of the Exchequer in such manner as the Minister for Finance may direct. (8) In this section and section 142, a reference to a decision to impose an administrative fine shall be construed as a reference to a decision by the Commission, under section 111, 112, 113 or 133 (9), to impose such a fine.
Data Sharing and Governance Act 2019, s 19.	(1) A data-sharing agreement shall— 1. (a) specify the names of the parties to the agreement in a schedule to the agreement, 2. (b) specify the information to be disclosed, 3. (c) specify the purpose of the data-sharing, 4. (d) specify the function of the public body concerned to which the purpose referred to in paragraph (c) relates,

	5. (e) specify the legal basis for the data-sharing and for any further processing, by the parties to the agreement, of the information to be disclosed under the agreement, 6. (f) specify whether the impetus for the disclosure of information under the agreement will come from a data subject or a public body, 7. (g) specify whether, where information is disclosed under the agreement, the disclosure will be of information in relation to individual data subjects or classes of data subjects, 8. (h) specify whether the disclosure of information under the agreement will be on a once-off or ongoing basis, 9. (i) specify how the information to be disclosed is to be processed following its disclosure, 10. (j) specify any restrictions on the disclosure of information after the processing referred to in paragraph (i), 11. (k) include an undertaking by the parties to the agreement to comply with Article 5 of the General Data Protection Regulation in disclosing information under the agreement, (l) where a data protection impact assessment has been carried out in relation to the data-sharing, include a summary of the matters referred to in Article 35(7) of the General Data Protection Regulation in a schedule to the agreement, (m) (n) (o) (p) (q) (r) Data Sharing and Governance Act 2019 [No. 5.] PT.4 S.19 specify the security measures to apply to the transmission, storage and accessing of personal data, in a manner that does not compromise those security measures, specify the requirements in relation to the retention of—

	(i) the information to be disclosed, and (ii) the information resulting from the processing of that information, for the duration of the agreement and in the event that the agreement is terminated, specify the method to be employed to destroy or delete— (i) the information to be disclosed, and (ii) the information resulting from the processing of that information, at the end of the period for which the information is to be retained in accordance with the agreement, specify the procedure in accordance with which a party may withdraw from the agreement, include such other matters as may be prescribed under subsection (2), include in a schedule to the agreement a statement summarising the analysis of the parties in relation to the extent to which— 1. (i) the disclosure of the information is necessary for the performance of the functions in relation to which the information is being disclosed, and 2. (ii) the disclosure and safeguards applicable to that disclosure are proportionate in the context of the performance of those functions and the effects of the disclosure on the rights of the data subjects concerned. (2) The Minister may prescribe matters, in addition to those listed in subsection (1), to be included in a data-sharing agreement where he or she is satisfied that the inclusion of those matters would— (a) be consistent with Article 5(1) of the General Data Protection Regulation, and (b) (i) improve transparency as regards the sharing of information by public bodies, or (ii) facilitate good governance in the sharing of information by public bodies.

	(3) A data-sharing agreement may provide for matters in addition to those listed in subsection (1).
Employment Equality Act 1998, s 27(1)(a)(i).	applies to the assignment of a man or, as the case may require, a woman to a particular post where this is essential— (i) in the interests of privacy or decency.
EU Charter of Fundamental Rights 2000, Article 7.	Respect for private and family life Everyone has the right to respect for his or her private and family life, home and communications.
EU Charter of Fundamental Rights 2000, Article 7.	Protection of personal data 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.
European Convention on Human Rights Act 2003, s 2(1).	In interpreting and applying any statutory provision or rule of law, a court shall, in so far as is possible, subject to the rules of law relating to such interpretation and application, do so in a manner compatible with the State's obligations under the Convention provisions.
General Data Protection Regulation 2018, Article 33.	1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data

	breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach. 3. The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. 4. Where, and in so far as, it is not possible to provide the information at the same time, the information may

	be provided in phases without undue further delay. 5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.
Irish Constitution Article 40.3.1	1° the state acknowledges that man, in virtue of his rational being, has the natural right, antecedent to positive law, to the private ownership of external goods. 2° the state accordingly guarantees to pass no law attempting to abolish the right of private ownership or the general right to transfer, bequeath, and inherit property.
Irish Constitution Article 40.3.2	The state shall, in particular, by its laws protect as best it may from unjust attack and, in the case of injustice done, vindicate the life, person, good name, and property rights of every citizen.
Irish Constitution Article 40.5	The dwelling of every citizen is inviolable and shall not be forcibly entered save in accordance with law.
Mental Health Act 2001, s 4(3).	In making a decision under this Act concerning the care or treatment of a person (including a decision to make an admission order in relation to a person) due regard shall be given to the need to respect the right of the person to dignity, bodily integrity, privacy and autonomy.

Bibliography

English titles

Legislation

Adoption Act 2008

Council and Parliament 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).

Council Directive 1995/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281.

Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105.

Council of the European Union, Council Resolution on Law Enforcement Operational Needs with Respect to Public Telecommunication Networks and Services, June 20, 2001.

Criminal Justice (Theft and Fraud Offences) Act, 2001.

Data Protection Act 1988.

Data Protection Act 2014.

Data Protection Act 2018.

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 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 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.

Directive 2016/1148 EU 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.

Directive 2018/1972 EU of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.

Employment Equality Act 1998.

EU Charter of Fundamental Rights 2000.

European Convention on Human Rights Act 2003.

General Data Protection Regulation 2018.

Mental Health Act 2001.

Proceeds of Crime (Amendment) Act 2005.

S.I No. 336/2011- European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011.

S.I No. 526/2008 - European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008.

S.I. No. 360/2018 - European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018.

Reports

An Coimisiún um Chosaint Sonraí (Data Protection Commission) 'Commonly Asked Questions about the Basics of Data Protection' (version updated July 2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190710%20Data%20Protection%20Basics.pdf> accessed 19 February 2021.

Council of Europe DGI (2-19) 05, 'A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework' <https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168096bdab> accessed 31 May 2021.

Data Protection Commission, Annual Report 2011 (2011) 22.

Department of Communications, Energy & Natural Resources, 'Doing More with Digital: National Digital Strategy for Ireland' (2013) <https://assets.gov.ie/27518/7081cec170e34c39b75cbec799401b82.pdf> date accessed 24 May 2021.

Department of Public Expenditure and Reform, 'Enabling Digital Ireland: A Summary Report on Ireland's Ambition to Be a Leader in the Provision of Digital Government Services' (2018) <https://pulse.microsoft.com/uploads/prod/2018/08/Enabling-Digital-Ireland-Whitepaper.pdf>.Date Accessed 24 May 2021.

Department of Public Expenditure and Reform, Enabling Digital Ireland (2018).

Department of the Environment, Climate and Communications, 'European Electronic Communications Code (EECC)' <https://www.gov.ie/en/publication/339a9-european-electronic-communications-code-eecc/> accessed 24 February 2021.

Department of the Environment, Climate and Communications, 'National Digital Strategy' <https://www.gov.ie/en/publication/f4a16b-national-digital strategy/> accessed 24 February 2021.

Departure of Public Expenditure and Reform on 1 June 2017 at <https://www.gov.ie/en/publication/63a31-egovernment-strategy-20172020/> accessed 27 February 2021.

End-User Rights text of draft Statutory Instrument transposing the European Electronic Communications Code <https://assets.gov.ie/77304/24998a57-3f1e-4bdb-9a72-f7bfec561bac.pdf> accessed 24 February 2021.

European Commission, 'Digital Economy and Society Index (DESI) 2020' (2020) 63 <https://ec.europa.eu/digital-single-market/endigital-economy-and-society-index-desi> date accessed 24 May 2021.

European Commission, 'Report from the Commission to the European Parliament and the Council Assessing the Consistency of the Approaches Taken by Member States in the Identification of Operators of Essential Services in Accordance with Article 23(1) of Directive 2016/1148/EU on Security of Network and Information Systems COM/2019/546 Final' (2019).

Human Rights Council, Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights (2020) <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf> accessed March 01, 2021.

Law Reform Commission, Report on Privacy (LRC 1998)

National Cyber Security Centre, 'National Cyber Security Strategy 2019-2024' (2019) 8 <https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf> accessed 31 May 2021.

The Law Library of Congress, 'Government Access to Encrypted Communications', <https://www.loc.gov/law/help/encrypted-communications/gov-access.pdf> accessed 25 February 2021.

Books

Byrne et al, The Irish Legal System (Seventh edition, Bloomsbury Professional 2020).

Doyle, O, and Hickey, T, Constitutional Law: Text, Cases and Materials (2nd edn, Clarus Press 2019).

Kelleher, D, Privacy and Data Protection Law in Ireland (2nd edn, Bloomsbury 2016).

Kelly, J, and Treacy, A, 'Republic of Ireland' in Monika Kuschewsky, Van Bael & Bellis, Data Protection & Privacy: Jurisdictional comparisons (Thomas Reuters 1st edn 2012).

McMahon, B, and Binchy, W, The Law of Torts (4th edn, Butterworths 2013).

Periodicals

Cannon, E, 'Data Protection Act 2018' (2018) 23(3) The Bar Review 79.

Casey, E, 'Practical Approaches to Recovering Encrypted Digital Evidence', (2002) Vol 1(3) International Journal of Digital Evidence.

Chakravorti et al, 'Digital in the Time of Covid' (2020) Digital Intelligence Index at 23 <https://sites.tufts.edu/digitalplanet/files/2020/12/digital-intelligence-index.pdf> accessed 28 February 2021.

Denning, D. E, 'Hiding Crimes in Cyberspace', (1999) Vol 2(3) Information, Communication and Society.

Dickson, B, 'Ireland's Human Rights Commission' 36 Irish Jurist (NS) 265.

Dietschy, L, 'GDPR Series: New Obligations on Data Processors' (2018) 18(4) Privacy and Data Protection.

Doyle, O, 'Constitutional Equality in Ireland: A Critical Account' Trinity College Dublin, Ireland School of Law 2004.

Egan, 'The European Convention on Human Rights Act 2003: A Missed Opportunity for Domestic Human Rights Litigation' (2003) 25 DULJ.

Elliot, S, 'The Right to Encryption? An Examination of Cryptography Law and Jurisprudence in the UK', Trinity College Law Review <https://trinitycollegelawreview.org/right-to-encryption/> accessed February 2021.

Foale, N 'Back to the Future: How Well Equipped Is Irish Employment Equality Law to Adapt to Artificial Intelligence?' (2020) 23 Trinity CL Rev 170.

Hirsch, D.D, 'The Law and Policy of Online Privacy: Regulation, Self – Regulation or Co – Regulation?' (2011) 34 Seattle University Law Review 439-480.

Kelly, R and Swaby, G, 'Consumer Protection Rights and "Free" Digital Content' (2017) 23(7) Computer and Telecommunications Law Review 165-170.

Kennedy, R and Murphy, M. H., Information and Communications Technology Law in Ireland (2017).

Kim, P. T., 'Data-Driven Discrimination at Work' (2017) 58 William and Mary Law Review 857.

Listokin, S, 'Industry Self-Regulation of Consumer Data Privacy and Security' (2016) 32(1) John Marshall Journal of Information Technology 15-41.

McIntyre, TJ, 'Regulating the Information Society: Data Protection and Ireland's Internet Industry' in David Farrell and Niamh Hardiman (eds), The Oxford Handbook of

Irish Politics (Oxford University Press, forthcoming 2021).

McLaughlin, S, 'Ireland: A brief Overview of the Implementation of the GDPR' (2018) 4 Eur Data Prot L Rev 227.

Mulligan, A, 'Case Comment: Constitutional Aspects of International Data Transfer and Mass Surveillance' 2016 Irish Jurist 207.

Murphy, T, 'The Justiciability of Data Protection Laws in Ireland: A New Dawn of Civil Litigation?' (2020) 27(11) CLP 238.

O'Dell, E, 'Compensation for Breach of the General Data Protection Regulation' (2017) 40(1) Dublin University Law Journal 99.

Shyy, S, 'The GDPR's Lose - Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business' (2019) 20 UC Davis Business Law Journal 156.

Wade, G, 'The Insurability of Fines and Sanctions Under the GDPR' (2018) 36(18) Irish Law Times 280.

Digital resources

'Commission Opens Infringement Procedures against 24 MS' (European Commission - European Commission) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_206> accessed 24 February 2021.

'Encryption: finding the balance between privacy, security and lawful data access', Digital Europe (16 March 2020) <https://www.digitaleurope.org/wp/wp-content/uploads/2020/03/DIGITALEUROPE-Position-on-Encryption-Policy-.pdf> accessed February 24, 2021.

'Europol and the European Commission Inaugurate New Decryption Platform to Tackle the Challenge of Encrypted Material for Law Enforcement Investigations', Europol (18 December 2020).

'Government Access to Encrypted Communications: European Union', The Law Library of Congress (30/12/2020) <https://www.loc.gov/law/help/encrypted-communications/european-union.php> accessed February 24, 2021.

'Mother secures order to stop use of child's image on eBay' The Irish Times (Dublin, 20 April 2020)

<https://www.irishtimes.com/news/crime-and-law/courts/high-court/mother-secures-order-to-stop-use-of-child-s-image-on-ebay-1.4233304?mode=amp> accessed 27 February 2021.

'NCSC: National Cyber Security Centre' <https://www.ncsc.gov.ie/> accessed 24 February 2021.

<https://www.bbvaresearch.com/wp-content/uploads/2018/10/Watch_Self-regulation-and-data-protection-1.pdf> accessed 12 March 2021.

<https://www.europol.europa.eu/newsroom/news/europol-and-european-…rm-to-tackle-challenge-of-encrypted-material-for-law-enforcement> accessed February 25, 2021.

<https://www.fdiintelligence.com/article/78473> accessed 12 March 2021.

Conway, J, 'Big Tech Picks Ireland as Data Centre Hub' (FDI Intelligence, 17 August 2020).

O Keefe, C, 'Gardaí call to access digital devices to tackle online child abuse imagery', The Irish Examiner (10 February 2020) <https://www.irishexaminer.com/news/arid-30980947.html> accessed 26 February 2021.

Council of the European Union, Council Resolution on Law Enforcement Operational Needs with Respect to Public Telecommunication Networks and Services, June 20, 2001, <https://www.statewatch.org/media/documents/news/2001/sep/9194.pdf> accessed at 25 February 2021.

Department for Business, Energy and Industrial Strategy, 'Industrial Strategy: Building a Britain fit for the future' (HM Government 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachme

nt_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf> accessed 14 March 2021.

Department of Justice, Dáil Éireann Irish Human Rights and Equality Commission Bill 2014 Second Stage Speech 8 April 2014 Alan Shatter, TD, Minister for Justice, Equality and Defence - The Department of Justice accessed 31 May 2021.

Equality and Human Rights Commission, 'What are Human Rights?' (Human Rights, 19 June 2019) <https://www.equalityhumanrights.com/en/human-rights/what-are-human-rights> accessed 28 February,

2021.

European Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ 2 215/7.

European Commission Statement "Statement by President von der Leyen at the roundtable 'Internet, a new human right' after the intervention by Simona Levi" Brussels, 28 October 2020 <https://ec.europa.eu/commission/presscorner/detail/en/statement_20_200> accessed 28 February 2021.

Goodbody, W, 'Twitter fined €450,000 by Data Protection Commission for data breach' (RTÉ Business News, 15 December 2020) <https://www.rte.ie/news/business/2020/1215/1184537-twitter-fined-by-data-protection-commission/> accessed 27 February 2021.

O'Dell, E, 'Ireland: Damages for Data Protection Breaches, 1: Why Collins v FBD Insurance is wrong (again)' (Informs' Blog, 19 December 2019) <https://inforrm.org/2019/12/19/ireland-damages-for-data-protection-breaches-1-why-collins-v-fbd-insurance-is-wrong-again-eoin-odell> accessed 27 February 2021.

Open Global Rights, 'How can technology be a powerful force in support of human rights?' (Technology and Human Rights, April 2018) <https://www.openglobalrights.org/technology/> accessed March 01, 2021.

Runnegar, C, 'Encryption and Law Enforcement Can Work Together', Internet Society <https://www.internetsociety.org/blog/2017/10/encryption-law-enforcement-can-work-together/> accessed February 24, 2021.

Scott, M, 'Irish Regulator Says Country Will Stay at Centre of Online Privacy Debate' The New York Times (New York, 23 June 2015) accessed 22 February 2021.

Segovia Domingo, A. I, and Desmet Villar, N, 'Self-Regulation in Data Protection' [2018] BBVA Research United Nations, 'Human Rights' (What are human rights) <https://www.un.org/en/global-issues/human-rights> accessed 31 May 2021.

Case-law

C-293/12 and C-594/12 Digital Rights Ireland Ltd and Seitlinger and Others (2014) ECJ.

Case 311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2018] ECLI 559.

Case 362/14 Maximillian Schrems v Data Protection Commissioner [2014] ECLI 238.

Collins v FBD Insurance plc [2013] IEHC 137.

Damache v DPP [2011] IEHC 197 (High Court); [2012] IESC 11 (Supreme Court).

Duggan v Commissioner of An Garda Síochána [2017] IEHC 565.

EMI v DPC [2012] IEHC 264.

Friends of the Irish Environment v The Government of Ireland [2020] IESC 49 31.

Kennedy v United Kingdom, application 26839/05, 18 May 2010.

Klass v Germany, application 5029/71, 6 September 1978.

Malone v United Kingdom, application 8691/79, 2 August 1984.

McGee v Attorney General [1974] IR 284.

Norris v Attorney General [1984] IR 36.

Schrems v Data Protection Commissioner [2014] IEHC 310.

Sullivan v Boylan (no 2) [2013] IEHC 104.

Weber and Saravia v. Germany, application 54934/00, 29 June 2006.

ELSA NORWAY

Contributors

National Coordinator
Sigurd Dyvik Vasseljen

National Researchers
Aleksandra Tomasiewicz
Amund Nørstebø
Anders Stray Bugge
Brage Breivik
Cathrine Kolle Varden
Emil Støten
Herman Andersen Kartnes
Leila Hadjaeva
Lina Breivik
Maria Lie Jordheim
Selma Treu Breimo
Snorre Sanner Sjaastad
Svetlana Zaychenko
Åsa Friedmann

National Linguistic Editors
Amalie Anda Vangen
Olivia S. Sánchez

National Technical Editor
Frida Åberg Mokkelbost

National Academic Supervisor
Cecilie Hellestveit

Introduction

The Norwegian society is one of the most digitised in the world. Norway is also internationally recognised as a world-leading welfare state, where democracy and human rights are integral parts. Norway has therefore a promising foundation for ethical integration of the advanced digital technologies.

In the following report we are aiming to give a perspective on the current state of digitalisation in Norway, with a particular focus on the digitised public and health sector. These areas are actively prioritised by the authorities, and can illustrate the current and upcoming challenges of creating a safe and unified digital system.

The authorities recognise that technological development in many ways goes faster than the relevant policy and legislation processes.[214] This particular problem was brought to life during the COVID-19 pandemic, where the Norwegian contact-tracing app (Smittestopp) received strong national and international criticism for neglecting privacy for efficiency.[215] The criticism led to the application being banned, which in its turn led to improving the privacy control settings. Instead of storing the user information on the central governmental server in Ireland, the new app was made to store relevant information only on the phones, avoiding the central server and limiting potential misuse.

This limitation is especially important in the light of possible DNA-disclosures by the government without the subject's consent. The question of such a possibility was posed to the Supreme Court of Norway in 2018, where the DNA material of a deceased person was requested for a paternity test. The Court found that such a disclosure will be in accordance with the law.[216]

This illustrates that Norwegian legislation is not fully adjusted to the rapid technological development, and is therefore a subject for difficult technical and ethical assessments.

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

In recent years, advanced digital technologies have been an important agenda for the development of the public and private sectors in Norway. By advanced digital technology, we mean both technological innovations that contribute to digitalisation as well as the use of Artificial Intelligence (AI). The investment in digitalisation in the Norwegian public sector has been a particularly important political priority. In 2019, the current Norwegian

---

[214] Justis- og beredskapsdepartementet og Forsvarsdepartementet, Nasjonal strategi for digital sikkerhet (2019), p. 7.
[215] See e.g. "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy", *Amnesty International* (16 June 2020) <www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/> accessed 24 February 2021.
[216] HR-2018-2241-U.

government prepared a strategy for further digitalisation of the public sector that will apply from 2019 to 2025. One of the areas which is emphasised, is the focus on optimisation and AI. The goal of the project is to increase the availability of the public sector for users. Through this strategy, every government agency must go through a digital transformation. This applies in particular to public services such as the health sector, norwegian labour and welfare administration or the tax authorities.[217]

The investment in digitalisation and technological innovation has led Norway, together with other Nordic countries, to be well under way with digital transformation, compared to other European countries. The focus on digitalisation has resulted in Norway topping the report on the Digital Economy and Society Index (DESI), every year. It was last published in 2020, and Norway came in third place, right after Sweden and Finland.[218]

The extensive digitalisation of the Norwegian public and private sectors has provided various benefits. However, the process also poses several challenges. Many of these challenges result in what can be described as human rights violations.

The importance of human rights is emphasised by the Norwegian government in the report "National strategy for artificial intelligence". In this report, the government states that "artificial intelligence developed and used in Norway shall be based on ethical principles, and respect human rights and democracy". [219]

The outstanding challenge of using AI, especially in the public sector, among other factors, has been the danger of discrimination due to the use of algorithms. Morten Goodwin, Deputy Head of the Center for Artificial Intelligence Research at the Norwegian University of Agder, has stated in his article that one should now read to create an algorithm oversight to ensure that computer systems with AI do not discriminate in ways that may be difficult to detect. [220]

In 2019, The Norwegian Institute for Human Rights (NIM) published the report «Elderly human rights: seven challenges». The report illustrated how digitalisation can weaken human rights for the elderly population of Norway. According to NIM, limited access to digital services can lead to the elderly population in Norway being restricted in their freedom of expression and information. The elderly population is included by the Convention on the Rights of Persons with Disabilities (CRPD). This is a convention that

---

[217] Kommunal- og moderniseringsdepartementet, En digital offentlig sektor - Digitalseringsstrategi for offentlig sektor (2019-2025).
[218] Kommunal- og moderniseringsdepartementet, "Norge rykker opp på pallen i digitaliseringsmesterskap i EU" (2020), <https://www.regjeringen.no/no/aktuelt/norge-rykker-opp-pa-pallen-i-digitaliseringsmesterskap-i-eu/id2710512/> accesed 3 March 2021.
[219] Kommunal- og moderniseringsdepartementet, Nasjonal strategi for kunstig intelligens (2020).
[220] Per Helge Selgsten, "Ekspert om AI-diskriminering: Vi trenger et algoritmetilsyn" (2020) <https://www.digi.no/artikler/ekspert-om-ai-diskriminering-vi-trenger-et-algoritmetilsyn/500881> accessed 3 March 2021.

Norway has signed. Article 21 of the Convention requires the authorities to take measures to enable everyone to exercise their freedom of expression and information. Norway has also signed human rights conventions that emphasise the authorities' duty to facilitate access to information.[221]

The use of advanced technology has also raised questions about privacy rights. Disclosure of personal data between a number of public and private bodies also raises an issue about the relationship with the right to privacy and surveillance. The right to privacy follows from Article 8 of the European Convention on Human Rights (ECHR) and is central to the EU Privacy Directive (95/46 EC). In 1999, the ECHR was incorporated into Norwegian law through the Human Rights Act. The Convention is today part of Norwegian law. The Convention on Human Rights also takes precedence over other legislative acts, see Human Rights Act article 2.

Although not a member of the EU, Norway is part of the EEA. The EU Privacy Directive (95/46 EC) is therefore incorporated into the Norwegian legislation. These international directives and rules form the basis for Norway's privacy legislation.[222]

The issues with privacy rules raises questions related to the collection of data and whether the connection between Article 8 of the ECHR protection of respect for the right to private and family life etc. sets for private actions.[223]

The clear goal for the use of advanced digital technology in Norway is efficiency, availability and preparation of services, especially in the public sector. However, the use of advanced digital technology can lead to conflicts with human rights, such as rights against discrimination, freedom of expression and information, equality, the right to privacy and privacy rules.

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

2.1. National legislation

2.1.1. "Personopplysningsloven"

The primary national legislation aimed at protecting personal information is *personopplysningsloven,* hereafter referred to as the Personal Data Act (PDA). The law is an incorporation of GDPR, which was deemed EEA relevant in 2018, see further section 2.2.

---

[221] Bufdir, "Digitalisering en utfordring for eldres menneskerettigheter" (2021) <https://bufdir.no/uu/Nytt/Digitalisering_en_utfordring_for_eldres_menneskerettigheter/> accesed 3 March 2021.
[222] De forente nasjoner (FN-sambandet i Norge), Personvernerklæring (2018), <https://www.fn.no/om-oss/Personvernerklaering> accessed 3 March 2021.
[223] Norges forskningsråd. "Forskning om menneskerettigheter i Norge" (1999) <https://www.forskningsradet.no/siteassets/publikasjoner/1108644084179.pdf> accesed 3 March 2021.

The Personal Data Act does not contain an explicit definition of "personal information", as it refers to and applies the general definition found in GDPR Article 4(1). The GDPR defines "personal data" as "any information relating to an identified or identifiable natural person".

2.1.2. The Norwegian Constitution and Article 8 ECHR

The Norwegian Constitution includes provisions protecting privacy and human rights. First, paragraph 102 in the Norwegian Constitution reads "… Everyone has the right to respect for his private life, his home and his correspondence". The wording of "private life" illustrates that also personal information is protected.

Further, the Norwegian Constitution was revised in 2014 to strengthen the position of human rights, by assigning human rights provisions a constitutional rank. Hence, it now has a chapter (E) that contains provisions with wording similar to ECHR Articles. Therefore, case law from ECtHR is an important legal source when National Courts interpret paragraph 102 and further.

2.2. The implementation of GDPR and the EEA Agreement

The Agreement on the European Economic Area (EEA) gives EFTA-states access to the EU Member States internal market. The GDPR was deemed EEA relevant due to its primary goal: "to protect the privacy of natural persons and to remove the obstacles to flows of personal data within the EU, which still exist because of divergent legal approaches of the EU Member States".[224]

EEA relevant regulation "shall be made part of the internal legal order of the Contracting Parties(...)", see Article 7 (a) in the EEA Agreement. Due to the dualistic Norwegian legal system, an active implementation is required for international law to become Norwegian.[225] As the GDPR has now been incorporated into Norwegian national law, one must assume that privacy related matters will lead to the same result as in the EU, and elsewhere in the EEA. Furthermore, there exists several principles that ensure that Norwegian law does not contradict its external obligations.[226]

[224]European Free Trade Association, "The Incorporation of the GDPR into the EEA Agreement" (April 2018) <https://www.efta.int/EEA/news/Incorporation-GDPR-EEA-Agreement-508041> accessed 26 February 2021.
[225]Halvard Haukeland Fredriksen and Gjermund Mathisen, *EØS-rett* (3rd edition, 2018), p. 358.
[226] ibid, 49-55 and 387-390.

2.3. Additional conditions in the Personal Data Act

The PDA is compatible with GDPR because of its incorporation. Nevertheless, as the GDPR allows for exceptions, different approaches are to be expected in national legislation.

All types of personal data must be processed in accordance with GDPR Article 5. Similarly, special categories of personal data will warrant a stronger protection. What falls under special categories of personal data is specified in GDPR Article 9, such as "political opinions" and "genetic data". Any "processing" of this data is prohibited, see GDPR Article 9(1).

However, GDPR Article 9(2) allows deviation from prohibition. The exceptions are in broad terms based on "consent", where it is necessary and where the data already is published, see Article 9(2) (a)-(j). Specified measurements to protect special categories of personal data are therefore mostly found in the national legislation.

PDA Article 6 to 10 regulates special categories of data. All these Articles have the condition of necessity in common, which mirrors GDPR Article 9(2) (b), (c), (f), (g), (h) and (j). However, the PDA operates with additional conditions, such as "in special cases" in Article 7 and where it "clearly outweighs the disadvantages for the individual" in Article 9. Both Articles regulate processing of personal data where the purpose is vaguely defined, in comparison with other Articles, such as "to carry out labor law obligations or rights" in PDA Article 6.

The vague purpose for processing, whether there is consent or not, warrants the involvement of different organs, such as the Data Protection Authority, see PDA Act Article 7, and a Data Protection Officer or similar, see PDA Article 9 and 10. GDPR Article 9(g), which mirrors PDA Article 7, does not demand an organ.

General data such as national identity number and information regarding criminal convictions and offences benefits of stronger legal protection, in comparison to the GDPR. The heightened protection for national identity number comes in the form of additional conditions, such as "the objective need for secure identification" and "necessity to achieve such identification", see PDA Article 12. For information regarding criminal convictions and offenses, GDPR Article 9 2(a), (c)-(f) and PDA Article 6, 7 and 9 will apply. This is a significant difference from GDPR Article 10, where the regulation just assigns which organ is allowed to process the information.

2.4. Greater protection after implementing GDPR

Personal information was protected prior to the implementation of GDPR by the earlier version of The Personal Data Act (2004)[227]. The implementation of the GDPR led to changes that strengthened the protection of personal data.[228] One of these changes was an extended scope of the PDA. For instance, Article 4 states that the PDA concerns "every" treatment of personal data in relation to Norwegian citizens. This is independent of whether the processor is based in an EEA state, or whether the actual treatment finds place in an EEA state or not.

2.5. Protection regardless of GDPR

According to PDA Article 26, the Norwegian Data Protection Authority (DPA) can impose infringement fines on processors in accordance with the rules in GDPR Article 83. Such fines can be imposed when violating Article 10 and 24 in GDPR, relating to criminal convictions and offences. The fines must be paid within four weeks, see Article 27. The DPA may also determine a coercive fine that runs for each day until the order has been complied with.[229] Opposing corrections from the DPA can thus be a costly affair.

2.6. ECHR as an alternative external instrumental

ECHR focuses on the relationship between the state and the individual, while GDPR also focuses on the relationship between private companies and individuals. The difference in the field of application gives one a variety of legal grounds for their data privacy.

"[R]ight to respect for his private […] life" in ECHR Article 8(1) also includes the right to personal data.[230] Interference in this right is forbidden unless there is consent[231] or the interference is in harmony with ECHR Article 8(2).

ECHR Article 8(2) allows interference if it is "in accordance with law and is necessary in a democratic society", as well as if it is done for the sake of one of the interests listed in the Article. The condition on legality will concern the GDPR, PDA, and similar acts. An interpretation of "necessary" in GDPR and in the ECHR results in the need for an assessment of proportionality. When it comes to the legitimate aims, the GDPR operates with a bigger selection, see GDPR Article 9 as an example.

---

[227] Rune Opdahl, Pernille Gjerde Lia, "Norway - National GDPR Implementation Overview" (2020) <https://www.dataguidance.com/notes/norway-national-gdpr-implementation-overview> accessed 1 March 2021.
[228] Datatilsynet, "Hva er nytt med personvernforordningen?" (2019) <https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/hva-er-nytt/> accessed 27 February 2021.
[229] General Data Protection Regulation (EU) 2016/679 (GDPR) art. 29.
[230] *S. and Marper v. The United Kingdom* (App nos. 30562/04 and 30566/04) ECHR (4 December 2008) para 66-67.
[231] *Axel Springer AG v. Germany* (App no. 39954/08) ECHR (7 February 2012) para 83.

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. Self-regulation

"Self-regulation" of data protection is defined as voluntary standards, made by the industry for the industry. These standards might involve a certain practice of the law or alternative regulatory instruments.

3.1.2. Codes of conduct

Codes of conduct are a collection of guidelines that companies, either alone or by working with public authorities, develop and agree to follow.[232] The codes of conduct may provide guidelines for how the legislation is to be understood in the relevant industry, as well as additional moments that must be accounted for when processing personal data.

The codes may be further approved by the DPA in accordance with GDPR Article 40, but it is not necessary for the codes to be of binding nature. This is due to codes of conduct often being drafted as contracts. As of 15 February 2021, the DPA has not approved any codes of conduct, as of 15 February 2021.[233] Regardless, codes of conduct are in effect within several different industries, two of which are the accounting industry and health sector, the latter is treated in 3.2.1.

3.1.2.1. Guidelines for processing personal information in the accounting industry

The document "Guidelines for processing personal information in the accounting industry" (Veiledning for behandling av personopplysninger i regnskapsbransjen) is made by The Norwegian labour union for accountants *Accounting Norway* (Regnskap Norge), the Norwegian labour union for economists *Economic Union* (Økonomiforbundet), and the Norwegian labour union for public accountants *The Norwegian Institute of Public Accountants* (Revisorforeningen), and was released on 11 May 2020.[234] This specific document is not a contract and therefore not binding. However, *Accounting Norway* highlights that the guidelines are useful for establishing a code of conduct for the industry.[235] For instance, the document frequently uses the word "shall", see page 5, which again expresses that the guidelines carry some authoritative weight in the industry.

---

[232] Datatilsynet, Ordliste, "atferdsnorm" og "bransjenorsm" <https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/> accessed 1 March 2021.
[233] E-mail from linda.torperbystrom@datatilsynet.no to author (15 February 2021).
[234] Regnskap Norge, Økonomiforbundet og Revisorforeningen, Veiledning for behandling av personopplysninger i regnskapsbransjen (2020).
[235] Hans Eilefsen , 'Veiledning for behandling av personopplysninger i regnskapsbransjen' *Regnskap Norge*, 11 May 2020 <https://www.regnskapnorge.no/faget/artikler/bransjeaktuelt/veiledning-for-behandling-av-personopplysninger-i-regnskapsbransjen/> accessed 2 March 2021.

The guidelines include several points meant to strengthen data protection. For instance it recommends the existence of "an overview of all personal data that the accounting firm processes on behalf of the client".[236] This goes beyond what follows from GDPR Article 30. Furthermore the accounting firm is to assign a "privacy contact", regardless of whether this is imposed by GDPR Article 37 or not.[237]

3.2 Cooperation between the public and private sector

The Norwegian public sector is wide, as the state has more control and generally cooperates with private firms to a larger extent than other European countries. Furthermore, the state has set a goal regarding the digitization of the public sector.[238] The cooperation between the public and private sector in regards to data protection may therefore differ a lot in comparison to other countries.

3.2.1. Cooperation in the form of codes of conduct

The customary practice for information security and privacy in the health and care sector, also known as "The Norm", is a code of conduct valid from 5 February 2020.[239] It is produced by several public and private actors in the Norwegian health and care sector[240], which illustrates a form of cooperation. "The Norm" applies to everyone who's a contracting party[241], including private and public bodies.

An obligation to log any processing is found in the Patient Record Act Article 22 and the Personal Health Data Filing System Act Article 21. However, the Articles do not indicate what specifically needs to be logged. Meanwhile, "The Norm" regulates this in pages 33 to 34. 'The Norm' also operates with a set of minimum standards for information security.[242] Both the minimum standards for information security and the regulation on logging leads to less flexibility than what follows from the laws. For example GDPR Article 32 and the

---

[236] Regnskap Norge, Økonomiforbundet and Revisorforeningen, Veiledning for behandling av personopplysninger i regnskapsbransjen (2020), p. 5.
[237] ibid, 6-7.
[238] Kommunal- og moderniseringsdepartementet, "Digitalisering i offentlig sektor" *Regjeringen* (1 February 2021) <https://www.regjeringen.no/no/dokument/dep/kmd/andre-dokumenter/brev/utvalgte_brev/2021/digitalisering-i-offentlig-sektor/id2830849/> accessed 14 May 2021.
[239] Direktoratet for e-helse, Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (2020) (Normen v6.0) <https://ehelse.no/tema/personvern-og-informasjonssikkerhet/_/attachment/inline/2309b361-3146-4e11-ae35-1e20acff5567:085dc760fecbf9141ee59f446495c41b1a73346f/Normen%20versjon%206.0%20PDF.pdf> accessed 18 February 2021.
[240] Direktoratet for e-helse, "Om normen" (2021) <https://ehelse.no/normen/om-normen#Styringsgruppe> accessed 02 March 2021.
[241] Direktoratet for e-helse, Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (2020) (Normen v6.0) <https://ehelse.no/tema/personvern-og-informasjonssikkerhet/_/attachment/inline/2309b361-3146-4e11-ae35-1e20acff5567:085dc760fecbf9141ee59f446495c41b1a73346f/Normen%20versjon%206.0%20PDF.pdf> accessed 18 February 2021.
[242] ibid, 15-16.

Personal Health Data Filing System Act Article 21 both regulate information security ambiguously compared to "The Norm". This demonstrates how a more defined processing can result in stronger protection.

"The Norm" also regulates emergency routines in case of a lapse, with regards to a list of how different systems are prioritised.[243]

3.2.2. Data protection officers and the cooperation with DPA

The role of a data protection officer (DPO) is to "ensure that the organisation processes the personal data of its staff, customers, providers or any other individuals in compliance with the applicable data protection rules".[244] DPA recommends all private and public sectors to appoint a DPO, regardless of if they are obliged to or not.[245] Public authorities or bodies are required to appoint a DPO if they process personal information, see GDPR Article 37 (1)(a). Further, the private sector is required to appoint a DPO if "the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale", see. Article 37 (1)(b).

The DPA provides guidelines for which sectors need and should appoint a DPO. Additionally, they have curated a step-by-step guide which helps determine who needs to appoint a DPO.[246] Furthermore, the DPA provides information on which qualifications a DPO needs, and how their independence can be secured.

3.3. Data Protection Impact Assessment and DPA

The Data Protection Impact Assessment (DPIA) is an assessment meant to describe how personal data is treated and protected by the processor, see Article 35 GDPR. The function of DPIA is to control that the consequences of personal data treatment are both necessary and proportional compared to the intended goal. When carrying out a DPIA the controller shall, where designated, seek the advice of the DPO.

The establishment must conduct a DPIA when certain forms of processing are likely to result in a "high risk". Although the GDPR does not define "high risk", the DPA has

---

[243] ibid, 44-45.
[244] European Data Protection Supervisor, "Data Protection Officer (DPO)" <https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en > accessed 26 February 2021.
[245] Datatilsynet, "Hvem må ha personvernombud" (2019) <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvem-ma-ha-personvernombud/> accessed 23 February 2021.
[246] Datatilsynet, 'Har din virksomhet plikt til ombud' (2018), <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvem-ma-ha-personvernombud/trinn-for-trinn-veileder> accessed 26 February 2021.

interpreted "high" as "bigger than normal".[247] Article 35 further lists when such DPIA is required. Based on this, the DPA has given a non-exhaustive list of factors that should be considered.[248] For example, it states that a DPIA should determine whether personal data is processed without a legal basis, in an unfair manner, or without sufficient transparency.

If the processing of data is especially risky, Article 36 states that the controller shall consult the supervisory authority prior to processing. If failing to reduce the high risk, the processor is forced to seek advice and consult the supervisory authority. PDA Article 14 also authorises that further rules are created to demand certain types of processing of personal data to be approved by the DPA. Such measures have not yet been made in Norway.[249]

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

4.1 Definitions

Judicial review is defined as a procedure by which an organ, usually the court, can examine the actions of the legislative and executive branches of the government and determine whether such actions are in accordance with the laws of the State, primarily the Constitution.[250] In this text the expression will be used in a broader sense and, in addition to the Courts, include various public appeal bodies.

Data protection, in a legal context, is defined as laws and regulations that make it illegal to store or share certain information about people without their knowledge and permission.[251] A data subject is the individual to whom the stored information can be linked to.[252]

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

---

[247] Datatilsynet, "Når er det høy risiko? - Vurdering av personvernkonsekvenser (DPIA)" (2019) <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/> accessed 27 February 2021.

[248] Datatilsynet, "Risiko og risikovurdering - Vurdering av personvernkonsekvenser (DPIA)" (2019) <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/risikovurdering/> accessed 25 February 2021.

[249] Kommunal- og moderniseringsdepartement, "Ny personopplysningslov" (2019) <https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/ny-personopplysningslov/id2340094/> accessed 1 March 2021.

[250] Encyclopedia Britannica, "Judicial review" <https://www.britannica.com/topic/judicial-review> accessed 20 February 2021.

[251] Cambridge Dictionary, 'Data protection' <https://dictionary.cambridge.org/dictionary/english/data-protection> accessed 21 February 2021.

[252] Datatilsynet, "Regelverk og verktøy - ordliste" <https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/> accessed 01 March 2021.

In some cases, you may request that the processing of your personal data be restricted. This right is defined in the GDPR Article 18 as a right to "restriction", and means that your personal information may be stored, but your information cannot be used.

The right to restriction occurs when further conditions are met. Article 18(1)(a)-(d) sets up four alternative conditions, one of which must be met. This includes, among other things, cases where the accuracy of the personal data is "contested" by the data subject, see (a, and situations where the processing is "unlawful", see (b).

The exceptions to the right to restriction are regulated under GDPR Article 18(2). There are three exceptions, the most important one being that the personal data can be used with the data subject's "consent".

The right to object is defined in GDPR Article 21. An objection means that the controller no longer can use the personal information. Unless the information is processed for other purposes that the data subject cannot oppose, the information must also be deleted. The right to object, as with the right to restriction, is not absolute. There are three exceptions, all set out in Article 21(1).

4.3 Breaches – the process to notify the data subject

The duty to notify the data subject, in cases of data protection breaches, is regulated in GDPR Article 33-34. Article 34 regulates the situations in which the data subject must be notified. According to Article 33(1) , a breach which is likely to result in a "high risk" to the rights and freedoms of natural persons, shall be communicated to the data subject without undue delay. Whether or not a breach represents a "high risk" to the rights and freedoms of natural persons, must be determined on the basis of the specific circumstances of the case. Key factors are the severity of the breach, the kind of breach, and its impact.[253]

The key takeaway is that the data subject shall be notified if the breach represents a "high risk" to the rights and freedoms of the subject, see article 34(1). The exceptions to this are regulated in Article 34(3), of which one of three alternative conditions must be met.

Firstly, Article 34(3)(a) states that notification is not necessary 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. This provision refers to already established security measures, such as encryption.

Secondly, Article 34(3)(b) states that notification is not deemed necessary if the controller has taken "subsequent measures" so that the high risk to the rights and freedoms of the data subject is no longer likely to materialise. This provision refers to subsequent measures.

[253] Datatilsynet, "Når melde avvik?" (2018) <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/nar-skal-jeg-melde-avvik/> accessed 22 February 2021.

Thirdly, Article 34(3)(c) states that notification is not necessary if it would involve "disproportionate effort". It is thus a question subject to a proportionality assessment. Accordingly, a balance must be struck between the individual's interest in his personal data, and how costly a notification is for the individual company.

In addition to the exceptions in Article 34(3), Norway also has some special legislation. Pursuant to The Personal Data Act s. 16 para 4, information concerning national security, among other things, are also excluded from the starting point set out in Article 34(1).

4.4 What is the optimal balance for necessity and proportionality when it comes to not noticing the data subject?

The purpose behind the rules in GDPR Articles 33-34 is to protect the personal information of the affected person. For instance, the affected person, by being informed, can contribute to reducing the extent of damage. In addition, the rules are also important for internal learning in the company, to prevent similar incidents from happening again.

These considerations must govern the proportionality assessment. This means that the affected person's need for notification will depend on the type of deviation in question. A high degree of sensitivity, for instance, will indicate that the individual would want to be notified. In such a case, the interests in minimising notifications, e.g because of reasons of efficiency, must be significant.

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

5.1. Which bodies conduct such review?

In Norway, the review of cases concerning data protection breaches is conducted both by the courts and by independent bodies. The rules on supervision and appeal follow by chapter 6 in The Personal Data Act.[254]

The supervisory authority is the Data Protection Authority (DPA).[255] DPA is an independent administrative body and can therefore not be consulted in individual cases. Furthermore, the government and ministry are not able to reverse the DPA's decisions. As supervisory authority, the DPA is responsible for the control of compliance with privacy regulations.[256] This is done by processing complaints from individuals and performing independent supervision. Other tasks for the regulatory authority are provided for in GDPR Article 57. The DPA is also a member of the European Data Protection Board, which provides them with another perspective. As a part of this Board the Norwegian

[254] GDPR Chapter VI.
[255] The Personal Data Act section 20 and GDPR art. 51.
[256] Datatilsynet, "Datatilsynets oppgaver" <https://www.datatilsynet.no/om-datatilsynet/oppgaver/> accessed 23 February 2021.

DPA contributes to the GDPR being interpreted and applied equally in the European Economic Area (EEA).[257]

The appellate body is the Privacy Appeals Board (PAB).[258] Similar to DPA, PAB is an independent administrative body. As the name implies, PAB reviews appeals about DPA's administrative decisions. In this context, the appellate body may review all aspects of the case, including the judicial assessment. PAB is made up of seven members appointed for four years. In addition, the board consists of a secretariat which prepares the cases for the review.[259]

Finally, the courts also conduct reviews of cases of data protection breaches. Decisions from PAB can be appealed further to the courts, on grounds of validity. In these cases, the lawsuit is directed against the state by PAB. In cases concerning supervisory activities, DPA takes part on behalf of the government. [260].

On a lower level, many businesses are required to have a data protection officer (DPO).[261] This applies if the processing is carried out by a public authority or body, or if the core activities of the controller consist of large-scale processing operations, or processing of special categories of data. Nevertheless, all businesses are recommended to have a DPO, regardless of whether they are imposed or not.[262] The considerations behind this are the DPO's tasks: the DPO shall inform and give advice regarding the commitments the business has through the PDA, see GDPR Article 39.

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

If the data subject experiences something that can qualify as a violation of the privacy regulations, they can send a complaint to the DPA. Before consulting state organs for judicial review, the DPA recommends the subject to contact the data controller.[263] In this sense, "data controller" is understood as the companies, firms, institutions etc. that process our personal data.[264] By recommending this, the DPA intends to secure efficient case processing. Further, as mentioned above, a number of firms are also required to have a

---

[257] Datatilsynet, "Det europeiske Personvernrådet (EDPB)" (2020) <https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/personvernradet/?fbclid=IwAR36_oSWi8IF_UDihUacO1hJ9WIDgCx1NpybyM9Nw2yIqoBxUJ7bzIaZfiI> accessed 23 February 2021.
[258] PDA s. 22.
[259] Personvernnemda, "Klage/saksgang" <https://www.personvernnemnda.no/klage> accessed 23 February 2021.
[260] The Personal Data Act s. 25
[261] GDPR art. 37 and section 3.2.2
[262] Datatilsynet, "Hvem må ha personvernombud" (2019) <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvem-ma-ha-personvernombud/> accessed 23 February 2021.
[263] Datatilsynet, "Klage til datatilsynet" <https://www.datatilsynet.no/om-datatilsynet/kontakt-oss/hvordan-kan-jeg-klage-til-datatilsynet/> accessed 23 February 2021.
[264] ibid.

DPO. The proper authority's main function is to act as a contact person for questions and issues about the processing of personal data and other rights incorporated in the law.[265] In most cases, the process stops at this point.

When the parties disagree, the data subject can send a complaint to DPA. The PDA and Public Administration Act (PAA) constitute the rules of procedure. According to The Personal Data Act s. 20(3), DPA's powers follow from GDPR Article 58. Pursuant to Article 58 (1)-(3) the DPA, as a "supervisory authority", has three main powers. Most important for the judicial review, is the investigation powers that follow from Article 58(1). With that, the organ has the capacity of reviewing the ongoing case. For instance, it follows from Article 58(e) that the organ can "obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law". Consequently, the DPA has the power to examine the case.

If the data subject disagrees with the DPA's administrative decision, the subject has the right to complain.[266] The case will then be sent to the DPA for another review. If the DPA maintains their decision, the case will be sent to PAB.[267] Unless the DPA's decision is made in accordance with GDPR Article 56, or Chapter VII, the right to complain is maintained. The appeal process in PAB is the last level in the public administration, and the subject will at this point no longer hold the right to complain. If the subject disagrees with PAB's decision, the person can bring civil action against the opponent.

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

If PDA-regulations are violated, the DPA has several measures available. These rules are found in the PDA Chapter 7 and GDPR Chapter VIII.

According to GDPR Article 58(2), DPA can, among other things, give warnings, make reprimands, make orders and impose an administrative fine pursuant to Article 83. If the decision from DPA is not followed, they can give a coercive fine.[268]

Regarding administrative fines, Article 83(2) lists several factors to take into account when considering whether to impose an administrative fine and deciding on the amount. Depending on the case and the circumstances, DPA can give an administrative fine of up to € 20 000 000.[269] DPA is also given the authority to impose administrative fines to public authorities.[270] In all cases involving an administrative fine, the fine shall be effective, proportionate and dissuasive.[271]

[265] ibid.
[266] PAA s. 28(1).
[267] PDA s. 20(2).
[268] PDA s. 29.
[269] GDPR art. 8(5) and (6).
[270] PDA s. 26(2) and GDPR art. 83(7).
[271] GDPR art. 83(1).

In 2019, the DPA imposed only three administrative fines pursuant to GDPR.[272] In addition, the supervisory authority imposed seven administrative fines pursuant to the previous PDA.[273] The administrative fines imposed pursuant to GDPR all regarded breaches in personal data security, and none of these were appealed to the PAB.[274] This is a decrease in the number of sanctions imposed compared to previous years, which is notable as the number of cases registered that year were at a record high of 3,118 new cases.[275] The reason is likely related to the introduction of GDPR in the Norwegian legislation. On the other hand, the number of administrative decisions imposed by DPA has more than halved compared to 2017.[276]

The above mentioned numbers show that data privacy has received increased attention, likely due to the incorporation of GDPR. As a result of this incorporation the number of administrative decisions has decreased, while the number of registered cases has increased. Meanwhile, there are fewer sanctions imposed, and no complaints on these sanctions to PAB. This indicates that the decisions from DPA are effective. As the GDPR was first incorporated to Norwegian law in 2018, it is uncertain to conclude whether the remedies are effective. The short trend taken into account indicates that GDPR has made the review more effective.

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

In the last couple of years, the risks and possibilities of Artificial Intelligence (AI) have attracted profound attention in the media and in the academic sphere. New machine learning techniques pose new threats in terms of privacy breaches and discrimination. This creates an increased demand for regulatory guidelines and procedures, in order to secure an ethical implementation of AI. This segment discusses (1) AI implementation and discrimination risks, (2) Norwegian regulatory bodies conducting review on AI, and (3) potential impediments from effective protection against discrimination.

6.1. Artificial Intelligence – potential problems and discrimination risks

There are especially three problems that typically occur when using AI in decision making processes. First, supervised machine learning models might reproduce biased outcomes by learning from human practice.[277] Secondly, Advanced AI techniques are often based on unsupervised machine learning, which entails that the algorithm finds its own patterns and

[272] Datatilsynet. 'Kontroll og saksbehandling - årsmelding for 2019' <https://www.datatilsynet.no/om-datatilsynet/arsmeldinger/arsmelding-for-2019/kontroll-og-saksbehandling/> accessed 23 February 2021
[273] ibid.
[274] ibid.
[275] ibid.
[276] ibid.
[277] Teknologirådet. Rapport om kunstig intelligens – muligheter, utfordringer og en plan for Norge (2018), p. 9.

relations in a dataset. Since the computer cannot explain the causal mechanisms behind its conclusions, it is difficult to assess whether a decision based on the model will be discriminatory or unjust in some other way.[278] Third, machines do not act ethically without being programmed to do so. Contrary to humans, these machines need to be explicitly programmed to take ethical considerations into account.[279]

6.2 Where does the Norwegian government stand in relation to Artificial Intelligence today?

The Norwegian government has expressed clear plans to implement a digitalisation program especially directed at health, justice, consumer protection and bureaucratic institutions, in alignment with EU guidelines.[280] It is thus reasonable to believe that AI will be increasingly utilised in the Norwegian public sector throughout the following years.[281] According to the National Strategy for Artificial Intelligence, the government plans to use the ethical guidelines proposed by the EU High Level Expert Group on AI as a basis for the forthcoming development.[282] Additionally, Norwegian lawmakers and ombudsmen have to follow the GDPR provisions, see the PDA Article 1.

6.3. Reviewing AI: The Equality and Anti-Discrimination Ombud

The Equality and Anti-Discrimination Ombud is the main regulatory authority when it comes to anti-discrimination cases in Norway. According to The Anti-Discrimination Ombud Act (AOA) section 5, see section 1, the Ombud is to provide guidance to citizens regarding discrimination and ensure that public and private actors act according to the provisions in The Equality and Anti-discrimination Act (EADA) and corresponding special provisions.

The Ombud is in the early stages of assessing the effects of AI. Nevertheless, the Ombud has expressed concern regarding AI and the potential for discrimination.[283] For one, the Ombud has expressed concern regarding the proposal to further develop automated case procedures in the public administration, see NOU 2019: 5 ch. 18. Secondly, ombudsman Hanne Bjurstrøm has criticised the Norwegian government for not providing sufficient guidelines on how to thoroughly follow up on the issue of algorithmic bias.[284]

---

[278] Frederik Zuiderveen Borgesius, "Discrimination, artificial intelligence and algorithmic decision-making", Directorate General of Democracy, Council of Europe (2018), p. 10.

[279] Teknologirådet. Rapport om kunstig intelligens – muligheter, utfordringer og en plan for Norge (2018), p. 53-54; World Economic Forum 'The Global Risk Report' (2017), p. 49.

[280] Kommunal- og moderniseringsdepartementet, Nasjonal strategi for kunstig intelligens (2020).

[281] Ragna Aarli and Arne Krokan, "Den digitale dommer" (2020) Lov og rett, 59 (3), p. 155.

[282] Kommunal- og moderniseringsdepartementet. Nasjonal strategi for kunstig intelligens (2020), p. 58.

[283] Likestillings- og diskrimineringsombudet, "Kunstig Intelligens" (2021); Likestillings- og diskrimineringsombudet, "Årsrapport 2019", p. 35.

[284] Hanne Bjurstrøm, "Vesentlig for likestilling" *Dagbladet* (27 October 2020).

6.4. Reviewing AI: The Norwegian Data Protection Authority

The Norwegian Data Protection Authority (DPA) has the authority to conduct inspections and check whether companies have a legal basis for using AI, whether they have satisfactory self-monitoring procedures and whether they have implemented technical and organisational measures for risk-evaluation and data protection, see GDPR Article 51 and PDA Article 20. Companies have to be able to explain and demonstrate that they are using data in accordance with privacy policies, and the DPA has the authority to fine companies that do not.[285]

DPA conducts relatively few technical reviews of IT systems, mainly because GDPR emphasises responsibility and self-monitoring more than external review from authorities.[286] On the other hand, DPA has established a so-called "regulatory toolbox", which offers free guidance for selected AI developers, with the objective to help develop solutions and models that do not violate the existing personal data regulations. This project is supposed to gather rule makers and companies in a discussion about privacy considerations and other AI issues and contribute to the development of privacy friendly regulations and guidelines. [287]

6.5. Does the current Norwegian review constitute effective protection against discrimination?

There are two main bodies in Norway with authority to review AI developers when it comes to privacy and discrimination. DPA employs GDPR and corresponding PDA guidelines as its legal framework, while EADA mainly operates with the Equality and Anti-discrimination Act. It should be noted that these frameworks are not specifically designed to regulate AI-systems. It is therefore questionable whether they can, in a consistent and satisfying manner, provide the regulatory authorities with sufficient premise on how to review and control for discrimination risks.

6.5.1 The Personal Data Act and European guidelines

The GDPR data protection principles and the EU Expert Group's seven principles on AI provide DPA with guidelines on how Norwegian personal data should be handled in relation to AI. Nevertheless, these principles have been criticised for being quite limited and vague.

According to Dag Wiese Schartum, former leader of the Legal Informatics Center at the University of Oslo, the GDPR was mainly developed to regulate rule-based AI systems.[288]

---

[285] Datatilsynet, Kunstig intelligens og personvern (2018).
[286] ibid, p. 23.
[287] Datatilsynet, "Sandkasse for ansvarlig kunstig intelligens" (2021) <www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens> accessed 2 March 2021.
[288] Likestillings- og diskrimineringsombudet, "Årskonferansen 2020" <https://www.youtube.com/watch?v=GLrLpu_cTJM&ab_channel=likestillingsombud> accessed 28 January 2021.

Today, advanced AI techniques are often based on unsupervised or enhanced machine learning. Since new machine learning techniques poses new threats in terms of privacy breach and discrimination, it is questionable whether the regulatory points derived from the data protection principles are sufficiently protective of fundamental rights.

Schartum emphasizes that GDPR (and the corresponding PDA) lack regulation regarding documentation and discrimination-risk evaluation. Schartum acknowledges that some documentation guidance can be found in GDPR Article 13(2)(f) which states that the data subject shall be provided with "meaningful information about the logic involved". On the other hand, this provision does not encompass a requirement regarding the explanation of AI decisions and results.[289] This does not harmonise with the right to explanation, which is included in both EU and GDPR principles of transparency. In Norway, however, there have been several proposals to add documentation requirements regarding AI in the forthcoming PAA and Archives Act, see NOU 2019: 5 and NOU 2019: 9.

When it comes to discrimination-risk evaluation, Schartum mentions that the second part of Article 13(2)(f) "the significance and the envisaged consequences of such processing for the data subject" entails a connection to Article 35 which requires a Data Protection Impact Assessment (DPIA). Article 35(1) requires an "assessment of the impact" when the processing "is likely to result in a high risk to the rights and freedoms of natural persons". Since machine learning often constitutes such "high risks", this provision might be interpreted to include a protection against AI discrimination. However, this connection is not particularly visible, which intuitively calls for a legal clarification.[290]

According to Professors Kristine Bærøe and Torbjørn Gundersen, the Norwegian government should specify how lawmakers and enforcers ought to balance the principles presented by the EU Expert Group. Firstly, these principles are quite general, and should be specified to different sectors by examining their respective institutions, conditions and challenges. Secondly, since these principles are mainly ethical, they need to be continuously weighed and considered. Additionally, the professors call for more thorough risk evaluations and implementation plans regarding AI, in line with Bjurstroms critique, see section 6.3. [291]

6.5.2. The Equality and Anti-discrimination Act

Regulation provided by the EADA appears to face a similar problem. This can be illustrated by the prohibition of "indirect discrimination" in EADA Article 8. As shown, decisions made with the help of AI-systems can lead to indirect discrimination, see section 6.1. The prohibition in Article 8 is applicable when the discrimination is based on a specific

[289] ibid.
[290] ibid.
[291] Kristine Bærøe and Torbjørn Gundersen. "Regjeringens strategi for kunstig intelligens svikter på vesentlige punkter" *Aftenposten* (16 February 2020) <www.aftenposten.no/meninger/kronikk/i/pL5JpG/regeringens-strategi-for-kunstig-intelligens-svikter-paa-vesentilge-pu> accessed 22 February 2020.

set of characteristics that are protected in EADA Article 6(1), such as race or gender, see Human Rights Act Article 14. Because of the inherent obscurity of advanced AI systems, it is often difficult to locate the specific variables that determine the final computer decision. Since the system finds its own patterns in a large dataset, the data developer and reviewers cannot always know whether the computer has categorised based on characteristics protected in Article 6(1). Thus, discriminatory AI systems will not necessarily be regulated by non-discrimination prohibitions such as EEA Articles 8 and 6. As a result, the review of discriminatory AI systems can end up lacking a legal basis and thus be difficult to perform.

6.6. Conclusion

In conclusion, it is clear that Norway is experiencing an increased awareness of AI and its discriminatory implications. Even so, public review of complex AI-systems appears difficult to practice thoroughly because of the lack of a consistent and comprehensive legal framework. As a consequence, Norwegian regulatory authorities seem to be struggling with how to uphold their responsibility of securing an ethical implementation of AI.

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

7.1 Introduction

This segment will look at (1) whether Norway has specific regulations on Advanced Digital Technologies, (2) whether there exists initiatives for such regulations, and (3) how EU regulations influence Norwegian legislation on Advanced Digital Technologies. First, key terms will be defined.

Big data means sets that are so large and complex that they are difficult to handle with conventional tools.[292]

*Artificial Intelligenc*e (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. [293]

Internet of things (IoT) is the network of identifiable objects equipped with electronics, software, sensors, actuators and networks that make the objects able to connect with each other and to exchange data.[294]

[292] Det kongelige kommunal- og digitalisetingsdepartementet, Meld. St. 23 (2013–2014).

[293] Jake Frankfield, "Artificial Intelligence (AI)" (2021) <https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp> accessed 26 May 2021.

[294] Wikipedia, "Tingenes internett" (2020) <https://no.wikipedia.org/wiki/Tingenes_internett> accessed 27 May 2021.

Encryption is a process that encodes a message or file so that it only can be read by certain people.[295]

7.2 Does Norway have any legislation in place?

Norway does not have any existing legislation that explicitly regulates the technologies mentioned above. However, there exists legislation regarding technology in other areas which protects the population.

For example, the Personal Data Act Article 2 states that the Act and the Privacy Ordinance apply to fully or partially automated processing of personal data and to non-automated processing of personal data that is included in or is to be included in a register. This law contributes to the protection of privacy rights as it constitutes the most important privacy protection legislation.

Another example is the Intelligence Service Act. This Act shall contribute to secure Norway´s sovereignty, and it has several provisions about electric technology for intelligence purposes. This law contributes to the protection of the population by providing rules which shall contribute to testing Norway's sovereignty, territorial integrity, democratic governance and other national security interests, including preventing, detecting and counteracting foreign threats to Norway and Norwegian interests. It helps to test the trust and secure the basis for control of the Intelligence Service's activities, ensure that the Intelligence Service's activities are carried out in accordance with human rights, see Article 1 of the Intelligence Service Act.

7.3 Does Norway have any initiatives to regulations?

On the 14th of January 2020, the Norwegian government presented a national strategy for AI. It states that AI enables greater efficiency in, for example, case and customer processing. The government wants Norway to be at the front of the development and use of AI with respect to the rights and freedoms of the individual. [296]

The development and use of AI also presents challenges to human rights. However, it is of central importance for the government that the AI that is developed and used in Norway builds on ethical principles, and respect for human rights and democracy. For this purpose, the government is clear that supervisory authorities shall control that systems based on AI in its area of supervision operate within the principles for reliable and responsible use of AI.

Data is an important starting point for the development and use of AI. Today, large amounts of information are generated from a number of different sources. AI can use this to give us important insight.

---

[295] Cambridge Dictionary, "Encryption" <https://dictionary.cambridge.org/dictionary/english/encryption> accessed 21 February 2021.

[296] Kommunal- og moderniseringsdepartementet, Nasjonal strategi for kunstig intelligens (2020).

To exploit the potential that lies within AI, access to datasets of good quality is paramount. The government will facilitate sharing of data, both in the private and public sector, and between the sectors. The government will do so through education and by developing methods to share data in a practical way.

In January 2019, the Norwegian government launched a national strategy for digital security. On the basis of this strategy, the government developed a strategy for a new crypto policy in November 2019. The crypto policy has several purposes. It shall contribute to building a secure society by maintaining necessary national crypto competence, stimulate innovation and product development, stimulate the use of crypto technology and maintain Norway's position as crypto supplier to the North Atlantic Treaty Organisation (NATO).[297]

The strategy for a new crypto policy will nevertheless have consequences. Financial and administrative consequences of the policy will include expenditure related to the implementation in the administration and in the private sector. According to the government, however, the purposes of the crypto policy weighs heavier than the financial and administrative consequences.

7.4 Does the EU have any regulation on this, and to which extent does this influence the Norwegian legislation?

The EU commission has set up an expert group that has developed ethical guidelines for the reliable use of AI, based on international human rights.[298] The commission has adopted a number of legal acts that will strengthen the rights of consumers in the digital area, such as the proposal package "A New Deal for Consumers".[299] The Norwegian government has been following EUs work in terms of modernising the rights of consumers, and will continue to do so.

The EU has no regulations in connection with AI at the moment, but is expected to suggest a proposal to the regulation of AI in the first quarter 2021. Norway is, however, not part of the EU. EUs regulations will therefore not have a direct effect for Norwegian legislation, except if the regulation is relevant in connection with the EEA cooperation.

[297] Forsvarsdepartementet, Justis- og beredskapsdepartementet, Norsk kryptopolitikk (2019).
[298] European Commission, "A European approach to Artificial intelligence" <https://ec.europa.eu/digital-single-market/en/artificial-intelligence> accessed 08 January 2021.
[299] European Parliament, "Modernisation of EU consumer protection rules: A new deal for consumers" (2020).

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

8.1 Introduction

According to the Criminal Procedure Act Article 216 o, the prosecution can in some cases decrypt encrypted personal messages for criminal investigations. The question that arises is to what degree this provision provides the prosecution with this ability, and how this affects human rights.

A relatively new case in Norway where the prosecution gathered information from a digital platform, was the case against the wife of the former Minister of justice, Laila Bertehussen, at the end of 2020.[300] Laila Bertehussen was charged with violation of the Criminal Code Articles 115, 263, 225 and 190. The total penalty frame of the mentioned provisions was 16 years. The prosecution used evidence gathered from digital platforms. The case provoked reactions from the society when people became aware of how much information the prosecuting authorities were able to obtain from personal messages.

8.2 Scope

According to the Criminal Procedure Act Article 216 o, the court can decide that the police can "read non-publicly available information in a computer system (data reading)".

A natural linguistic understanding of the wording "non-publicly data reading" assumes personal digital messages. Furthermore, the preparatory work states that computers, tablets and smartphones are included.[301] In addition, it emerges from the preparatory work that the included means mentioned above, and therefore the Criminal Procedure Act Article 216 o, gives the police access to surveillance of the data system, and to gather information that is saved or generated in the system.[302] Subsequently, it follows that Article 216 o gives the police and prosecutors legal basis for decryption of encrypted personal messages.

8.3 Circumstances in which such decryption may be conducted

According to the Criminal Procedure Act Article 216 o, information can only be gathered when "someone with good reason is suspected of an action or attempted action that a) which by law may result in imprisonment for 10 years or more, or b) which is affected by the Penal Code", see articles *121, 123, 125, 126* …"".

The wording "which by law may result in imprisonment for 10 years or more" means that gathering evidence is legal if the accused person is accused of a violation that has a penal frame of 10 years or more.

[300] Oslo Tingrett, Staten versus Laila Anita Bertheussen, Saksnummer: 20-020518MED-OTIR/04.
[301] Prop. 68 L (2015-2016), p. 283.
[302] ibid .

Additionally, the interpretation conclusion that emerges from the wording is strengthened by the fact that the legislators deliberately chose to include two terms to be fulfilled in order to allow gathering of evidence from encrypted personal messages. Firstly, there must be a situation where data reading, including decryption will be of "significant importance in resolving the matter". Secondly, it must be a situation where resolving the matter without such access will "significantly complicate" the investigation. In view of the threshold that follows from the first paragraph of Article 216 o, the fulfilment of these two terms assumes a significantly high threshold for when the police can decrypt data in criminal investigations.

8.4 Does Article 216 o give the police too much power?

The next issue we will raise is whether Article 216 o gives the police too much power. To be able to answer this question, we first need to place the discussion in a context.

8.4.1 What does too much power mean?

There are several ways to look at whether Article 216 c provides the police with too much power. One viewpoint is a political one. However, this is a problematic approach, due to varying opinions in society. Another approach is a legal viewpoint. This viewpoint is, however, also challenging, due to the fact that the statutory provision is legal, since they have been able to add it to the penal code.

Our approach to the questions is therefore whether the statutory provision could be abused by the police and therefore undermine the human rights that they are bound to follow.

8.4.2 Does the police have too much power?

In the Penal code, it is only the most serious actions that have a penalty frame that could lead to more than 10 years in prison. These actions, and the actions that are specifically mentioned in The Criminal Procedure Article Article 216 letter b, are actions that are in the society's best interest to minimise as much as possible. When the police are allowed to decrypt data, in compliance with the terms of Article 216 o, it will decrease the number of these actions.

As mentioned earlier, Norway has human rights obligations. These obligations are included in the Constitution and the ECHR. Article 100 of the Constitution states that "there shall be freedom of expression". The same right follows from Article 10 of the ECHR. This is one of the most fundamental rights in the Norwegian society. When the police are allowed to decrypt all personal messages of an individual, this can lead to the individual being cautious when exercising his right to freedom of speech, because the police could possibly use the messages to justify decryption of the data. However, the situations in Article 216 o, where the police are allowed to decrypt data, is quite limited and aimed at serious situations. Therefore, a lot of expressions about these actions would presumably not be

protected by the right to freedom of speech according to the Constitution or the ECHR. This does mean that Article 216 o does not, at least not to a significant degree, undermine the right to free speech.

Norway also has an obligation to ensure and respect the right to privacy. This is not an absolute right, meaning the government could intervene if the following terms are fulfilled: the interference is "accordance with the law", it pursues a legitimate consideration and is "necessary in a democratic society".

The ability of the policy to decrypt data could be problematic in regards to the right to privacy. For example, a situation could arise where the penalty frame for the crime committed is over 10 years, but the police know that the crime in question will result in no more than, for example, 5 years. Regardless of this information, they are able to decrypt the person´s data. Subsequently, the police are allowed to intervene more in the person's private life than what the purpose of Article 216 o suggests. Therefore, Article 216 o opens for potential violation of the right to privacy according to the Constitution and ECHR Article 8.

In light of the above mentioned considerations, the question could arise as to whether Norway is moving in the direction of a surveillance state. Article 216 o sets relatively clear boundaries for when decryption is allowed in letter a and b. It does allow the police to obtain more data. One way to look at it is that the consequence of this increased digitalisation is that the inhabitants have begun to exchange information in new ways. In order for the police to be able to get the same amount of information, they must be able to decrypt data. However, due to the increased use of the Internet, information is easier accessible. As the police are able to access all the data within the framework of Article 216, they will have access to more information about the citizens than they did before. We have therefore arrived at the conclusion that Article 216 could lead Norway in the direction of a surveillance state.

8.5 Conclusion

The conclusion we have arrived at is that Article 216 o of the Criminal Procedure Act is not giving the police too much power. This is because it benefits society greatly that the police should be able to decrypt the data for criminal investigation purposes. As stated above, this may contribute to greater encroachment on some human rights, but as we see it, this is offset by society's benefit of Article 216 of the Criminal Procedure Act.

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

The balance between allowing digital advancements and protecting human rights is based on their interfusion. The further analysis will focus on proactive interactions between such values as democracy, human rights, innovation and digitalisation. Since the implementation

of GDPR by The Personal Data Act (2018), the government has been developing holistic ICT and AI strategies for a transparent, trustworthy, ethical and accessible digital public sector, nurtured by Norwegian excelling democracy, respect for rule of law and world-leading digital infrastructure institutions.[303]

9.1 Step one: National Cyber Security

The Norwegian Minister of Digitalisation was appointed in 2018, and in the following years the ministry has presented three key strategies for implementation of digital advancements to the public sector. Since the first National Cyber Security Strategy (2919) was presented as a work of cooperation between Norwegian ministries, data protection and data security were specifically pointed out as a joint responsibility deployed between ministries, local governments and other stakeholders involved in design, development and use of the digital government. The public authorities now have to obtain "in-house" digital competence for data protection, security prevention and damage control.[304]

The Cyber Security Strategy established a National Cybercrime Centre and Norwegian National Cyber Security Centre to prevent, detect and combat threats and crime in cyberspace. The National Security Authority (NSA) initiated an annual Comprehensive digital risk assessment (*En helhetlig digitalt risikobilde*). Its latest report for 2020 concluded with a need for further development of legal and regulatory framework for data centres regulation and improvement of the state dependence on international vendors, especially for cloud services.

The subject of advancing the capacity and security of Norwegian data centres was already introduced in a strategy for Norway as a data centre nation (2018), which put into perspective a Cloud computing strategy (2016). The strategy seemed to show little effect: according to the opinion of professionals at ICT Norway the capacity of the existing data centres is insufficient to cover the needs of the public sector, as well as the industry falling behind on its developmental potential.[305] This opinion resonates with the aforementioned 2020 assessment made by the NSA. However, a certain movement can be noticed: ICT Norway mentioned that it is awaiting a new data center strategy.[306]

The data centre and cloud technologies vendor and chain supply dependence weaken the level of cyber protection for sensitive and personal data of the residents, digital independence of the state, and integrity of the data which can be easier obtained for

[303] 'Freedom House: Freedom in the World 2021' Norway <https://freedomhouse.org/country/norway/freedom-world/2021> accessed 9 March 2021; World Intellectual Property Organization, 'Global Innovation Index 2020: Who Will Finance Innovation?', p. 302.
[304] Innst. 191 S (2020-2021), p. 27.
[305] ICT Norway is a trade organisation for the Norwegian ICT industry.
Øyvind Husby, 'Datasentre i Norge er svært viktig – det er fakta' *Dagsavisen* (27 November 2020); Fredrik Syversen, 'Digital suverenitet – ny virkelighet for Norge og Europa' *Dagens Perspektiv* (26 October 2020); Fredrik Syversen, 'Norge trenger datasentre og datasentre trenger Norge' *Stavanger Aftenblad* (19 September 2020).
[306] Fredrik Syversen, 'Strategien må ikke havne i en skuff' *Finansavisen* (15 September 2020).

influence and processing. The NSA has not indicated the problem as urgent. It is, however, the most serious shortcoming of the Norwegian online protection of human rights.

9.2 One digital public sector, powered by AI

As opposed to digital independence, Norway excelled with digitalisation of the public sector.[307] From a Norwegian perspective, a "seamless" digital public sector can contribute to a fair and more accessible distribution and implementation of rights and obligations, especially for the most disadvantaged members of society and people living in remote regions. The digital strategy for the public sector (2019-2025) prioritises, for example, digitalisation of public services provided to persons who «became parents», persons who have a seriously ill child, persons who have recently moved to Norway, services connected to inheritance questions, and services for voluntary organisations. [308]

The National Strategy for Artificial Intelligence (2020) complement and nuance the Digital public sector strategy focusing on explainability of AI processes and cautious testing of AI solutions. The AI research shall be based on "ethical principles and respect for human rights and democracy" while safeguarding "the integrity and the privacy of the individual".[309]

The strategy facilitates "faster and more coordinated" collaboration between stakeholders from business, technology, administrative and legal sectors through The Digitalisation Agency.[310] The National resource centre for data sharing (est. 2020) was a step further in the enhancement of AI research, as it promotes reuse of data. The focus area for AI research is eHealth, where AI tools can open for personalisation and, therefore, improvement of public health services.[311] The Norwegian Tax Authority is developing a synthetic, but representative set of personal data.[312]

The data sharing and machine learning initiatives will soon be followed by a Report to the Storting on data driven economy and innovation (April 2021).

9.3 Promotion of ICT and AI knowledge

Introduction of such comprehensive measures in line with the strategies was possible because of an already high level of electronic and digital maturity amongst Norwegian

---

[307] WIPO: GII 2020 [1], p. 302.
[308] Ministry of Local Government and Modernisation: 'One digital public sector — Digital strategy for the public sector' 2019–2025, p. 3, 19.
[309] Norwegian Ministry of Local Government and Modernisation, "National Strategy for Artificial Intelligence" (2020), p. 56.
[310] Digdir: About the Norwegian Digitalisation Agency. Quoting Nikolai Astrup, then Minister of Digitalisation. <https://www.digdir.no/om-oss/about-norwegian-digitalisation-agency/887>, accessed 9 March 2021.
[311] Trine Rogg Korsvik, Marie Hulthin and Anne Sæbø, "English summary: What do we know about artificial intelligence and gender equality? A review of Norwegian research", *Kilden genderresearch.no*, p. 4.
[312] DigDir: Skatteetaten: 'Nasjonal tilgang til syntetiske persondata for testformål' <https://www.digdir.no/digitalisering-og-samordning/skatteetaten-nasjonal-tilgang-til-syntetiske-persondata-testformal/994> accessed 9 March 2021.

residents. Nonetheless, the government recognises that further promotion of ICT and AI knowledge will benefit digitalisation goals, and therefore actively promotes free educational opportunities for its residents (e.g. an online course Elements of AI, podcasts Personvernpodden and Innopodden).[313] Some public and non-profit organisations offer their digital competence to small, medium-sized enterprises and startups through different platforms (e.g. Digital21, DigitalNorway, StartOff, Sandbox for Artificial Intelligence, FinTech Sandbox).
The industry professionals, business and non-profit organisations generally approve of and participate in the government-driven digital evolution.[314] The initiatives undertaken by the state seem to be an efficient, balanced and transparent response to the issues and needs posed by digitalisation of the public sector.

9.4 Has Norway reached an adequate balance?

The key values and principles of the Norwegian society, such as democracy, trust, transparency and equality represent a solid foundation for a successful implementation of advanced digital technologies while ensuring protection of basic human rights. The legal system, which is in itself mostly technologically neutral, provides much needed flexibility for technological development.

Norwegian authorities actively facilitate supervision of the undertaken measures and provide for an active political and legislative arena. Furthermore, they encourage residents of all age groups and backgrounds, professionals, trade and non-profit organisations to participate in the public debate around the creation of one digital public centre.[315]
The measures undertaken by Norwegian authorities to reach an adequate balance between allowing digital advancements whilst ensuring the protection of human rights online can therefore be described as satisfactory, from both the national and international perspective.

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?

Based on the previous analysis, the question arises as to which line the Norwegian legislation follows; strict or liberal. Where will we be in five years, and can we keep up with technological developments in the future? To answer these questions, we must look to the trend in legislation and in the political and judicial authorities.

---

[313] Kommunal- og moderniseringsdepartementet, 'Gratis kurs i kunstig intelligens – mange skal kunne litt!' (2020) <https://www.regjeringen.no/no/aktuelt/gratis-kurs-i-kunstig-intelligens--mange-skal-kunne-litt/id2700313/>, accessed 9 March 2021.
[314] Øyvind Husby, 'IKT-bransjen leverte som best, når den trengtes som mest' *INSIDEtelecom* (18. des. 2020); Anam Javid Norwegian Artificial Intelligence Research Consortium. 'Norway's first National Strategy for Artificial Intelligence launched' <https://www.nora.ai/news-and-events/news/norway's-first-national-strategy-for-artificial-in.html>, accessed 9 March 2021; Syversen. Finansavisen, 15 September 2020 [93].
[315] Innst. 191 S (2020—2021) p. 27; Meld. St. 30 (2019—2020) p. 67-71.

As noted, there is no doubt that the pace of technological development is increasing. The Norwegian authorities stated already in 2014 that this development is in many areas faster than they are able to implement preventive measures for vulnerabilities.[316] This is particularly visible when it comes to the lack of legislation for securing an ethical implementation of AI, and might make the authorities struggle to keep up with technological developments in the future as well. In their national strategy for digital security from 2019, the authorities nevertheless emphasised that private individuals should be able to trust the individual's welfare and that their democratic values are safeguarded in the digital society.[317] This corresponds with the revision of the constitution in 2014, where Norway gave a clear expression that human rights should be in focus with Article 102. In this way, the Norwegian authorities have for a long time shown that there is a political goodwill to promote technology in accordance with human rights. This is important as the Norwegian society is one of the most digitised in the world.

Nevertheless, the adoption of the first infection control app (Smittestopp) in regards to the COVID-19 pandemic, shows that the authorities did not maintain an equally clear position on human rights under pressure. They were unable to keep up with the rapid technological development that has taken place at this time. Politicians emphasised efficiency over privacy. The Norwegian Minister of Health, Bent Høie, commented in this regard, that the function of the app was proportionate due to the COVID-19 situation, and that it was, after all, voluntary to download.[318] The application was downloaded more than 1.5 million times, which can illustrate that the Norwegian society has a great deal of confidence in the authorities.[319]

However, the authorities had to succumb to massive criticism, both from home and abroad.[320] Finally, the DPA put its foot down, and demanded a temporary ban on the processing of personal data through the app. The decision was based on the fact that the monitoring of the population was not a proportionate interference with the freedom of

[316] Utenriksdepartementet, 'Melding til Stortinget, Muligheter for alle – menneskerettighetene som mål og middel i utenriks- og utviklingspolitikken' (2014–2015), p. 43 <https://www.regjeringen.no/no/dokumenter/Meld-St-10-20142015/id2345623/> accessed 1 June 2021.
[317] Justis- og beredskapsdepartementet og Forsvarsdepartementet, 'Nasjonal strategi for digital sikkerhet', 2019, p. 7 <https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/> accessed 1 June 2021.
[318] Iselin Elise Fjeld, 'Amnesty: Norges Smittestopp-app blant de verste i verden på personvern', *NRK* (16 June 2020) <www.nrk.no/norge/norges-smittestopp-app-blant-de-verste-i-verden-pa-personvern-1.15054311> accessed 5 March 2021.
[319] Martin S. Folkvord, Oline Birgitte Nave, Martha C. S. Holmes, 'Smitteapp mangler over 1,3 millioner brukere for å nå FHIs mål', *VG* (7 May 2021) <www.vg.no/nyheter/innenriks/i/1nJM1M/smitteapp-mangler-over-13-millioner-brukere-for-aa-naa-fhis-maal> accessed 24 February 2021.
[320] See e.g. 'Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy', *Amnesty International* (16 June 2020), <www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/> accessed 24 February 2021.

persons, and thus not compliant with the PDA.[321] In other words, the stressful COVID-19 situation was not enough to justify such a serious intervention. Following this criticism, political and legislative authorities had to adjust to demands for better legal certainty. A new application that sought to do this, as well as the development being openly available, was therefore developed to replace the old one. The authorities show in this way that they are bound by democratic values. Specifically, it points to a development where the authorities will continue to have a liberal policy in order to maintain trust from the people. This also actively demonstrates a trend that state and private authorities cannot freely dispose of information.

Within this liberal policy, in a landscape that contains several general guidelines, there is also a kind of vacuum when it comes to legislation for advanced technology. As mentioned above, the Norwegian authorities agree that the technology is moving at a rapid pace. This may justify the fact that the authorities are increasingly using strategies and codes of conduct, instead of specific legislation in the area. This tactic seems to be the focus going forward as well.

The authorities demonstrate this by pointing out that they are not equipped to tackle the digital challenges alone going forward. Thus, they will focus on increased cooperation between state and private actors.[322] At the same time, the authorities point out that large parts of the country's critical digital infrastructures are owned and operated by private companies. Therefore they will focus largely on good cooperation, to prevent the field from being managed by private companies alone.[323] The previously mentioned "The Norm", is a good example of this strategy. This indicates that Norwegian legislation and regulations will be on a liberal line in the years ahead.

Nevertheless, as previously discussed, the Criminal Procedure Act Article 216 will raise challenges regarding the monitoring of the individual citizen. It could be a challenge for the authorities in the coming years to find a way to process information, without abusing their power. In other words, how to use their authority without compromising the individual's right to privacy. Finding a balance between this will be important in order to maintain the people's trust and the country's fundamental democratic values.

Conclusion

The use of technology in today's society brings with it several benefits and advantages, but today's society must be aware of the challenges associated with increasing use of technology. The use of advanced digital technology is a complicated topic, which in

[321] Datatilsynet, "Vedtak om midlertidig forbud mot å behandle personopplysninger – appen Smittestopp" (6 July 2020), p. 2.
[322] Justis- og beredskapsdepartementet og Forsvarsdepartementet, 'Nasjonal strategi for digital sikkerhet', (2019), p. 6 <https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/> accessed 1 June 2021.
[323] ibid, p. 9.

Norway can raise several legal issues such as discrimination and algoritms, right to privacy and information. This causes a need for greater legal regulation.

Table of legislation

Provision in Norwegian	Corresponding translation in English
Grunnloven (1814)	The Norwegian Constitution
Den europeiske menneskerettskonvensjonen (EMK)	The European Convention on Human Rights Act (ECHR)
FN-konvensjon om rettigheter for mennesker med nedsatt funksjonsevne	The Rights of Persons with Disabilities (CRPD)
EUs Personverndirektiv	The EU Privacy Directive (95/46 EC)
Pasientjournalloven (2014)	Patient Record Act
Lov **o**m styrking av menneskerettighetenes stilling i norsk rett (mrl.) (1999)	Act relating to the strengthening of the status of human rights in Norwegian law
Helseregisterloven (2014)	The Personal Health Filing Data Act
Personopplysningsloven (2018)	The Personal Data Act (PDA)
Personopplysningsloven (2000)	The Previous Personal Data Act
Likestillings- og diskrimineringsloven (2017)	The Equality and Anti-Discrimination Act
Personvernforordningen	The General Data Protection Regulation (GDPR)
Lov om likestillings- og diskrimineringsombudet og Diskrimineringsnemnda (2018)	The Anti-Discrimination Ombud Act
Straffeprosessloven (1981)	The Criminal Procedure Act
Straffeloven (2005)	The Penal Code
Forvaltningsloven (1967)	The Public Administration Act (PAA)

Bibliography

English titles

Legislation

Agreement on the European Economic Area (EEA Agreement)

Act relating to the strengthening of the status of human rights in Norwegian law (The Human Rights Act) (1999)

EU Privacy Directive

European Convention on Human Rights (ECHR)

General Data Protection Regulation (EU) 2016/679 (GDPR)

Rights of Persons with Disabilities (CRPD)

Reports

Borgesius, F. Z. "Discrimination, artificial intelligence and algorithmic decision-making", Directorate General of Democracy, Council of Europe (2018) <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> accessed 1 June 2021

Center for AI and Digital Policy, 'Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020' (AISCI-2020) <https://caidp.dukakis.org/aisci-2020/> accessed 9 March 2021

Norwegian Ministeries. 'National Cyber Security Strategy for Norway' (January 2019) <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf> accessed 9 March 2021

Norwegian Ministry of Local Government and Modernisation. 'Cloud Computing Strategy for Norway' (June 2016) <https://www.regjeringen.no/en/dokumenter/cloud-computing-strategy-for-norway/id2484403/> accessed 9 March 2021

Norwegian Ministry of Local Government and Modernisation. 'One digital public sector: Digital strategy for the public sector 2019–2025' (October 2019) <https://www.regjeringen.no/contentassets/db9bf2bf10594ab88a470db40da0d10f/en-gb/pdfs/digital_strategy.pdf> accessed 9 March 2021

Norwegian Ministry of Local Government and Modernisation. 'National Strategy for Artificial Intelligence' (January 2020) <https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi_en.pdf> accessed 9 March 2021

Norwegian Ministry of Trade, Industry and Fisheries. 'Powered by Nature: Norway as a data centre nation' (February 2018) <https://www.regjeringen.no/globalassets/departementene/nfd/dokumenter/strategier/strategi-nfd-eng-nett-uu.pdf> accessed 9 March 2021

OECD Public Governance Policy Papers 'Digital Government Index No. 03.' (2020) <https://www.oecd-ilibrary.org/governance/digital-government-index_4de9f5bb-en> accessed 9 March 2021

World Economic Forum, The Global Risk Report (2017) <http://www3.weforum.org/docs/GRR17_Report_web.pdf> accessed 1 June 2021

World Justice Project, 'Rule of Law Index 2019' <https://worldjusticeproject.org/sites/default/files/documents/ROLI-2019-Reduced.pdf> accessed 9 March 2021

World Intellectual Property Organization, 'Global Innovation Index 2020: Who Will Finance Innovation?' <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020.pdf> accessed 9 March 2021

Periodicals

Robinson, S.R. "Trust, transparency and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI)" (2020) *Technology in Society* 63 101421 <https://doi.org./10.1016/j.techsoc.2020.101421> accessed 9 March 2021

Digital resources

Amnesty International, "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy" (16 June 2020) <www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/> accessed 24 February 2021

Cambridge Dictionary, "Encryption" <https://dictionary.cambridge.org/dictionary/english/encryption> accessed 21 February 2021

Cambridge Dictionary, "Data protection" <https://dictionary.cambridge.org/dictionary/english/data-protection> accessed 21 February 2021

Data Protection Authority, "Sandbox for artificial intelligence" <https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/> accessed 9 March 2021

Datatilsynet "About Us" (2021) <www.datatilsynet.no/en/about-us/> accessed 2 March 2021

DigDir, "About the Norwegian Digitalisation Agency" <https://www.digdir.no/om-oss/about-norwegian-digitalisation-agency/887> accessed 9 March 2021

"Elements of AI" <https://course.elementsofai.com/no/> accessed 9 March 2021

Email from linda.torperbystrom@datatilsynet.no to author (15 February 2021)

Encyclopedia Britannica, "Judicial review" <https://www.britannica.com/topic/judicial-review> accessed 20 February 2021

European Commission, "A European approach to Artificial intelligence" <https://ec.europa.eu/digital-single-market/en/artificial-intelligence> accessed 08 January 2021

European Data Protection Supervisor, "Data Protection Officer (DPO)"<https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en> accessed 26 February 2021

European Free Trade Association, "The Incorporation of the GDPR into the EEA Agreement" (April 2018) <https://www.efta.int/EEA/news/Incorporation-GDPR-EEA-Agreement-508041> accessed 26 February 2021

European Parliament, "Modernisation of EU consumer protection rules: A new deal for consumers" (2020) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/623547/EPRS_BRI(2018)623547_EN.pdf> accessed 2 June 2021

Freedom House, 'Freedom in the World. Norway' (2021) <https://freedomhouse.org/country/norway/freedom-world/2021> accessed 9 March 2021

Javaid, A. 'Norway's first National Strategy for Artificial Intelligence launched' (2020) Norwegian Artificial Intelligence Research Consortium <https://www.nora.ai/news-and-events/news/norway's-first-national-strategy-for-artificial-in.html> accessed 9 March 2021

Korsvik, T. R., Hulthin M and Sæbø A, 'English summary: What do we know about artificial intelligence and gender equality? A review of Norwegian research' (2020) Kilden genderresearch.no <https://kjonnsforskning.no/en/what-do-we-know-about-artificial-intelligence-and-gender-equality-review-norwegian-research> accessed 9 March 2021

Norwegian Artificial Intelligence Research Consortium, <https://www.nora.ai> accessed 9 March 2021

Norwegian National Security Authority, <https://nsm.no/home/> accessed 09 March 2021

Norwegian National Security Authority, 'National Cyber Security Centre' <https://nsm.no/areas-of-expertise/cyber-security/norwegian-national-cyber-security-centre-ncsc/> accessed 9 March 2021

Politiet, 'National Cybercrime Sentre (NC3)' <https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/national-cybercrime-centre/> accessed 9 March 2021

Case-law

Axel Springer AG v. Germany (App no. 39954/08) (ECHR, 7 February 2012)

S. and Marper v. The United Kingdom (App nos. 30562/04 and 30566/04) (ECHR, 4 December 2008)

Norwegian titles

Legislation

Den europeiske menneskerettskonvensjon

EUs Personverndirektivet

FN-konvensjon om rettigheter for mennesker med nedsatt funksjonsevne

Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) (1999)

Helseregisterloven (2014)

Pasientjournalloven (2014)

Personopplysningsloven (2018)

Lov om forsøk i offentlig forvaltning (1992)

NOU 2019: 5 Ny forvaltningslov

NOU 2019: 9 Ny lov om samfunnsdokumentasjon og arkiver

Innst. 191 S (2020—2021)

Reports

Det kongelige kommunal- og digitalisetingsdepartementet, Meld. St. 23 (2013–2014)

Det kongelige kommunal- og digitalisetingsdepartementet, Meld. St. 30 (2019—2020) <https://www.regjeringen.no/no/dokumenter/meld.-st.-30-20192020/id2715113/> accessed 9 March 2021

Det kongelige utenriksdepartementet, Meld. St. 10 (2014–2015) <https://www.regjeringen.no/contentassets/261f255d028b42cab91ad099ee3f99fc/no/pdfs/stm201420150010000dddpdfs.pdf> accessed 1 June 2021

Datatilsynet, 'Rapport om kunstig intelligens og personvern' (2018) <www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/rapport-om-ki-og-personvern.pdf> accessed 27 January 2021

Forsvarsdepartementet og Justis- og beredskapsdepartementet, Norsk kryptopolitikk (2019) <https://www.regjeringen.no/contentassets/b10fc813bf6e4746aca8a7011f9eafae/strategi-for-ny-kryptopolitikk.pdf> accessed 28 May 2021

Justis- og beredskapsdepartementet og Forsvarsdepartementet, Nasjonal strategi for digital sikkerhet (2019) <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf> accessed 1 June 2021

Kommunal- og moderniseringsdepartementet. 'En digital offentlig sektor - Digitaliseringsstrategi for offentlig sektor (2019-2025)' (2019), <https://www.regjeringen.no/no/dokumenter/en-digital-offentlig-sektor/id2653874/?ch=1> accessed 2 March 2021

Kommunal- og moderniseringsdepartementet, 'Nasjonal strategi for kunstig intelligens' (2020) <https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-kunstig-intelligens/id2685594/?ch=1> accessed 1 February 2021

Likestillings- og diskrimineringsombudet, "Årsrapport 2019" <www.regjeringen.no/contentassets/7810678ef3fe48d2927637a83abcd90f/ldo-arsrapport-2019-med-riksrevberetning.pdf> accessed 12 February 2021

Nasjonalt Cybersikkerhetssenter. Helhetlig digitalt risikobilde. September 2020 <https://nsm.no/getfile.php/134267-1601027852/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2020_1609_LR.pdf> accessed 9 March 2021

Norges forskningsråd. 'Forskning om menneskerettigheter i Norge' (1999) <https://www.forskningsradet.no/siteassets/publikasjoner/1108644084179.pdf> accesed 3 March 2021

Teknologirådet. Rapport om kunstig intelligens – muligheter, utfordringer og en plan for Norge (2018) <https://teknologiradet.no/wp-content/uploads/sites/105/2018/09/Rapport-Kunstig-intelligens-og-maskinlaering-til-nett.pdf> accessed 1 June 2021

Books

Fredriksen, H. H. og Gjermund Mathisen, *EØS-rett* (3. urgave, Fagbokforlaget 2018)

Periodicals

Aarli, R. and Arne Krokan (2020) 'Den digitale dommer – Om endring av ardeidsprosesser i domstolene' *Lov og rett*, vol. 59, 3, 2020, s. 149–166 <https://www.regjeringen.no/contentassets/367acaf16a2941bfaf5e3b1ae7bfe95f/no/sved/07.pdf> accessed 1 June 2021

Husby Ø, 'Datasentre i Norge er svært viktig – det er fakta' *Dagsavisen* (27 November 2020) <https://www.ikt-norge.no/kommentar/datasentre-i-norge-er-svaert-viktig-det-er-fakta/> accessed 9 March 2021

Husby Ø, 'IKT-bransjen leverte som best, når den trengtes som mest' *INSIDEtelecom* (18. des. 2020) <https://www.insidetelecom.no/artikler/debatt-ikt-bransjen-leverte-som-best-nar-den-trengtes-som-mest/504515>, accessed 9 March 2020

Syversen, F. 'Digital suverenitet – ny virkelighet for Norge og Europa' *Dagens Perspektiv* (26 October 2020) <https://www.dagensperspektiv.no/2020/digital-suverenitet-ny-virkelighet-for-norge-og-europa> accessed 9 March 2021

Syversen, F. "Norge trenger datasentre og datasentre trenger Norge" *Stavanger Aftenblad* (19 September 2020) <https://www.aftenbladet.no/meninger/debatt/i/9Om8vW/norge-trenger-datasentre-og-datasentre-trenger-norge>, accessed 9 March 2021

Syversen, F. 'Strategien må ikke havne i en skuff' *Finansavisen* (15 September 2020) <https://www.ikt-norge.no/kommentar/26884/>, accessed 9 March 2021

Digital resources

Bjurstrøm H, ´Vesentlig for likestilling` (2020) <www.dagbladet.no/meninger/vesentlig-for-likestilling/7299239> accessed 13 February 2021

Bufdir, "Digitalisering en utfordring for eldres menneskerettigheter" <https://bufdir.no/uu/Nytt/Digitalisering_en_utfordring_for_eldres_menneskerettigheter/> accessed 3 March 2021

Bærøe K and Torbjørn Gundersen. "Regjeringens strategi for kunstig intelligens svikter på vesentlige punkter" *Aftenposten* (16 February 2020) <www.aftenposten.no/meninger/kronikk/i/pL5JpG/regeringens-strategi-for-kunstig-intelligens-svikter-paa-vesentilge-pu> accessed 22 February 2020

Datatilsynet, "Datatilsynets oppgaver" <https://www.datatilsynet.no/om-datatilsynet/oppgaver/> - accessed 23 February 2021

Datatilsynet, "Det europeiske Personvernrådet (EDPB)" <https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/personvernradet/?fbclid=IwAR36_oSWi8IF_UDihUacO1hJ9WIDgCx1NpybyM9Nw2yIqoBxUJ7bzIaZfiI> accessed 23 February 2021

Datatilsynet, "Har din virksomhet plikt til å ha ombud?" (2018) <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvem-ma-ha-personvernombud/trinn-for-trinn-veileder> accessed 26 February 2021

Datatilsynet, "Hva er nytt med personvernforordningen?" (2019) <https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/hva-er-nytt/> accessed 27 February 2021

Datatilsynet, "Hvem må ha personvernombud" (2019) <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvem-ma-ha-personvernombud/> accessed 26 February 2021

Datatilsynet, "Hvordan klage til datatilsynet?" <https://www.datatilsynet.no/om-datatilsynet/kontakt-oss/hvordan-kan-jeg-klage-til-datatilsynet/> accessed 23 February 2021

Datatilsynet, "Når og hvordan skal jeg melde avvik?" <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/nar-skal-jeg-melde-avvik/> accessed 21 February 2021

Datatilsynet, "Personvernpodden" <https://www.datatilsynet.no/regelverk-og-verktoy/personvernpodden/> accessed 9 March 2021

Datatilsynet, "Regelverk og verktøy - ordliste" <https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/> accessed 01 March 2021

Datatilsynet, "Sandkasse for ansvarlig kunstig intelligens" (2021) <www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens> accessed 2 March 2021

Datatilsynet, "Vedtak om midlertidig forbud mot å behandle personopplysninger – appen Smittestopp" (6 July 2020) <www.datatilsynet.no/contentassets/ae1905a8b88d4d869f1e059b60be35fd/Vedtak-om-midlertidig-forbud-mot-a-behandle-personopplysninger.pdf> accessed 19 May 2021

Datatilsynet, "Årsmelding for 2019 – Kontroll og saksbehandling" <https://www.datatilsynet.no/om-datatilsynet/arsmeldinger/arsmelding-for-2019/kontroll-og-saksbehandling/> accessed 23 February 2021

De forente nasjoner (FN-sambandet i Norge), Personvernerklæring (2018), <https://www.fn.no/om-oss/Personvernerklaering> accessed 3 March 2021

DigDir, "Nasjonalt ressurssenter for deling av data" <https://www.digdir.no/digitalisering-og-samordning/nasjonalt-ressurssenter-deling-av-data/1914> accessed 9 March 2021

DigDir: "Skatteetaten: Nasjonal tilgang til syntetiske persondata for testformål" <https://www.digdir.no/digitalisering-og-samordning/skatteetaten-nasjonal-tilgang-til-syntetiske-persondata-testformal/994> accessed 9 March 2021

Digi, "Ekspert om AI-diskriminering: Vi trenger et algoritmetilsyn" <https://www.digi.no/artikler/ekspert-om-ai-diskriminering-vi-trenger-et-algoritmetilsyn/500881> accesed 3 March 2021

Direktoratet for e-helse, Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (2020) (Normen v6.0) <https://ehelse.no/tema/personvern-og-informasjonssikkerhet/_/attachment/inline/230

9b361-3146-4e11-ae35-1e20acff5567:085dc760fecbf9141ee59f446495c41b1a73346f/Normen%20versjon%206.0%20PDF.pdf> accessed 18 February 2021

Direktoratet for e-helse, "Om normen" (2021) <https://ehelse.no/normen/om-normen#Styringsgruppe> accessed 02 March 2021

Ellefsen, Hans, "Veiledning for behandling av personopplysninger i regnskapsbransjen", *Regnskap Norge* (11 may 2020) <https://www.regnskapnorge.no/contentassets/d1e263a4d94542668b2ad099a3c2fc52/veiledning-for-behandling-av-personopplysninger-i-regnskapsbransjen-v1_1.pdf> accessed 18 February 2021

Equality and Anti-Discrimination Ombud, The: Our Work <www.ldo.no/en/ldo-english-page> accessed 2 March 2021

Fjeld, I. E. 'Amnesty: Norges Smittestopp-app blant de verste i verden på personvern', *NRK* (16 June 2020) <www.nrk.no/norge/norges-smittestopp-app-blant-de-verste-i-verden-pa-personvern-1.15054311> accessed 5 March 2021

Finanstilsynet (Independent government agency for supervision of the financial sector), 'Fintech and regulation sandbox' <https://www.finanstilsynet.no/tema/fintech/> accessed 9 March 2021

Folkvord, M. S., Oline Birgitte Nave og Martha C. S. Holmes, 'Smitteapp mangler over 1,3 millioner brukere for å nå FHIs mål', *VG* (7 May 2021) <www.vg.no/nyheter/innenriks/i/1nJM1M/smitteapp-mangler-over-13-millioner-brukere-for-aa-naa-fhis-maal> accessed 24 February 2021

Forsvarsdepartementet og Justis- og beredskapsdepartementet, 'Ny strategi for kryptopolitikk' (2019)

https://www.regjeringen.no/contentassets/b10fc813bf6e4746aca8a7011f9eafae/strategi-for-ny-kryptopolitikk.pdf, accessed 1 November 2019

Frankfield J, 'Artificial Inteligence (AI)' (2021), Investopedia,

<https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp> accessed 6 January 2021

Innovasjon Norge, 'Innopodden' <https://www.innovasjonnorge.no/no/om/podcast/> accessed 9 March 2021

Kommunal- og moderniseringsdepartementet, 'Norge rykker opp på pallen i digitaliseringsmesterskap i EU' (16 June 2020) <https://www.regjeringen.no/no/aktuelt/norge-rykker-opp-pa-pallen-i-digitaliseringsmesterskap-i-eu/id2710512/> accesed 3 March 2021

Kommunal- og moderniseringsdepartementet, "Digitalisering i offentlig sektor" *Regjeringen* (1 February 2021) <https://www.regjeringen.no/no/dokument/dep/kmd/andre-dokumenter/brev/utvalgte_brev/2021/digitalisering-i-offentlig-sektor/id2830849/> accessed 2 June 2021

Kommunal- og moderniseringsdepartementet, Pressemelding 29. april 2020. 'Gratis kurs i kunstig intelligens – mange skal kunne litt!' <https://www.regjeringen.no/no/aktuelt/gratis-kurs-i-kunstig-intelligens--mange-skal-kunne-litt/id2700313/> accessed 9 March 2021

´Kunstig Intelligens' <www.ldo.no/en/ombudet-og-samfunnet/ombudets-arbeid/etnistiet/> accessed 2 March 2020

Likestillings- og diskrimineringsombudet, "Årskonferansen 2020" (n8) <https://www.youtube.com/watch?v=GLrLpu_cTJM&ab_channel=likestillingsombud> accessed 28 January 2021

Personvernnemda, 'Klage/saksgang' https://www.personvernnemnda.no/klage accessed 22 February 2021

Regnskap Norge, Økonomiforbundet og Revisorforeningen, Veiledning for behandling av personopplysninger i regnskapsbransjen (2020) <https://www.regnskapnorge.no/contentassets/d1e263a4d94542668b2ad099a3c2fc52/veiledning-for-behandling-av-personopplysninger-i-regnskapsbransjen-v1_1.pdf> accessed 18 February 2021

Wikipedia, 'Tingenes internett', <https://no.wikipedia.org/wiki/Tingenes_internett accessed 28.01.2015> accessed 28 January 2021

Case-law

HR-2018-2241-U, The Supreme Court of Norway (23 November 2021) <https://www.domstol.no/globalassets/upload/hret/avgjorelser/2018/avgjorelser-november/hr-2018-2241-u-sak-nr-18-155656-anonymisert.pdf> accessed 1 June 2021
20-020518MED-OTIR/04, Oslo Tingrett, Staten versus Laila Anita Bertheussen (27 August 2020)

ELSA Poland

Contributors

National Coordinator
Agnieszka Fortuna

National Researchers
Michał Wołotowski
Adam Rybczyński
Daniel Polak
Michał Gębicki
Zofia Flaczyńska
Daniel Matwiejczuk
Anna Wojciechowska
Mikołaj Stacherski

National Linguistic Editor
Emilia Chybowska

National Technical Editor
Zofia Matczuk

National Academic Supervisor
Edyta Bielak-Jomaa, doctor of the University of Lodz

Introduction

Our generation has the undoubtful privilege to witness the rapid development of Advanced Digital Technology. It shall presumably affect our lives in positive as well as negative ways in following years and decades. Some circumstances and challenges may look similar to issues that have already been regulated by international and national law. However, it is also expected that Advanced Digital Technology shall induce new, advanced legal difficulties.

That being said, the report below presents an overview of personal data protection and the issues concerning Advanced Digital Technology in the Polish legal system. It also includes presumptions about its development and possible steps that shall be taken to ensure more effective protection of human rights.

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

1.1. Advanced Digital Technologies

To begin with, the term 'Advanced Digital Technologies' refers to all kinds of programs, mechanisms, patents and algorithms which aim at processing information or carrying out an advanced manufacturing process. This definition will vary depending on the context. Polish legislation lacks legal definitions which define the concept of ADT. This is mainly due to the extraordinary complexity of this phenomenon and to the fact that technological progress has increased in recent years. For the purpose of this paper, we will focus only on digital technologies that are primarily used to obtain various information. That is any type of technology that is used for the processing of information by computer systems.[324]

Over the last decade or so, there has been significant development of new techniques for information acquisition and processing. Despite many benefits for the information society, it should be mentioned that it has also created a number of threats to the privacy and personal life of individuals. This includes the freedom and privacy of communication, the right to protection of personal information and the freedom from an arbitrary collection of information about individuals by public authorities.[325]

The right to privacy has been recognised as a fundamental guarantee and should be subject to protection by the state and its organs. The Constitution of the Republic of Poland, which stands on top of the hierarchy of legislation, refers to it in article 47. It indicates that everyone has the right to legal protection of his private and family life. Privacy is

[324] Górski Łukasz, Racjonalność technologiczna. Technologia jako system kontroli; Opublikowano: PPP 2015/7-8/200-208.
[325] Sarnecki Paweł, Prawo konstytucyjne RP, 9. Wydanie; C.H. Beck Warszawa 2014; s. 108.

understood broadly as a sphere related to private life, family life, honour and good name and the role of the state is not to violate these freedoms.[326]

Noteworthily, article 51 of the Constitution protects everyone from the disclosure of personal data without a proper legal basis. This provision is a reference to the right to privacy and defines the grounds under which information concerning a person may be disclosed. According to this provision, public authorities may collect and make available only information concerning citizens that is necessary for a democratic state ruled by law. Furthermore, this procedure cannot take place without the knowledge of the individual who should always have access to official documents and data files concerning them under certain conditions and demand the removal of untrue, incomplete information or acquired by means contrary to the statute. Moreover, every person has the right to so-called information autonomy, which means that they have the right to decide for themselves whether to disclose information concerning them to others and to exercise control over the information held by authorities.

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

2.1 Sources of law in Republic of Poland

It is crucial to start analysing the issue of citizen data protection in the Polish law system by defining the sources of law in Poland and then researching how a single type of it protects citizens' data. Another sector of this section will cover the topic of implementation of GDPR in the Polish law system.

Sources of law in Poland are divided into two types. The first one is the sources that are generally applicable provisions of law and the second is these acts of law that are internally applicable (e.g. regulations internally proclaimed in NGOs). There is a limited catalogue of acts of law that are generally applicable and the Constitution of Poland lists them in Article 87.[327] They are the Constitution itself, Acts of Parliament, ratified international conventions, decrees, and in the area of application local law acts (proclaimed e.g. by city councils or regional parliaments).

Since 2004 Poland is a member of the European Union which means that European laws are applicable in Poland - both primal (e.g. EU founding conventions) and secondary (regulations, directives and decisions). Last but not least are judicial decisions of the Court of Justice of the European Union which can help in the interpretation of hereinbefore mentioned acts.

2.2 Constitution of Poland, as basis of citizen privacy protection

[326] Tuleja Piotr (red.), Konstytucja Rzeczypospolitej Polskiej. Komentarz; Opublikowano: WKP 2019.
[327] 1. The Constitution of Poland, Article 8.

The rule of protection of privacy and personal data can be derived strictly from the Constitution of Poland and international treaties. For example, the Republic of Poland has ratified the European Convention on Human Rights. Poland has also ratified the United Nations' conventions that protect human freedom, such as The United Nations Convention on the Rights of the Child (UNCRC). It is worth mentioning that both conventions are functioning. But the most significant document is the Constitution of Poland and in the Constitution the most relevant is Article 51 which in paragraph one points out that a person can be forced to reveal information about himself only by the Acts of Parliament, which are the basic and most common method of enacting the law in Poland. The second paragraph of the mentioned article limits the amount of data which can be collected by state institutions to those that are essential to a democratic state of law. Noteworthily, paragraph four guarantees people the right of correcting or removing data that is[328] False; Not full; Gathered illegally.

The fifth and last paragraph of the Article obliges state institutions to enact regulation which will define methods of collecting and sharing hereinbefore mentioned data.

2.3 Acts of parliaments preventing privacy and personal information

The main law which protects citizens' data is regulation on protecting personal data as of 10 May 2018. But firstly, it is worth analysing other laws. E.G. the Polish Civil Code which in Article 23 makes it possible to protect personal rights in case of unlawful infringement. It is an open catalogue but Article 23 points out a few examples and one of them is the right to protect surnames.

The main instrument of protecting personal data in the Polish legislation is The Personal Data Protection Act of 10 May 2018 and 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 (General Data Protection Regulation later referred to as GDPR). That act in the very first article refers to GDPR, which is a way of transposing European Law into the Polish law system. It is worth mentioning that GDPR is a regulation which means that it has a direct effect on the law of the Member States of the EU. That means the Polish Personal Data Protection Act has an auxiliary role to GDPR so the Polish law regulates some technical aspects of personal data protection like data protection officers, the structure of the Personal Data Protection Office, the President of it and procedure in case of data protection breaches. The Personal Data Protection Act does not provide for a regime of the procedure before the President of Personal Data Protection and only makes reference in Article 7 to the Code of Administrative Procedure.

Moving to the next type of laws in Poland, domestic regulations, enforced on the basis of the Personal Data Protection Act, do not have additional methods of protecting personal

[328] The Constitution of the Republic of Poland, Article 51.

data. These regulations have a technical nature and e.g. the model of the ID card of a clerk of the Office for the Protection of Personal Data.
Acts of local councils do not have extra means of data protection but bodies of territorial self-government, which processes personal data, are obliged to appoint personal data officers. Examples of such authorities are officers acting in communes or voivodeship personal data officers.

2.4 Definition of personal data in the Polish legal system.

As mentioned above, Polish legislation does not contain a definition of personal data, instead derives a definition of it from GDPR, which means that European regulations are a good place to find such definition. GDPR in Article 4 states that personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This definition is a bit complicated so there are both domestic and foreign publications that help in that task. One of the main sources is GDPR itself and especially motives of them included in the preamble. Motive 30 makes an enumeration of online identifiers which with natural persons can be associated with internet protocol addresses or cookie identifiers. Motive 35 clarifies the term of personal data concerning health such as genetic tests results or information about disability, medical history and clinical treatment. Motive 26 of GDPR determines which data has to be protected and points out that the information is the one that allows identifying natural persons but only in cases where costs of identification are responsible and in technical means. That motive also concludes that anonymous information does not have to be protected in scientific or statistical research and purposes.

There are also domestic interpretations of GDPR e.g. Data Protection Officer Vademecum published in 2020. It is a practical commentary which also points out which actions a Data Protection Officer can conduct to protect the data legally. Other helpful information, which can be found in this publication, is related to which cases data needs to be protected. And these are the data which was:

1) acquired, transmitted and modified in the processes of acquisition, registration, profile changes and cooperation with the parties;
2) collected in the procedure of importing data from external sources, including the transfer of personal data provided for in the national legislation
3) processed in the course of the data subjects' use of the services and the fulfilment of the administrator obligations, including public authorities and obligations, the exercise of rights or contracts

4) produced at the initiative of, at the request of, or for the benefit of the data subject
5) produced by the activity of data subject in relationship with the administrator
6) produced by the controller for the data subject or about the data subject
7) inferred or deducted by the controller about the data subject.[329]

The following section of the Vademecum discusses these categories and gives practical leads to data protection officers e.g. in point one there is a term 'identification test' which is a method that can classify data as personal. Moving further to the second point, vademecum suggests notifying the moment when data has been transferred.

2.5 Implementation of GDPR in the law of the Republic of Poland

Given the examples indicated above, it can be concluded that the Data Protection Act is compliant with the GDPR. That compliance comes from two sources:
-The indication of GDPR directly in the Act
-The creation of tools which are the implementation of the articles of the GDPR
The first situation occurs not only in the most important fragment of the Act, e.g. the definition of personal data but also in Article 8 concerning the appointment of a data protection officer, which states that the officer shall be appointed in the cases and according to the procedure set out in the GDPR.

Situation no. 2 occurs in case of certification of entities, which is encouraged by the GDPR in Article 42, while the Act on personal data protection implements this postulate by creating an appropriate legal framework in Articles 15 - 26. A similar situation occurs in case of appointment and functioning of the President of the Office for Personal Data Protection, which is included in Chapter 6 of the Act on personal data protection 'The President of the Office', which is a supervisory authority in the meaning of Article 51 of the GDPR. From 2019 the President of the Personal Data Protection Office is Jan Nowak. It is important to emphasise that the procedure includes acceptance from both Chambers of the Polish Parliament, which is a guarantee of impartiality and independence from political parties. Other guarantees are mentioned in Article 34 Paragraph 5 which says that the President of Office in exercising his duties is subject to the act and only to it. There is also another guarantee in the mentioned article which states that the dismissal of the President can be done only in certain situations.

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 Importance of self-regulation

[329] List and later references to it, are from M. Kołodziej (red.), Vademecum Inspektora Ochrony Danych, Warszawa 2020.

National regulations are not always a sufficient way to regulate specific areas of social relations. This is particularly true in the private sector. This allows private entities to manage risks more effectively and to tailor appropriate policy solutions within their organisations. Of the many areas of regulation affecting businesses and other organizations is personal data protection. This field is particularly vulnerable to various complications, which in European legislation involve high financial penalties, and costly to implement obligations. The private sector is aware of these consequences and therefore tries to avoid them by demonstrating to the authorities that it is acting in accordance with the data protection law. This is where the reference to internal regulations proves to be particularly effective.

Both the regulations of the European Union,[330] of which Poland is a member, and the regulations of Poland[331] itself allow the private sector to use mechanisms based on the creation of internal regulations and then obtain approval for them from a competent authority. Although self-regulation in the field of personal data protection is complementary to external regulation, it has an important function in the process of adapting regulations to specific sectors.

3.2 Code of conduct

The principle of accountability introduced in the GDPR indicates controllers as the entities responsible for complying with the provisions of the Regulation and demonstrating compliance. The provisions in Articles 40 and 41 of the GDPR refer to codes of conduct (hereinafter 'code') as an effective and applicable way to achieve adequate coherence of protection in terms of personal data protection rights. As mentioned in EU guidelines: Codes can act as a mechanism to demonstrate compliance with the GDPR. Notably, they can help to bridge the harmonisation gaps that may exist between the Member States in their application of data protection law.[332] The regulations also provide an opportunity for collaboration in the development of sector-specific data protection rules that will meet the requirements of the GDPR.

3.2.1 Code of conduct in EU regulation

The content of Article 40 of the GDPR defines codes of conduct as documents intended to assist in the proper application of the Regulation (GDPR). However, they are not generally applicable law and are therefore referred to as self-regulation i.e. voluntary

[330] 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), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[331] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, <http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000&type=3> accessed 26 March 2021.

[332] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Version 2.0, 4 June 2019 <https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en.> accessed 26 March 2021.

commitments by the entities that implement the code. There is widespread agreement that "Codes can provide a degree of co-regulation and they could decrease the level of reliance tha controllers and processors may sometimes place upon data protection supervisory authorities."[333] The creation of codes of conduct is carried out by entities that represent a group of entrepreneurs. The most common initiators of codes of conduct include industry organisations that bring together entrepreneurs from a particular sector. Usually, the legal form of those organizations are associations, professional and business self-governments. The indication of the relevant legal provisions does not constitute the exhaustive content of the code of conduct but may be accessory to the detailed procedures created on the basis of the characteristics of the given sector. Modifications of the code of conduct can only be carried out by the entity responsible for its creation. The supervisory authority does not have this possibility, but it is competent to give its opinion on the draft and to approve the code. It follows from paragraph 4 of Article 40 of the GDPR that the content of the code must mandatorily include a mechanism for monitoring compliance with the code.

3.2.2 Procedure for approving the code of conduct

The essence of cooperation between the public and the private sector can be seen in the procedure for the opinion on the draft code indicated in paragraph 5 of the above article. The entity, to which the authorship of the code is attributed, is obliged to present the draft to the national supervisory authority. On verification, the supervisory authority gives a positive opinion with approval of the draft if it meets the requirement of adequate security. In case of an unfavourable opinion, this will require the draft to be reconfigured and then resubmitted to the authority. This can be considered as an area where the supervisory authority interferes with the content of the code of conduct at its drafting stage. The procedure described above also includes amendments to the code of conduct. Detailed issues concerning the procedure of preparation and approval of the code have been included in the national regulation on personal data protection. It has found its externalization in the Act of 10 May 2018 on personal data protection. Article 27 complements the regulation placed in Article 40 of the GDPR. Paragraph 2 of Article 27 of this law contains the obligation to consult the stakeholders (i.e. the persons to whom the code is to apply) before the code is presented to the supervisory authority. The object of the consultation is to present a draft and to provide an opportunity to give an opinion on the provisions included therein. The fact that a consultation has taken place, together with its results and the draft code of conduct, must be submitted to the supervisory authority. The President of the office (Polish supervisory authority) may request the entity to consult again if, in the opinion of the president of the office, the consultation is not sufficient while specifying its scope. The person applying for the approval of the code of conduct shall be deemed to be a party to the procedure for approving the code of conduct.

[333] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, 4 June 2019.

Amendments to the code are also subject to mandatory consultation and reporting of the results to the supervisory authority.

3.2.3 Publication of the code of conduct

It is the responsibility of the authority, among other things, to place the approved code of conduct in the relevant register and to publish it. The issue of a draft code of conduct covering processing activities in several Member States is addressed in paragraph 7 of Article 40 GDPR. The supervisory authority, before approving the draft code, submits it to the European Data Protection Board, which is competent to give an opinion on the compliance of the draft code with the regulation. Only a positive opinion of this body allows the national supervisory authority to approve the code. Paragraph 8 of the Article indicates that the procedure is continued with regard to the approved draft and that it is presented to the Commission which may, by means of an implementing act, declare the code of conduct to be generally applicable in the EU. It is also the responsibility of the Commission to adequately publicise the codes and to collect already approved codes of conduct in a register and make them available to the public. As outlined above, the procedure for setting up and approving a code of conduct requires the sectoral stakeholders to reach an appropriate agreement on the content of the code with the authority responsible for its approval. However, it leaves a wide margin for developers to design solutions that take into account the specificities of a given sector.

3.2.4 Accreditation

For the code to fulfil its function and be effective, an entity responsible for monitoring compliance with the code is needed. Article 41 of the GDPR indicates the requirements this entity must meet, namely:

1) have an adequate level of expertise in the field covered by the code
2) has been accredited by the relevant supervisory authority

It is important to mention here that the aforementioned article stipulates that the act of monitoring compliance with the code of conduct by an accredited entity does not deprive the supervisory authority of its authority to monitor compliance with the GDPR. Further requirements for the monitoring entity also appear in relation to obtaining accreditation. These are, in turn:

1) the need to demonstrate to the relevant supervisory authority independence and expertise in the field covered by the code;
2) to have procedures in place that allow the monitor to assess the ability of specific controllers and processors to apply the code, to monitor their compliance with the code and to review its operation periodically;
3) having procedures and structures in place to address complaints about violations of the code by a controller or processor or about the way the code is implemented or enforced by a controller or processor and to ensure that these procedures and structures are transparent to data subjects and the public;

4) the need to demonstrate to the competent supervisory authority that its tasks and responsibilities do not give rise to a conflict of interest.

All of these requirements must be met together to obtain accreditation. The issues related to the application for accreditation are further clarified in the Polish Data Protection Act in Articles 29 and 30. The necessary elements of the application are information to identify the entity applying for accreditation, its address data and confirmation that the accreditation criteria are met. To process the application efficiently, the national legislator has introduced a 3-month period from the moment of submitting the application for accreditation for the assessment of the condition of meeting the accreditation criteria. A positive assessment results in a notification of granting accreditation to the applicant, whereas a negative assessment results in a notification of refusal to grant accreditation. In the situation of formal deficiencies in the application, there are two solutions, depending on the type of deficiencies. In case of lack of information identifying the applicant or his address data, the consequence is leaving the application without examination. Failure to include in the application information confirming meeting the accreditation criteria, failure to attach documents required by the regulations or failure to meet the requirements related to the form of the application is less severe in its consequences as the consequence of these deficiencies is a call for supplementation as well as an instruction on leaving the application unrecognized in the event of failure to meet the deadline of 7 days from the date of delivery of the call. The authority refuses accreditation if they find that the applying entity does not meet the accreditation criteria. The refusal takes the form of an administrative decision, which can be appealed to the administrative court. Successful completion of the accreditation process is crowned with the issuance of an accreditation certificate which is a document confirming the fulfilment of accreditation criteria.

The obligation to propose accreditation requirements for the entity responsible for monitoring compliance with the code of conduct to the European Data Protection Board lies with the supervisory authority. This is directly related to the consistency mechanism whereby supervisory authorities cooperate among themselves and with the European Commission.

3.2.5 Breaching code of conduct

The code monitor must take appropriate action if there is a breach of the code by a processor or controller. This takes the form of suspending or excluding that processor. At the same time, it shall inform the supervisory authority of the incident, which is entitled to exercise its tasks and powers with respect to the entities responsible for violations of the code of conduct as well as with respect to the code monitors. Another power of the supervisory authority in this area is the possibility of a withdrawal of accreditation if the monitoring entity does not meet or no longer meets the requirements for accreditation or if its actions do not comply with the provisions of the Regulation. However, monitoring compliance with the Code does not apply to public authorities and entities carrying out (data) processing. A breach of the obligation of the monitoring entity to take appropriate

action in the event of a breach of the Code may result in the imposition of a fine by the supervisory authority.

3.3 The code of good practices in the scope of processing of personal data by banks and credit register as example of self-regulation

In Poland, at the moment, draft codes of conduct are being prepared, while none of them has been officially approved yet. One example of such a project is "The code of good practices in the scope of processing of personal data by banks and credit register" (hereinafter referred to as the Project of Code or Project).[334] The Project mentioned above shows the importance of adjusting regulations at the sectoral level. The code of good practices was an attempt to adapt the GDPR regulations to the banking sector, where the regulations are highly relevant.

3.3.1 Origins of the code of good practices

The Polish Banks Association was guided by the desire to design an accessible and easy to read Code of Conduct so that it could serve the largest possible number of entities connected with the banking sector. The Project of Code constitutes a set of rules of conduct on personal data protection in the Polish banking sector, being a further specification of the principles of personal data processing and protection defined in the GDPR, taking into account the specificity of the banking sector. It contains a direct statement that it constitutes a Code of Conduct within the meaning of Article 40 of the GDPR. Its scope of application covers domestic banks and credit registers operating in the territory of the Republic of Poland, which are also members of the Polish Bank Association. Interestingly, other entities may also be included in the application of the Project of Code with the reservation that only to the extent of providing such services to banks and credit registers. The subject matter of the Project relates to the processing of personal data of clients, including persons whose data is processed by credit registers, in connection with the implementation by these registers of the duties and powers indicated in the relevant provisions of law. At the same time, it is necessary to mention that the Project does not apply to the processing of personal data of employees, co-workers and candidates for work in banks and credit registers.

3.3.2 Contents of the Project of Code of good practices

The Project of Code is structured in eight thematic parts which are divided into chapters. The first of these acts as a collection of information and abbreviations used in its content. Covered in the glossary are definitions such as 'controller', 'personal data', 'profiling', 'pseudonymization', 'consent', 'supervisory authority', 'credit registry', 'customer', and 'group'. The next part of the Project is a descriptive account of the three most relevant issues to which specific chapters are devoted. These are, in turn, principles concerning the processing of personal data; legal grounds for the processing of personal data; conditions

[334] <https://uodo.gov.pl/pl/file/2362> accessed 26 March 2021.

for obtaining consent to the processing of personal data. In the next part of the Project, the principles are presented together with the way banks and credit registers realise the rights of persons to whom the data are attributed. The rules are divided into general ones, i.e. referring to each right indicated in the Project, and detailed provisions related to the realisation of specific rights. The Project of Code also includes precise regulations related to storing and deleting personal data. Implementing the general principle that personal data of actual or potential clients must not be stored in a form that allows its identification for longer than it is necessary for the purposes for which the data is processed. The Project provides that once the intended purposes have been achieved, the data should be deleted unless there is a legal justification for doing so. The set of principles on the process of profiling and automated processing of personal data placed in the Project explains that profiling is a method of processing personal data that can be based on various models and algorithms. It also provides a possibility for banks, which in their role of controllers may use the exemplary provisions included in one of the appendices of the Project in contracts concluded with other processors. From the point of view of data protection, the important provisions are those covering the situation where a personal data breach has occurred that is subject to notification to the supervisory authority or to the persons to whom the data relate. In the context of assessing the effects of data processing, the Project of Code sets out examples of circumstances in which banks and credit registers should carry out such assessments. The integral elements of the Project also include appendices containing, among others, a model notification of a personal data breach; a description of an exemplary scoring model; the scope of information provided to the client; exemplary provisions of agreements concluded with processors; examples of automated processing of personal data. It can be concluded that the Project is of great importance in acting as a tool for the Polish banking sector to properly adapt to the requirements provided by the GDPR.

3.4 Summary

The Code of Conduct is a unique institution that uses the mechanism of self-regulation with simultaneous support in its compliance by the authorities. It allows an advanced adaptation of data protection procedures to the specifics of a particular sector. Cooperation between the private and the public sector is regulated by the provisions explained above which allow achieving the intended effects.

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

4.1 Legislation on the process of judicial review of cases of data protection breach

In order to provide an answer to the question on the process of judicial review of cases of the data protection breach in the Polish legal system, provisions of multiple different acts need to be taken into account. First and foremost, the legal basis for judicial review in such

cases is regulated by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter: GDPR). Chapter 8, Art. 77 to Art. 84 deal with remedies, liability and penalties under GDPR. Art. 79 GDPR provides that data subject is entitled to an effective judicial remedy against a controller or processor, without prejudice to any available administrative or non-judicial remedy, in cases of infringement of rights resulting from non-compliance with GDPR. Furthermore, Art. 82 GDPR sets forth that any person who has suffered either material or non-material damage resulting from non-compliance with GDPR is entitled to receive compensation from the controller or processor for the damage. The action aimed to exercise this right can also be brought before the court.

With the general framework of regulation found in GDPR, the detailed nature of the proceeding is determined by national legislation. In the Polish legal system provision on judicial review of cases of data protection breach is found in numerous acts.

One of them is the Act on Personal Data Protection of 10 May 2018 (hereinafter: PDP Act). The purpose of the PDP Act is to ensure the application of GDPR in Poland. Within its regulatory scope, it also implements Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. The subject matter of proceedings before the court is regulated by provisions of chapter 10, Art. 92 to Art. 100 of the PDP Act. Regulations of this chapter forejudge the civil character of such proceedings and determine that claims are to be pursued in accordance with the procedural civil law.[335] Furthermore, as stated in the substantiation to the project of the PDP Act, provisions of this act are order-related.[336]

However, the PDP Act does not provide exhaustive regulation on the process of judicial review. As provided by Art. 100 PDP Act, the provisions of the Code of Civil Procedure Act of 17 November 1964 (hereinafter PCCP Act) are to be applied to proceedings concerning the claims arising from a breach of personal data protection provisions referred to in Art. 79 and Art. 82 GDPR. PCCP Act contains the core of Polish procedural civil law, governing court proceedings in civil, family and custodial law and labour law cases, as well as in social insurance cases and other cases to which the provisions of the PCCP Act apply by virtue of special provisions of different acts.[337]

Furthermore, by virtue of Art. 92 of the PDP Act, to the extent not regulated by GDPR, the claims arising from a breach of personal data protection provisions referred to in Art. 79 and Art. 82 GDPR, the provisions of the Civil Code Act of 23 April 1964 (hereinafter: Civil Code) are applicable. With that in mind, it could be said that the role of the Civil Code's regulations is to supplement the provisions of GDPR on civil claims of the data

[335] B. Gubernat/S. Szczepaniak *[in:]* Ustawa o ochronie danych osobowych. Komentarz, *red. M. Czerniawski, M. Kawecki*, Warszawa 2019, Art. 92.
[336] Substantiation to the project of the Act on Personal Data Protection, p. 41; found on: <https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2410> accessed 25 February 2021.
[337] Code of Civil Procedure Act of 17 November 1964, Art. 1.

subject.[338] Considering the nature of proceedings in cases of data protection breach, it can be expected that in particular provisions on the infringement and protection of personal interests (Art. 23 and Art. 24 Civil Code) and the provisions on delicts (Art. 415 et seq. Civil Code) will be applied.[339][340]

4.2 Jurisdiction of the court

4.2.1 State of the court and territorial jurisdiction of the court

Article 79.2 GDPR sets forth two important rules. Firstly, it indicates the Member State whose court will have the power to issue a judgment. Secondly, it determines the territorial jurisdiction of the courts of that particular Member State. The territorial jurisdiction of the courts is alternative, meaning that the data subject can choose before which court the action will be brought. The data subject can bring action against a controller or a processor either before the court of the Member State, where the controller or processor has an establishment or before the court of the Member State, where the data subject has their habitual residence. In cases in which the controller or processor is a public authority of a Member State acting in the exercise of its public powers, alternative jurisdiction of the courts is excluded. In such cases, action should be brought before the court of the Member State where the controller or processor has an establishment.[341] In cases of exercising the right to receive compensation under Art. 82 GDPR, jurisdiction of the court is to be determined with the same principles as under Art. 79 section 2 GDPR.

4.2.2 Subject-matter jurisdiction of the court

When the provisions of the GDPR indicate the Polish court as the court competent to decide on the claim, the subject-matter jurisdiction of the court is to be determined following provisions of the PDP Act. As provided by Art. 93 of the PDP Act, the claims arising from a breach of personal data protection provisions referred to in Art. 79 and Art. 82 GDPR lie within the subject-matter jurisdiction of the district courts. It should be noted that with the adoption of the PDP Act the PCCP Act was amended. In accordance with newly added Art. 17.4^5, all claims resulting from the violation of rights under the provisions on the protection of personal data are included in the scope of jurisdiction of district courts.

As indicated by the legislator in the substantiation to the PDP Act, the decision to grant jurisdiction to the district courts in those matters was dictated by the principle of procedural economy. It has been argued that it would prevent unnecessary prolongation of proceedings since the number of cases heard by district courts is lesser than that of

[338] P. Fajgielski [in:] *Komentarz do ustawy o ochronie danych osobowych [in:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, Art. 92.
[339] ibidem
[340] B. Gubernat/S. Szczepaniak *[in:]* Ustawa o ochronie danych osobowych. Komentarz, *red. M. Czerniawski, M. Kawecki*, Warszawa 2019, Art. 92.
[341] P. Barta [in:] Ustawa o ochronie danych osobowych. Komentarz, red. *P. Litwiński*, Warszawa 2018, Art. 93

regional courts.[342] This, however, seems not to be the only factor. As a general rule, district courts rule on cases in which specific knowledge and expertise are required, such as cases on industrial property rights[343] or intellectual property rights.[344] Furthermore, cases of data protection breaches are closely bound with cases of protection of personal interests, over which district courts also have jurisdiction.[345] Considering the importance of issues related to the protection of personal data and the highly specialized nature of this matter, placing it within the subject-matter jurisdiction of the district courts can only be deemed as reasonable.[346]

4.3 Bringing an action before court

Action (lawsuit) is a core institution in civil proceedings. It is a demand of the complainant, addressed to the court, to issue a judgement based on specific factual circumstances.[347] Action brought must satisfy certain formal requirements established by the PCCP Act. Among others, the action is to specify the claim, indicate the facts on which the claim is based on and, if necessary, justify the jurisdiction of the court. Furthermore, information on whether the parties have attempted either mediation or other forms of alternative dispute resolution, and if such attempts have not been made, an explanation of the reasons for not taking them should be included.[348] Filed action has to also meet the general requirements for any other procedural document and include, inter alia, a designation of the court to which it is addressed, forenames and surnames or names of the parties, their statutory representatives and plenipotentiaries, a signature of the party or its statutory representative or plenipotentiary and listing of the attachments.[349]

As discussed before, following Art. 79 GDPR, each data subject, whose rights have been infringed upon as a result of non-compliance with GDPR, is entitled to bring such an action before the court against a controller or a processor. Similarly, as provided by Art. 82 GDPR, action before the court can be brought by any data subject who has suffered either material or non-material damage resulting from non-compliance with GDPR and has the right to pursue compensation from the controller or processor for the damage.

4.4 Composition of the court and appellate proceeding

In the Court first instance, the case is to be heard by a single judge, unless specific provisions provide otherwise.[350] However, the president of the court may order for a case

[342] Substantiation to the project of the Act on Personal Data Protection, p. 41; found on: https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2410 [Accessed on the 25th of February 2021].
[343] Industrial Property Law Act of 30 June 2000, Art. 294.
[344] Code of Civil Procedure Act of 17 November 1964, Art. 479[90]
[345] ibid art. 17.1.
[346] N. Zawadzka [in:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Warszawa 2019, Art. 93; O. Legat [in:] *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Warszawa 2018, Art. 93.
[347] A. Marciniak [in:] Postępowanie cywilne w zarysie, 13 edition, red. T. Pietrzak, Warszawa 2020.
[348] Code of Civil Procedure Act of 17 November 1964, Art. 187 § 1.
[349] ibid art. 126 § 1.
[350] ibid, art. 47 § 1.

to be heard by three judges if they deem it advisable due to the particular complexity or precedential nature of the case.[351]

The principle of two-instance proceedings of the courts is guaranteed by virtue of Art. 176 of the Constitution. This, together with the constitutional right to appeal against judgments and decisions made in the first instance proceeding,[352] serves to fulfil the fair trial principle.[353] Accordingly, Art. 367 § 2 PCCP Act sets forth that appeals from the ruling of district courts given in the first instance are to be heard by the appellate court. PCCP Act adopted a system of full appeal (cum beneficio bonorum).[354][355] The Court of second instance is the second substantive instance in civil proceedings, and as such appellate proceeding retains the nature of the examination procedure. The court of second instance therefore has full jurisdictional freedom, limited only by the limits of the appeal.[356] At the same time, although the appellate proceeding is substantive in its nature, it also is of a control character.[357] This serves not only to control any errors of the court of first instance but also allows to remedy the errors of the parties by allowing the parties to invoke new facts and evidence.[358]

Before the court of second instance, the case is heard by three judges.[359] In this case, the collegiality serves to guarantee both the independence and impartiality of the judges and the pluralization of the judgment.[360]

4.5 Role of the President of the Office for Personal Data Protection in the process of judicial review of cases of data protection breach

GDPR imposes an obligation on each Member State to establish at least one independent public authority (supervisory authority) responsible for monitoring the application of the GDPR. Polish regulations on supervisory authority are subject to the PDP Act. The Polish national supervisory authority is President of the Office for Personal Data Protection (hereinafter: President of the Office).

4.5.1 General provisions

By virtue of Art. 94 PDP Act, the court is to notify the President of the Office of a lawsuit concerning claims arising from a breach of personal data protection provisions referred to in Art. 79 and Art. 82 GDPR. The court is also obliged to notify the President of the

[351] ibid art. 47 § 4.
[352] The Constitution of the Republic of Poland of 2 April 1997, Art. 78.
[353] A. Łazarska/K. Górski [in:] Kodeks postępowania cywilnego. Komentarz. Komentarz. Art. 1–505[39]. Tom I, *T. Szanciło* (red.), Warszawa 2019, Art. 367.
[354] *K. Flaga-Gieruszyńska*, *A. Zieliński*, Kodeks postępowania cywilnego. Komentarz. Wyd. 10, Warszawa 2019, Art. 367.
[355] Łazarska (n 353).
[356] Judgment of Supreme Court of 15 February 2006, case number IV CK 384/05.
[357] Judgment of Supreme Court of 16 May 2006, case number I PK 210/05.
[358] Flaga-Gieruszyńska (n 354).
[359] Code of Civil Procedure Act of 17 November 1964, Art. 367 § 3.
[360] Łazarska (n 353), Art. 47.

Office of final and non-appealable rulings given in such proceedings.[361] Furthermore, after being notified of a pending proceeding, the President of the Office is to inform the court of any case concerning the same breach of personal data protection provisions that is either pending or has already been concluded before the supervisory authority or before the administrative court.[362] This provision aims to ensure swift communication between courts and the President of the Office.[363]

PDP Act also provides regulations on the mutual relation between pending civil court proceedings and proceedings pending before the President of the Office or before administrative court.[364] Art. 95 PDP Act sets forth that the court is to suspend the proceedings if the case concerning the same infringement of the provisions on the protection of personal data has been initiated before the President of the Office. The suspension is not facultative but obligatory. After the decision is issued by the President of the Office (or a judgment of administrative court issued in lieu of a decision in the event of inactivity of the supervisory authority) the court is to resume proceedings ex officio, in accordance with provisions of The PCCP Act.[365,366]

Furthermore, Art. 96 PDP Act provides that the court is to discontinue the proceedings to the extent to which a final and non-appealable decision of the President of the Office or a final and non-appealable judgement of the administrative court (issued in lieu of a decision in the event of inactivity of the supervisory authority) declaring a breach of personal data protection provisions covers the claim pursued before the court. This is due to the fact that issuing a judgment by a civil court becomes redundant to the extent that the decision of the President of the Office or a judgment of an administrative court fulfils the request of the complainant.[367] Instances, when controller or processor are imposed with an administrative fine by the decision the President of the Office or a judgment of an administrative court, do not provide grounds for discontinuation of the civil proceeding in which damages for breach of the provisions on the protection of personal data are pursued, since both are different types of liability (administrative liability and civil liability).[368369]

Those provisions aim to prevent situations in which disparate rulings on the subject of the same facts would be issued by the court and the supervisory body.[370] This is due to the fact that by virtue of Art. 97 PDP Act findings of the final and non-appealable decisions of the

[361] Act on Personal Data Protection of 10 May 2018, Art. 94.1.
[362] ibid, Art. 94.2.
[363] Substantiation to the project of the Act on Personal Data Protection, p. 41; found on: <https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2410> [Accessed on 25 February 2021].
[364] ibidem, p. 41-42.
[365] Zawadzka (n 346), Art. 95.
[366] Legat (n 346), Art. 95.
[367] ibidem, Art. 96.
[368] Fajgielski (n 338), Art. 96.
[369] B. Gubernat/S. Szczepaniak *[in:]* Ustawa o ochronie danych osobowych. Komentarz, *red. M. Czerniawski, M. Kawecki*, Warszawa 2019, Art. 96.
[370] ibid art. 94.

President of the Office and findings of final and non-appealable judgements of the administrative court issued in lieu of a decision in the event of inactivity of the supervisory authority declaring a breach of personal data protection provisions bind the court in the civil proceedings for damages resulting from said breaches. Such regulation is a result of the highly specialised nature and role of the President of the Office.[371] As such, provisions of Art. 94, Art. 95 and Art. 96 PDP Act were adopted with the consideration of prejudicial character of above discussed rulings.[372]

4.5.2 Powers of the President of the Office in the proceeding

By virtue of the PDP Act, the President of the Office is given substantial powers in the process of judicial review. First and foremost it should be noted that, as provided by Art. 98 PDP Act, in cases concerning claims arising from the violation of the provisions on the protection of personal data, that may be pursued only in proceedings before the court, the President of the Office may bring an action on behalf of the data subject, with the consent of the data subject. Furthermore, with the consent of the complainant (in this case-data subject who brought an action before the court on its behalf), may join the proceedings at any stage.[373] This serves to fulfil the obligation imposed by Art. 58.5 GDPR, which provides that each Member State shall provide supervisory authority with the power to initiate proceedings before judicial authorities, or engage in such proceedings otherwise, in cases related to the violation of the provisions of GDPR.[374][375] Furthermore, in other cases concerning claims arising from the violation of the provisions on the protection of personal data, the President of the Office may, with the consent of the complainant, join proceedings before the court at any stage. However, in such cases, joinder is not possible when any proceeding concerning the same violation of the provisions on the protection of personal data is pending before the President of the Office.[376]

The provisions of the PCCP Act on public prosecutors are to be applied accordingly to the participation of the President of the Office in such proceedings before the court.[377] In particular, it should be noted that it grants the President of the Office power to appeal against any court decision against which an appeal is permitted.[378] This, however, is limited only to actions taken for the benefit of the complainant.[379]

Moreover, as provided by Art. 99 PDP Act, if the President of the Office deems that it is in the public interest, they present to the court a view relevant to the case concerning claims arising from the violation of the provisions on the protection of personal data. It is

[371] Fajgielski (n 368), Art. 97.
[372] O. Legat [in:] *Ustawa o ochronie danych osobowych. Komentarz,* red. B. Marcinkowski, Warszawa 2018, Art. 94.
[373] Act on Personal Data Protection of 10 May 2018, Art. 98 § 1
[374] Zawadzka(n 346), Art. 98.
[375] O. Legat [in:] *Ustawa o ochronie danych osobowych. Komentarz,* red. B. Marcinkowski, Warszawa 2018, Art. 98.
[376] Act on Personal Data Protection of 10 May 2018, Art. 98 § 2.
[377] Act on Personal Data Protection of 10 May 2018, Art. 98 § 3.
[378] Art. 60 PCCP Act applied accordingly by virtue of Art. 98 PDP Act.
[379] Fajgielski (n 338), Art. 98.

understood that 'public interest' should be perceived through the scope of nature of the case or the impact that future judgement might have on public order or the rights of the data subjects.[380] As such, this power should not be exercised in cases where it would only be justified by the private interest of the complainant.[381] Exercising this power is possible before courts of both instances and also in the cassation appeal proceeding.[382] Presenting such a view does not amount to the joinder of the President of the Office to the pending proceeding.[383] While the court is not bound by the presented view, it should address it in the justification of the judgement.[384]

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

As was mentioned above, the Polish supervisory authority is the President of the Office.[385] He replaced the General Inspector of Personal Data Protection, who did not hold strong enough competencies to supervise compliance with GDPR.[386] However, it has to be taken into account that an effective review of data protection requires cooperation between various entities and diversified measures.

5.1. Institutional safeguards of supervisory authority

The independence of the President of the Office as the supervisory authority is guaranteed through not being bound to any instructions, term of office, immunity. They shall not belong to a political party as well. Their position is assessed in legal literature as similar to other bodies responsible for the protection of rights and control of the state. However, they are not mentioned in the Constitution.[387] The President of the Office may request to change national provisions in order to ensure more effective data protection.[388]

5.2. Measures given to supervisory authority to conduct a review

According to both GDPR and the PDP Act provisions, the President of the Office monitors enforcement of data protection regulation through investigations, receiving complaints from affected persons and reports about breach threads from controllers.

Controllers shall complete a form with necessary information about incidents and define a thread of data protection and personal rights violation as well as whether they have informed the data subject about possible consequences. In 2019 the President of the Office received 6039 reports - whilst 2446 in 2018 from 25 May - which may indicate an

---

[380] B. Gubernat/S. Szczepaniak *[in:]* Ustawa o ochronie danych osobowych. Komentarz, *red. M. Czerniawski, M. Kawecki*, Warszawa 2019, Art. 99.
[381] Fajgielski (n 338), Art. 99.
[382] Zawadzka (n 346), Art. 99.
[383] Legat (n 346), Art. 99.
[384] Zawadzka (n 346), Art. 99.
[385] Article 34 of the Act of 10 May 2018 on personal data protection.
[386] Anna Dmochowska, Marcin Zadrożny, *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem wytycznych GR art. 29, ustawy o ochronie danych osobowych z 2018 roku,* CH Beck 2018.
[387] Paweł Litwiński, Ustawa o ochronie danych osobowych. Komentarz, CH Beck 2018.
[388] Article 52 of the Act of 18 May 2018 on the protection of personal data.

increase of awareness in matters of data protection among controllers. In 2019 growth of reports related to breaches caused by malware, phishing etc. has led the President of the Office to cooperate with the National Research Institute NASK in order to share information about data protection breaches in civilian cyberspace.[389, 390]

Articles 78 and 84 of the PDP Act regulate the conditions and safeguards of an investigation. In case of provided data protection breaches, the President of the Office initiates a proceeding based on article 60 of the PDP Act. It is conducted in accordance with the Polish Code of Administrative Procedure (further as the CoAP).[391] The single-instance nature of the proceeding is an exception of the constitutional principle of two-instance proceedings, which are recognised as a better guarantee of access to a court (or a public authority) and procedural control of the proceedings.[392] The punished subject cannot appeal the decision to the higher instance on the administrative path. Despite that, the President's decisions still can be appealed to the administrative court. The action in administrative court may be, however, time- and cost-consuming. In 2019, 89 of 1329 decisions of the President of the Office have been appealed to the administrative court.[393] Thus decisions were appropriate and their recipients admitted to violating regulations. In 2019 more than 9000 complaints have been submitted to the President of the Office by the data subject or its authorised person.[394] However, before submission, a complainant is obliged to request the controller to prevent or stop unlawful actions. In case of no answer or success, a complaint to the President of the Office is available. Legal protection by the supervisory authority also requires some additional steps and takes time, which, in case of data breaches, plays a relevant role. If there has been a violation, the President of the Office orders, as a result of an administrative proceeding, to restore the legal status or a financial penalty. The latter is a discretionary decision of the President of the Office and shall not be required by a complainant.

Even the most appropriate imposes do not ensure data protection if they cannot be effectively executed. In proceedings conducted by the President of the Office applies the Act of 17 June 1966 on enforcement proceedings in administration.[395] In 2019 all decisions were enforced with 92% sufficiency, which is positively assumed.[396]

5.3. Support in data protection provided by Data Protection Officers

---

[389] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych z 2019 roku, site 122, <https://uodo.gov.pl/437>, access 25 February 2021.
[390] NASK is a national research institute subordinated by the Chancellery of the Polish Prime Minister. Its task is to ensure and develop cybersecurity in Poland.
[391] Official Journal of Laws Dz. U. 2020, position 256.
[392] Bogusław Banaszak, Konstytucja Rzeczypospolitej Polskiej. Komentarz, CH Beck 2012.
[393] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych z 2019 roku, site 25, <https://uodo.gov.pl/437>, access 25 February 2021.
[394] ibid.
[395] Official Journal of Laws Dz.U. 2020, position 1427.
[396] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych z 2019 roku, site 85-88, <https://uodo.gov.pl/437>, access 25 February 2021.

In some cases, controllers who are liable to comply with data protection law shall receive professional support from data protection officers (hereinafter: DPO) to ensure effective data protection. The DPO monitors compliance with data protection regulations, advises in matters of data processing, as well as cooperates with the President of the Office. Controllers are obliged to designate DPO in three kinds of cases. Two of them refer to a large scale of data processing and special categories of data. The last circumstance is processing by a public authority, except for courts acting in their judicial capacity.[397] Referring to art. 9 of the Act, in matters of data protection law, public authorities are entities of the public finance sector, research institutes and the National Bank of Poland. However the provisions do not oblige every controller to appoint DPO, it is recommended because of its positive influence on data protection.[398] However, the DPO's advising (or even not advising, when DPO is not considered in the matter of data protection) does not release the administrator from liability of data protection. It shall be questioned, how to raise awareness among administrators about how the DPOs' support plays a significant role in ensuring data protection and their advice shall be taken into account in each case. In addition to that, DPOs shall be more sufficiently funded and informed by the organisation to fulfil the compliance effectively.

5.4 Features of judicial review which are relevant for effective data protection

Besides remedies available in administrative proceedings, legal actions to protect personal data may be taken by the court. The matter of data protection breaches is a case for one of 45 district courts.[399] Article 79 sec. 2 of GDPR provides alternative local jurisdiction, which is more favourable for the complainant. Namely, competent is a court where the controller has an establishment or a court where the data subject has its habitual residence. A lawsuit in the matter of data protection breach shall comply with formal requirements, including a court fee in the amount of 600,00 PLN (133 EUR).[400] Compared to other court fees, that one is considerably low. Referring to the doctrine and jurisprudence, the high of court fees might be a significant obstacle in exercising the rights to a fair trial granted in article 45 of the Constitution and article 6 section 1 of the European Convention on Human Rights.[401]

The court is bound by the former decision of the President of the Office. Thus evidence hearing will be shorter if the decision stated data protection breach. Moreover, if the President of the Office did not constitute a breach, in a matter of damage caused by (possible) data protection infringement, the court is entitled to state otherwise. To conclude, only breach-constituting decisions are binding. Due to the principle of

[397] Articles 37 and 39 of General Data Protection Regulation; Article 8 of the Act of 10 May 2018 on personal data protection.
[398] Article 29 Working Party Guidance on data protection officers issued on December 2016 and revised April 2017.
[399] Announcement of the Minister of Justice of 15 February 2016 on list of entities subordinated or supervised by the Minister of Justice.
[400] Article 26 of the Act of 28 July 2005 on Court Fees in Civil Cases.
[401] Wesołek v. Poland, ECHR Judgement 13 June 2019, application no. 65860/12, Paweł Grzegorczyk, Karol Weitz [in:] Leszek Bosek, Marek Safjan, Konstytucja RP. Tom I. Komentarz do art. 1–86, CH Beck 2016.

two-instance proceeding, each of the parties is allowed to file an application to the higher instance (appeals court), eventually in the Supreme Court.[402]

5.5. Remedies in administrative proceeding

GDPR in recital 129 recommends that "legally binding measure of the supervisory authority should be in writing, be clear and unambiguous(…)give the reasons for the measure, and refer to the right of an effective remedy." The purpose of the proceeding conducted by the supervisory authority is to restore legal status. The President of the Office shall choose the remedy which intrusiveness is the most proportional to the breach and the abovementioned purpose. The most common are the 'soft' ones such as a reminder, a warning, an order to notify the subject of a breach of his personal data or an order to limit data processing. Undoubtedly, the most intrusive remedy is an administrative financial penalty, which may be imposed separately or cumulative with other measures.[403]

It is to emphasize that, among remedies which are available for the supervisory authority, it lacks the compensation for the suffered subject from the administrator or processor, pursuant to Art. 82 GDPR. The right to compensation and the liability of the administrator or processor are the matter of the court proceeding, which will be specified below.

The amount of a financial penalty differs in the public and private sector. The first one, regulated on the national level, amounts to 100.000,00 PLN (22.181 Euros).[404] Thus public authorities are also strongly supported in the protection of data. The Polish private sector applies GDPR provisions.[405] The amount of the maximal penalty as well as the short payment deadline (14 days) undoubtedly fulfil a deterrent effect and compel indirectly to comply with data protection regulations. In some cases, it is questioned if the penalty was appropriate and proportional to the breach. An example of that may be the decision of the President of the Office from 18 February 2020,[406] which stated that processing of biometric data (by such ADT as fingerprints reader) of 680 pupils to distribute lunches on primary school's mensa was against the data protection law. Although the school violated the ban of processing special categories of data as well the fact that affected persons were children and those pupils, whose parents did not allow to process biometric data, were discriminated against, the President of the Office decided to order a penalty in the low amount of 20.000 PLN (4.430 EUR). In this case, the administrator has received the financial penalty because of the unlawful processing of personal, sensitive data. It is also an

[402] Articles 367 § 1 and 431 § 1 of the Polish Code of Civil Procedure.
[403] Article 83 s.2 of the General Data Protection Regulation; Article 101 of the Act of 10 May 2018 on personal data protection.
[404] Paweł Litwiński, Ustawa o ochronie danych osobowych. Komentarz, CH Beck 2018.
[405] Article 83 of General Data Protection Regulation
[406] Decision of the President of the Office of Personal Data Protection of 18 February 2020, no. ZSZZS.440.768.2018.

example of an administrator who did not succeed in ensuring data protection despite having the DPO as a public entity.

The largest financial penalty so far imposed by the President of the Office has been 2.830.410 PLN (660.000 EUR), which has been addressed to a hosting platform. The data protection breach was caused by a phishing attack resulting from a lack of appropriate security measures.[407] The President of the Office addressed the penalty to the administrator, although the purpose of data processing was legal, as well as the breach of data protection was caused by someone else.

Besides measures specified in the decision, the President of the Office may order during the proceeding to limit temporary data processing if otherwise, it would cause a severe and difficult to remove effect.[408] This measure shall be assumed as positive as it ensures more efficient data protection even if a decision in that matter has not been taken yet.

5.6. Remedies in civil proceedings

Measures provided in administrative proceedings may be effective in the matters of data protection but do not guarantee protection for affected persons. In case of material or non-material damage caused by data protection breach, they may require legal protection through judicial procedure. The appropriate measures are compensation and reparation. In case of compensation, the complainant chooses either to restore to the legal status or monetary compensation. If restoration is not possible or would cause severe difficulties for the defendant, only monetary compensation is possible.[409] Estimates of non-material damage due to personal data breaches (e.g. data leakage) may meet difficulties. It is to highlight that non-material damage is not defined in the GDPR. However, the Court of Justice of the European Union has recently been asked to rule on when non-material damage is severe enough to justify a claim under Art.82 GDPR. In the Polish legal system, non-material damage is called 'harm' and means mental suffering caused by the actions of another person. Reparation aims to alleviate this pain[410] and belongs to measures provided in matters of personal rights mentioned in Question no.2.

5.7. Complementary remedies in criminal procedure

There are also specific remedies in criminal procedure, according to data protection breaches. According to Article 84 section 1 and recital 149 of GDPR, Poland also provides criminal sanctions in articles 107 and 108 of the Act. Unlawful processing or ones without authorisation, as well as sabotage of investigation, may face such punishments as fines, restriction of freedom or imprisonment to two years. Punishments are provided only to

[407] Decision of the President of the Office of Personal Data Protection of 10 September 2019, no. ZSPR.421.2.2019.
[408] Article 7 s.1 of the Act of 10 May 2018 on personal data protection.
[409] Zbigniew Radwański, Adam Olejniczak, *Zobowiązania-część ogólna*, CH Beck 2018, sites 101-109; Article 415 of the Polish Civil Code.
[410] ibid, Article 415.

natural persons, which means that employees of the controller or processor might be sentenced.[411] To the proceeding apply the Polish Criminal Code and the Code of Criminal Procedure.[412] According to GDPR recitals, one of the sanctions might be the deprivation of the profits obtained through infringement. Polish criminal law provides such measures in article 44 and following of the Criminal Code. Compared to the polish provisions in force before 25 May 2018, the range of criminalisation of data protection has been reduced.[413] The abovementioned crimes are prosecuted *ex officio,* which shall be assessed positively. They belong to intentional crimes, which at the first sight may weaken the effectiveness of data protection, because unwilling data breaches may cause negative consequences as well.[414] Nevertheless, the necessity of extended criminalisation in matters is questioned, as it does not achieve purposes of data protection. Criminal remedies shall be provided only for the most severe breaches and play complementary roles to administrative and civil measures.[415]

To conclude, provisions in the Polish legal system indeed provide institutional safeguards (however, the support of DPOs is not considered completely) and various remedies to ensure effective data protection. The question is, which result is more preferable for a data subject. The financial penalty (especially the largest amounts) has a deterrent function and the temporary order of limiting data processing ensures data protection. If more expected is to impose a financial penalty or restore the legal status than satisfy the affected data subjects, then an administrative procedure shall be more appropriate. However, the amount of complaints and investigations conducted by the President of the Office per year slows down its activity. Additionally, the procedure does not include the affected person and its damage. Compensation and reparation from a particular controller may be ordered only in case of judicial review, which leads to more than one proceeding in the matter of data protection breach. Criminal sanctions are complementary to administrative and civil measures.

It is worth to mention that each decision taken by the President of the Office, as well as its informative and educational activities, lead to increased awareness of the importance of data protection among administrators, controllers and data subjects. The review mentioned in the Question is on the right track to the effective protection of personal data.

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

6.1 Admission

[411] Arkadiusz Lach, *Problem kryminalizacji naruszenia przepisów rozporządzenia ogólnego w sprawie ochrony danych osobowych,* MOP 2017, no. 22, site 1191.
[412] Official Journal of Laws Dz.U.2020, position 1444; Official Journal of Laws Dz.U. 2020, position 30.
[413] Malgorzata Zimna *Odpowiedzialność karna za naruszenie ochrony danych osobowych*, Prokuratura i Prawo 2020/ no.1/site 57.
[414] ibid
[415] ibid

In Poland, anti-discrimination cases are frequently resolved within the scope workplace, unit in which they occur, and each unit has its forms of dispute resolution, i.e. anti-discrimination regulations, good codes practices, special offices for anti-discrimination matters. In case of inability to resolve the dispute within the entity, we turn to the court. There are several ways to choose from, including civil action for compensation for discrimination on the basis of the so-called regulation on anti-discrimination, mediation proceedings, conciliation, civil action for infringement of personal rights, criminal proceedings. Particularly noteworthy is the attitude of the academic community associated with innovations. There is a trend among universities in Poland on the popularization of this issue. There have recently arisen special regulations proceeding sin cases of anti-discrimination at the University of Warsaw.[416] At many universities, there are rectors' plenipotentiaries for discrimination. This practice has also been developing among technical universities implementing projects in the field of artificial intelligence, robotics and widely understood new technologies.[417, 418, 419]

In Poland, there are many acts concerning the legal rights of anti-discrimination, in which legal norms of this nature appear.

- the Act of 3 December 2010 on the implementation of certain provisions of the European Union in terms of equal treatment, the so-called anti-discrimination act
- the Act of 26 June 1974 - Labour Code
- the Act of 20 April 2004 on promotion of employment and on labour market institutions
- the Act of 23 April 1964 - Civil Code
- the Act of 6 June 1997 - Penal Code
- the Act of 20 May 1971 - Code of Petty Offenses
- the Act of 19 August 2011 on sign language and other measures of communicating
- the Act of 24 April 2003 on public benefit activity and volunteering
- the Act of 23 May 1991 on Trade Unions

In terms of court procedures, the law procedural in specific areas is worth familiarizing with. In the context of the development of this branch of law in Poland, the Polish law society is very active in anti-discrimination.

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

In Poland, the anti-discrimination procedure is not specified on the judicial level. Everything is settled in terms of civil proceedings or criminal cases. Some cases are

[416] Zarządzenie Rektora UW w sprawie Procedury antydyskryminacyjnej na Uniwersytecie Warszawskim z dnia 31 sierpnia 2020 roku.
[417] Zarządzenie nr 176/2020 Rektora Politechniki Warszawskiej z dnia 22 grudnia 2020 r. w sprawie przeciwdziałania mobbingowi i dyskryminacji w Politechnice Warszawskiej.
[418] Zarządzenie nr 50/2019 Rektora Politechniki Łódzkiej z dnia 23 września 2019 w sprawie wprowadzenia regulaminu praktyk antydyskryminacyjnych w Politechnice Łódzkiej.
[419] Zarządzenia nr 4 Rektora Uniwersytetu w Białymstoku z dnia 9 kwietnia 2014 r. w sprawie wewnętrznej polityki antymobbingowej.

brought to administrative courts or Local Government Boards of Appeal when, for example, an administrative decision causes unequal treatment. However, in the so-called anti-discrimination act, there are two detailed bodies dealing with this subject. That is the Ombudsman and Government Plenipotentiary for Equal Treatment. However, only and exclusively. The Ombudsman is an independent body in the performance of its tasks from the so-called anti-discrimination law. Ombudsman, in the context of the political system, is defined as the supreme body, at the highest level of the state organization, functioning as an independent body. It is independent of the executive and judiciary over which it is not entitled to any means to direct its activities.[420]

Within the framework of the previously mentioned procedures, it is possible to appeal to a higher court or a cassation appeal to the Supreme Court. These non-governmental organizations may participate in the proceedings.

6.3 Which bodies conduct such review?

As a rule, higher courts, i.e. the Court of Appeal or the Supreme Court for criminal or civil discrimination cases. Whereas in the case of discrimination in administration it is the Provincial Administrative Court and Supreme Administrative Court. These are adjudicative bodies. In exceptional circumstances, it is the Constitutional Court which upon request made by The Ombudsman for Citizens' Rights interprets the law provided that the provisions introduced by the legislator are discriminatory and inconsistent with Art. 32 Constitution of the Republic of Poland.[421] In ordinary cases of a civil nature, inspections are carried out by the court of second instance as above, and as the last resort by the Supreme Court, which can cancel previously issued sentences and order a new consideration of the case.

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

The Polish system adopted a full appeal system with certain limitations. The appeal procedure is of a verification and control nature, but it also retains an examination nature - the court of second instance has full jurisdictional freedom limited only by the limits of the appeal. The appeal court is not only entitled but obliged to reconsider all the collected material and make a proper legal assessment of it and in case of noticing errors to repair the violations found. The court of second instance may omit new facts and evidence if the party could invoke them in court proceedings first instance unless the need arose afterwards. Court of the second instance adjudicates on the basis of the material collected in the proceedings in first instance and on the appeal. The main elements that are taken into account by the court are violations of substantive law in the course of trial or

[420] A. Gajda, Directions of development of the institution of the Human Rights Defender in Poland, Warsaw 2013, p. 86.
[421] Tuleja Piotr (red.), Konstytucja Rzeczypospolitej Polskiej. Komentarz.

procedural errors. Importantly, errors and violations must have a significant impact on the edition decision so that the decision can be changed.[422]

6.5 Does the review constitute effective protection against discrimination?

As a rule, yes,[423] although the awareness of Polish people has assessed citizens very low as to situations in which they are legally protected against discrimination. The situation is slightly better when they understand when they are dealing with discrimination, although it is very difficult for the majority of Polish citizens to indicate a specific legal situation in which they have the possibility of legal protection and asserting their rights. On the other hand, as a result of misunderstanding and too low level of education in this matter there are cases in which a natural person claims to be discriminated against while under the law and objective assessment of the court in a given case there has been no discrimination.

6.6 What is a considered role of the technical aspects that result in discrimination (such as algorithmic bias)?

This is a relatively new topic in Poland. One of the latest topics that concern the issue of discrimination in state pensions was raised by a certain group of citizens. Although the current jurisprudence suggests that algorithms included in legal acts created by the legislator are usually equal and meet the constitutional norms resulting from Art. 32 constitutions as of EU legislation.[424]

6.7 How are these problems tackled?

Cases in this area are usually settled in favour of the employee. One of the most well-known cases of last year was a trial between a former employee and Amazon - using a special motivational algorithm. Finally, to the employee's advantage, the Court found the algorithm unlawful.[425]

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?

Currently, in Poland, there exists an area of law dedicated to the new technologies, called the new technologies law, which can be defined as "a set of legal norms that relate to the areas of necessary adjustment, in the sphere of relations of both public and private nature,

[422] Manowska Malgorzata (red.), Kodeks postępowania cywilnego. Komentarz. Tom I. Art. 1-477(16), wyd. IV

[423] "right anti-discriminatory in practice of Polish common courts " Monitoring report edited by Monika Wieczorek and Katarzyna Bogatko, 2013, Polish Anti-Discrimination Society p. 20

[424] (III AUa 870/18 - judgment of the Court of Appeal in Warsaw with
30 July 2020).

[425] "Amazon przegrał w sądzie z byłym pracownikiem. Chodzi o system oceniania" M.Adamski, Rzeczpospolita dostęp 26 February 2020.

directly influenced by new technologies."[426] The law of new technologies comprises of, inter alia, personal data protection law, copyright and related rights law, industrial property law, e-commerce law, consumer law, competition law, data and cyber law. This field includes a wide range of other fields of law in which regulations can affect the protection of certain rights in connection to the newly emerging technologies. Thus, there are no specific acts that cover the new technologies, including advanced digital technologies, such as big data, artificial intelligence, Internet of Things and encryption by the means of regulations distinctly and directly targeting them. Notwithstanding, Polish law tackles given subjects through vertical regulations in several legal acts.[427] The following short analysis aims to provide a few examples of such vertical regulations in relation to big data, artificial intelligence, the Internet of Things and encryption as mentioned in the question in the subject.

What is necessary to be mentioned is that Poland is a part of the European Union and consequently falls under the EU law directly. Hence, in some parts of the below analysis this fact is more or less underlined. However, this section focuses on answering the question of whether Poland has its own specific regulations regarding Advanced Digital Technologies.

7.1. Big data

In the Polish legal system, there is no legal definition of big data and special regulation dedicated to such.

7.1.1. Big data as an infringer of rights.

Poland, as a member of the European Union, implemented General Data Protection Regulation (GDPR).[428] Regarding GDPR in relation to big data, we can talk about Article 6 (1) GDPR and the processing of the data under certain circumstances. If it concerns big data, we may take into consideration only 4 out of 6 subpoints:[429]
"(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

[426] Chałubińska-Jentkiewicz K., Karpiuk M. "Prawo nowych technologii. Zagadnienia Wybrane.", Wolters Kluwer, 2015, p.21.
[427]<https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/Internet-Rzeczy-ochrona-prywatnosci-a-bezpieczenstwo-danych.html> accessed 21 February 2021.
[428] 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.
[429]<https://www.twobirds.com/pl/news/articles/2019/poland/190611-przetwarzanie-danych-osobowych-w-kontekscie-big-data> accessed 25 February 2021.

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[430]
In accordance with GDPR's data protection impact assessment, big data could also be subject to Article 35 (1) GDPR, which mentions direct new technologies, as well as Articles 35 (3), 35 (4) and 35 (5).[431]

We can also talk about big data in the context of telecommunication law. Poland has its Telecommunication law Act from 16 July 2004, implementing a number of European Union directives. It is worth taking a look at Article 173[432] which says that "storing information or accessing information already stored in the telecommunication final devices of the subscriber or end-user is allowed, inter alia, only if person is directly informed in an imbigenous and understandable manner about the purpose of storing and accessing this information, as well as about the possibility of defining the conditions of storing accessing the information through the settings of software installed in the telecommunication device or service configuration."[433]

7.1.2. Big data as the subject of protection.

When talking about big data as the subject of protection, what could be taken into consideration is the protection under the copyright law or in the context of sui generis as the data sets or databases.[434] The database created as a result of using big data technology could be recognised as the 'work' on the basis of Polish copyright law.[435][436] In Poland, there also exists the Protection of Databases Act from 27 July 2001[437] and big data could be attached under the protection of the databases, which gives them special protection under the copyright law, however, it is not common practice.[438]

7.2. Artificial Intelligence

---

[430] GDPR, Article 6 (1).
[431]<https://www.twobirds.com/pl/news/articles/2019/poland/190611-przetwarzanie-danych-osobowych-w-kontekscie-big-data> accessed 25 February 2021.
[432]<https://interaktywnie.com/biznes/newsy/biznes/wykorzystanie-big-data-a-prawo-o-tym-trzeba-pamietac-255981> accessed 25 February 2021.
[433] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. 2004 nr 171 poz. 1800) (Act of 16 July 2004 on telecommunication law).
[434]<https://bartakalinski.pl/artykuly/big-data-cz-i-big-data-a-prawo-autorskie-i-ochrona-sui-generis-baz-danych/> accessed 25 February 2021.
[435] See Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24 poz. 83) (Polish Copyright and Related Rights Act).
[436]<https://itwiz.pl/analizy-big-data-wlasnosc-intelektualna/> accessed 25 February 2021.
[437] Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. z 2019 r. poz. 2134). (Polish Protection of databases Act).
[438]<https://www.twobirds.com/pl/news/articles/2019/poland/190611-przetwarzanie-danych-osobowych-w-kontekscie-big-data> accessed 25 February 2021.

In the Polish legal system, the legal definition of Artificial Intelligence (AI) does not exist.[439] Thus, Poland has not developed its own regulation tackling the topic of AI directly. However, we could talk about Artificial Intelligence in the context of intellectual property law. AI itself could be protected as 'work' in the light of the Polish Copyright and Related Rights Act. Besides that, the relevance of the GDPR (as the act implemented into the Polish legal system) in relation to AI in the light of intellectual property could be mentioned. For example, Article 25 GDPR. The relation of Article 25 GDPR and AI, is that "the essence of the privacy by design is the obligation of the controller to include the protection of the personal data already in the design phase of the specific solution, service or system based on the AI."[440]

7.2.1. For the future of AI in Poland.

Polish Ministry of Digitalization in 2018 created a document called 'Assumption for the AI strategy in Poland. Action plan of Ministry of Digitalization'. The document sets goals that should be achieved by the governmental administration, which are: ensuring effective protection of fundamental rights, effective acquisition of knowledge about the social effects of AI, setting ethical standards for AI, supporting high-quality legislation to regulate the areas where AI could be used.[441] The document underlines the conclusion of the expert group which analysed selected legal issues. The conclusion states that the country should focus on such aspects as: "ensuring the protection of human rights, ensuring wide access to data in full compliance with the data protection rules, as well as protection of consumers rights in connection to use of AI, defining the rules and conditions for the use of AI in process of concluding contracts, considering introducing the support system for the people who will lose their job due to implementation of AI."[442]

The governmental administration decided to create another document entitled 'Policy of Development of Artificial Intelligence in Poland for the year 2019-2027' which was introduced as a project for public consultations. In the document, it is underlined that the creation of legal definition is at the most important, especially to be able to set the rules for liability of the damages caused by AI and in the context of intellectual property of the works created by the AI.

Poland is in favour of the technical definition. Moreover, the country stands on the position that AI shall not have a legal personality, as well as the meaning of AI in the field of intellectual property law should be divided on the AI in narrow meaning (as softwares, hardwares) and AI in large meaning (as works created using this programmes), when the IP rights are in question.[443] In the text, it is also mentioned that in the issue concerning

[439]<https://fintek.pl/aspekty-prawne-w-polskiej-polityce-rozwoju-sztucznej-inteligencji/> accessed 25 February 2021.
[440] Lubasz, D., Chomiczewski, W., "Privacy by design a sztuczna inteligencja", Monitor Prawniczy 20/2020, 9.
[441] "Założenia do strategii AI w Polsce. Plan działania Ministerstwa Cyfryzacji.", Warsaw, 9 November 2018, 120.
[442] ibid, 120-121.
[443] "Polityka Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027",Warsaw, 20 August 2019, p.42-43.

liability for damages caused by the AI there should be introduced a compromise which could be "introducing an adequate liability for product liability or introducing a separate liability regime for damages caused as a result of activities of artificial intelligence."[444] The government also proposes rules for public administration in regards to financing the development of AI by grants, help for start-ups, or any other public/governmental programmes, as well as setting some standards in regards to norms, certification and data administration.[445]

7.3. Internet of Things

In the Polish legal system, there is no legal act that covers Internet of Things technology in any specific regulation on that matter. Notwithstanding, the Polish law tackles the Internet of Things subject (it is not mentioned directly) through vertical regulations in multiple legal acts.[446] Those legal acts concern the legislation in the fields of cybersecurity, data protection and privacy, civil law and liability for damages, and intellectual property law.[447]

7.3.1. Cybersecurity legislation

Main legal acts:

- Act of 5 July 2018 on the national cyber security system (ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa)
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

7.3.2. Data protection and privacy

- 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)

7.3.3. Civil law and liability for damages

- Polish Civil Code (Ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny), Article 449^1 (the liability caused by the product)

7.3.4. Intellectual property law

- Polish Copyright and Related Rights Act (Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych) - the question from the perspective of the buyer

[444] ibid, 44.
[445] ibid, 45.
[446] <https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/Internet-Rzeczy-ochrona-prywatnosci-a-bezpieczenstwo-danych.html> accessed 25 February 2021.
[447] <https://digitalandmore.pl/iot-regulacjeprawne/> accessed 25 February 2021.

of IoT device, especially computer programs installed in these devices and the right to use those programs as well as the possibility to dispose of such device, but also the issue of making it available for use by third parties.[448]

7.4 Encryption

In Poland, there is no special regulation dedicated to encryption.

Poland as a part of the European Union was obliged to incorporate the GDPR into its legal system. The encryption requirement is based on the GDPR. According to article 30 GDPR "the record of processing activities shall contain where possible, a general description of the technical and organisational security measures referred to in Article 32(1)."[449] Following that, according to Article 32 GDPR, encryption is one of the good ways to achieve an appropriate level of security of protection of certain data.[450]

Another legal act of the EU, which Poland was obliged to incorporate into its national legislation, is the 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). As the NIS Directive is an example of the act, which ensures the minimum harmonisation within the EU, Poland transposed it through several acts:

- Act of 5 July 2018 on the national cybersecurity system,
- Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and thresholds for the materiality of incident's disruptive effect for the provision of key services (Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych),
- Regulation of the Council of Ministers of 31 October 2018 on the thresholds for considering an incident as serious (Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny),
- Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland 2019-2024 (Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024).

Article 14 (1) of the NIS Directive states the security requirements for the operators of essential services. In this regard, the Polish legislator in the Act of 5 July 2018 on the national cybersecurity system sets the obligations on the operators of essential services (OES) in its Article 8 "to implement safety management system in the information system, which has to provide"[451] inter alia: "implementation of technical and organizational

[448]<https://digitalandmore.pl/iot-regulacjeprawne/> accessed 25 February 2021.
[449] GDPR, art.30 (1)(g).
[450] ibid art.31 (1)(a).
[451] Act of 5 July 2018 on the national cybersecurity system, Article 8.

measures appropriate and proportional to the assessed risk",[452] "use of mechanisms ensuring confidentiality, integrity, availability and authenticity of the data processed in the information system."[453] The legislation does not mention the exact security systems leaving the margin of interpretation to the OES.

The Polish legislator is not able to approach the development of new advanced digital technologies on their own.[454] The Polish legal system is not modernized enough to accommodate the digital transformation of technology. Taking small steps toward modernization (e.g. documents discussing the AI issue), it can be noticed that the country prefers and relies mainly on the development of European legislation in regards to regulation of new technologies.

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

8.1. Access to personal messages.

As mentioned earlier, there are no regulations in Polish law relating to the 'encryption' of data. However, there are provisions in the Polish legal order that regulate the admissibility of inspection and recording of conversations by services for the purposes of criminal proceedings. According to Article 237 of the Code of Criminal Procedure, the court after the initiation of proceedings may, at the request of the prosecutor, order the inspection and recording of the contents of telephone conversations to detect and obtain evidence for the ongoing proceedings or to prevent the commission of a new crime. The inspection is only permissible for strictly defined offences in the law, which include inter alia murder, exposure to general danger or bringing about a catastrophe, abduction of a person etc.

Control of correspondence and telephone conversations shall be admissible with respect to the suspect, the accused and the victim or any other person with whom the accused may have contact or who may have a connection with the perpetrator or the threatening crime. Evidence obtained as a result of such control shall be subject to use in proceedings upon the decision of a prosecutor. Article 237a, however, leaves no doubt that evidence obtained in violation of the law will not be admissible in the proceedings and shall be destroyed.[455]

Article 240 of the Code of Criminal Procedure also allows the person subject to the inspection to file a complaint against the court's decision in which they may demand that the legality and legitimacy of the inspection are investigated. Importantly, they can also demand the destruction and deletion of records of correspondence and other evidence at

[452] ibid, art 8 (2).
[453] ibid, art 8 (5)(a).
[454] prof. ALK dr hab. Przemysław Polański, "Inwigilacja, dostępność, blockchain i sztuczna inteligencja: pytania o kierunki rozwoju prawa nowych technologii w erze rewolucji internetowej", Monitor Prawniczy MOP 2019, Nr 2, s.110.
[455] Kala Dariusz (red.), Zgoliński Igor (red.), Postępowanie przed sądem I instancji w znowelizowanym procesie karnym; Opublikowano: WKP 2018.

the end of pre-trial proceedings if the inspection of the conversations did not provide any evidence of a crime at all.[456]

In conclusion, while in certain cases the law allows for inspection and access to Internet correspondence for the purposes of an investigation, there are no detailed regulations concerning the obligation of services to decrypt and allow access to messages and correspondence. In particular, there are no legal regulations that would impose such obligation on telecommunication providers or other entities such as the police, etc.

Regarding these issues, it is also worth mentioning the so-called Surveillance Act which, although it does not contain regulations relating to downloading or decrypting telecommunication data, gives the services broad powers to remotely search devices and media with the consent of the court. In the regulations on the police or the Internal Security Agency and the Intelligence Agency, there are no provisions that would oblige the services to inform a person about activities related to inspection or to submit requests to service providers for access to electronic correspondence.

There is no doubt that operational control is used by secret services around the world. In particular, the possibility of the services gaining access to increasingly sophisticated surveillance tools, which combined with the vague provisions on operational control pose the risk of too far-reaching surveillance, raises concerns. At risk are also freedom of speech, the right to privacy, and even freedom of assembly - values which protection is fundamental in a democratic society.

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

9.1 Protection of human rights online

There is no exception to validating human rights in cyberspace. According to the statements presented in the Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users,[457] every Internet user has "a legitimate expectation that its services are accessible, provided without discrimination, affordable, secure, reliable and ongoing. Furthermore, no one should be subjected to unlawful, unnecessary or disproportionate interference with the exercise of their human rights and fundamental freedoms when using the Internet."

Thus, Poland as a member of the Council of Europe is obliged to ensure human rights protection in the context of Internet use. Furthermore, human rights guarantees are included in the abovementioned acts such as the Constitution or GDPR.

[456] Kardas Piotr (red.), Sroka Tomasz (red.), Wróbel Włodzimierz (red.), Państwo prawa i prawo karne. Księga jubileuszowa Profesora Andrzeja Zolla, tom II; Opublikowano: WKP 2012.
[457] Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies.

This part of the report presents selected cases concerning human rights applicable online in Poland, which may be an interesting illustration of the condition of human rights protection in times of new technologies development.

It should be borne in mind that new technologies affect human rights in the offline sphere both positively and negatively. An example of various threads caused by the use of advanced technology may be audio-video monitoring, omnipresent in public (but also in private) space, although an average citizen is clueless about how and by whom their data is processed.[458]

9.2. The right to access to the Internet and the right to the public information

Undoubtedly, one of the human rights strongly bound to cyberspace is the right to participate in it. More than 86% of households in Poland had Internet access in 2019.[459] It may seem obvious that there is access to the network, especially among younger people. However, the legal system still lacks regulation on that right, that is why it shall be derived from the Constitution and other acts. Article 61 of the Constitution sets out the right to be informed about activities of public authorities, which is broadened in Act of 6 September 2001 on access to public information (Act of access).[460] Pursuant to Art. 8 of the Act of access, public information is published in the ICT system of the Public Information Bulletin (BIP). To public information belong information about the functioning of data authorities, competencies of the officers, bills and acts, public property.

To ensure access to public information, connection to the global network shall be guaranteed. However, it does not indicate free access to any citizens' claim against the state to connect them to the Internet in every household. Nevertheless, public authorities shall take steps to develop appropriate technical infrastructure to allow uninterrupted and instant connection to public information.

9.3. The right to privacy online

Pursuant to many international provisions as well as to Art. 47 of the Constitution, every person has the right to privacy. Despite such detailed regulation of that matter, it remains one of the biggest threats to human rights violations online. It needs to be noted that advanced technology to efficiently achieve purposes may require lower privacy protection. A significant example is the worldwide use of cross-tracking applications to observe the spread of the SarsCoV-2 virus among society. The Polish government has provided an application regarding the cross-tracking of citizens and collecting their data - ProteGO Safe. After heavy criticism regarding the first version, it is now recognized as safe in the matter of processing data; it does not collect data on geolocalisation, provides encryption

[458]<https://panoptykon.org/monitoring-wizyjny>, access 15/03/2021, Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego, Czerwiec 2018.
[459] *Społeczeństwo informacyjne w Polsce w 2019 r.,* Główny Urząd Statystyczny 2020
[460] Journal of Laws 2001 No. 112 item 1198 as amended.

of transmitting data and processes it only on the device of the user.[461] Despite the large and expensive information campaign, as well as consultations with experts to improve privacy protection, ProteGO has not met expectations and does not ensure effective monitoring of social contacts during the pandemic. The reason for that is the growing distrust of the citizens to share data with the Polish government. What shall be noted is the worldwide suspicion concerning tracking systems used by governments to monitor virus spread – and in the opinion of many people – to surveillance society during and after the pandemic. Polish people are no exception in that case. The situation is aggravated by the fact that not just states provide official tracing technology but also private global firms such as Apple or Google. For some reason, that makes people even more worried about their privacy. According to MIT's Covid Tracking Tracker, governments' applications vary with the level of transparency, data minimalisation and obligation of use. The Polish ProteGO Safe's latest version is described as 'more secure' than the first strongly criticised version.[462]

It should be noted that the right to privacy may also be limited by operational and investigative activities of the secret service and police, which use various new technologies to receive information and evidence. Such unexpected surveillance meets the objections of society. On the other hand, new technologies allowing wiretapping, correspondence control and tracking are necessary to fight crime and terrorism and need to be justified as a key to ensuring state and public security. Nevertheless, the main threat and doubt regarding that matter is the scope of surveillance. It should be highlighted that not just the 'object of observation' is under surveillance but every person around it. The problem of surveillance is generally conducted by the Polish secret services and policy is examined by the European Court of Human Rights. Non-government organisations and the Polish Ombudsman have signalised through the years that the Act of 10 June 2016 on anti-terrorist activities[463] and the Act of 6 April 1990 on the Police[464] provide extensive surveillance measures without appropriate control. Another controversial issue is – officially unconfirmed by the government - Pegasus, an advanced spy system that supposedly has been bought by one of the secret services in order to fight terrorism. The purchase of Pegasus has been noticed by a Canadian research group yet only a few Polish politicians informed about it. What is interesting about this spy system is it is almost undetectable. It can be installed wirelessly on any electronic device and gets free access to the camera, microphone, files, contacts, and activity on the Internet. Eventually, it removes itself from the device, leaving no trace behind. Despite politicians' statements that Pegasus is in fact no mass surveillance system, information about such control measures has electrised society because there is no evidence of the fact that one has been under such

[461]<https://panoptykon.org/czy-instalowac-protego-safe> accessed 25 February 2021, <https://www.gov.pl/web/protegosafe> accessed 25 February 2021.
[462] MIT Technology Review, <https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/>, accessed accessed 5 February 2021.
[463] Journal of Law Dz.U. 2016 poz. 904.
[464] Journal of Law Dz.U.2020.360 t.j.

detailed surveillance. The issue has been examined by the Polish Ombudsman with a group of experts.[465]

The necessity of using efficient measures, including advanced technology, by secret services in order to fight crimes and terrorism and improve the protection of the state and its citizens, should be emphasised. Nevertheless, the security conditions shall not lessen the importance of the right to privacy and other human rights ensured in the Constitution and international provisions. It always has to be a compromise between these principles.

9.4. The omnipresence of new technologies and question of equal access

Polish public authorities see the necessity of applying new technologies into daily life. Undoubtedly, such tools as digitisation of justice and administrative matters, electronic evidence in proceedings positively influence ensuring the effective relationship between the state and its citizens. On the other hand, in some cases, the desire to develop diminishes the human right to equal treatment. Once again, it occurs clearly during the struggle with the Covid-19 pandemic, which demands effective, transparent and affordable tools to provide information and collect data on patients, infected, cured, convalescents and willing to vaccine.[466] However, not every citizen, especially the elderly, has digital skills to fulfil the online form and use an e-mail box or at least someone on their side who could help them in that matter. Notwithstanding, the Polish government has assumed that in the era of new technologies every citizen has the appropriate electronic devices, digital knowledge of using them, the abovementioned access to the Internet. Because of the same assumptions, the tracking system for smartphones has been provided as well as the model of remote school education through internet platforms. International organisations such as UNICEF in Poland highlight that states shall provide infrastructure for organizing remote education and counteracting the phenomenon of digital exclusion of children and teachers.[467] The shortage of equipment and Internet access is felt by the poorest families, more often in the countryside than in the city.[468] It should be noted that many duties and activities are required from people that in many cases cannot afford them because of increasing digital inequality or even of digital discrimination in the matter of access to education, health services, information.

9.5. Conclusion

That said, Poland has not reached an appropriate balance between using new technologies and ensuring human rights protection online yet. Uncontrolled activities of the special services in order to secure the state and its citizens raise doubts about the bounds of mass

[465] *How to saddle Pegasus*, Commissioner for Human Rights's Bureau, 2019, <https://www.rpo.gov.pl/sites/default/files/HOW%20TO%20SADDLE%20PEGASUS%20%28OSIOD%C5%81A%C4%86%20PEGAZA%29.pdf> accessed 25 February 2021.
[466]< https://www.gov.pl/web/szczepimysie/zgloszenia> accessed 25 February 2021.
[467]<https://unicef.pl/co-robimy/aktualnosci/dla-mediow/edukacja-zdalna-w-czasie-pandemii> accessed 25 February 2021.
[468] M. Zaporska, Sukces czy porażka zdalnego nauczania? Forum Idei Fundacja Batorego, 2020

surveillance. The Covid-19 pandemic challenges Poland, like every other country with the issue of compromising sufficiency, transparency and equality of taken activities.

At the same time, Polish law does not succeed in following the rapid development of new technology.[469] Significantly, general matters of human rights protection in cyberspace, mass surveillance, specific advanced digital technologies, data protection are regulated (or at least planned to be) at the EU level and Poland as a Member State takes steps only to implement them.It is to strongly emphasize the specific nature and broad scope of GDPR, which is applicable in every matter related to personal data, including advanced digital technology issues. Additionally, the abovementioned new technologies injustice and administrative proceedings, as well as other sectors, still require appropriate legal amendments and human rights safeguards to meet the efficiency.

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. The importance of regulation

What is law and why do we need it? That is one of the most substantial questions of society and certainly one of the most difficult ones. Humans did not manage to agree upon a certain, common, clear definition of the law. However, we can describe the system of legal norms at least by specifying what it does and what it provides to society.
To loosely translate the description of the legal norms system provided by one of the greatest Polish lawyers Zygmunt Ziembiński "The system of legal norms is characterized as an orderly set of general norms ordering or prohibiting a certain behaviour either directly or by granting certain entities legislative powers."[470]

The main task of law is to regulate - to tell certain individuals what one can and what one cannot do and to connect such regulations with the authority of The State in order to assure citizens that they will always be provided, alongside other things, with justice as said in the preamble of The Constitution of the Republic of Poland established "as the basic law for the State, based on respect for freedom and justice."[471]

The task of providing individuals with justice lies in the hands of separate power, independent of other branches of power - the Supreme Court, the common courts, administrative courts and military courts.[472]

10.1.1. The fight of judicature against the lack of comprehensive regulation

[469] prof. ALK dr hab. Przemysław Polański, Monitor Prawniczy MOP 2019, Nr 2, s.110
[470] "TWORZENIE A STANOWIENIE I STOSOWANIE PRAWA", ZYGMUNT ZIEMBIŃSKI, in RUCH PRAWNICZY, EKONOMICZNY I SOCJOLOGICZNY Rok LV — zeszyt 4, (1993 r.).
[471] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.).
[472] ibid, art. 175

Ensuring justice is no easy task. Every filed case has to be ended with a final judgment and that judgment has to be based on applicable provisions of law.

The process of application of the law is a complex task. One of the most important steps everyone that applies the law has to start with is finding the right norms that regulate the considered singular legal situation of a certain legal entity. That is why good, well-versed, thoughtfully established legal norms can vastly improve the process of applying the law and in consequence, ensure that every entity is treated in the same way.

Every field of life is regulated by the law and every norm in the legal system is derived from a norm established in the Constitution since, as it is written in the Constitution itself "The Constitution shall be the supreme law of the Republic of Poland."[473]

Some fields of human activity are regulated by more specific norms usually collected in acts dedicated to regulating the specific field. The purpose of all the norms in any act of law is to ensure that constitutional values are applied. For instance, Article 38 of The Constitution of the Republic of Poland states that "The Republic of Poland shall ensure the legal protection of the life of every human being." but there are numerous regulations in The Penal Code that articulate that law in-depth.

Unfortunately, not every field of human activity is comprehensively regulated by the legislator. That is when the search for norms that can be applied in a certain legal problem is much more difficult but not impossible.

As mentioned above, every norm has its roots in fundamental values expressed in other norms. That is why it is allowed, assuming that the system of norms is always based on certain consistent axiological values, to conclude that a certain norm is applicable and binding even if it is not directly expressed in a form of a written provision of law.

The way of solving the problem that the lack of norms directly regulating certain behaviours is - is to conclude that based on existing norms (or their axiological justification), it is explainable that a different norm also exists. There are many ways of coming to such a conclusion, based on inferential reasonings, shaped by the legal doctrine.[474]

10.1.2. The threat of facing the lack of comprehensive regulation

It is possible to solve a legal problem without a written provision of law but to do so is no easy task and more importantly, not every conclusion is going to be the same. That poses a threat to the everyday life of the citizen living in a country governed by the legal system of civil law. How? In the civil law system, the legal doctrine fills the 'small' holes in the legal system created by the legislator. It is not and never will be the task for the legal doctrine to make law in the sense of legislation.

[473] ibid, art 8.
[474] M. Zieliński, Wykładnia prawa, Warszawa 2017.

As mentioned before, the legal doctrine is equipped with some tools allowing it to answer some important questions in the process of applying the law. However, these tools are not suitable to answer the questions that should be answered by the legislator. There are issues that are said to be "of a grounded position in the doctrine" as well as the ones that are said to be "in the dispute of the doctrine." The role of the legislator is to provide the legal system with clear, definitive answers - norms. Some issues cannot be left for the doctrine to dispute and need to be answered by The Sovereign (The People, represented by the legislator expressing the will of The Nation).

Leaving the questions unanswered creates a dangerous situation for everyone - a situation where one's fate can be decided not by the norms expressed in a form of a written provision of law, that is to be decided by the court, but by the doctrine, that can be in dispute. That poses a threat to the legal system itself as that is how it can become unstable, unreliable and no longer trusted.

10.2. What needs to be regulated?

There are areas of human rights that are quite well-regulated when it comes to the aspect of comprehensiveness, such as, mentioned in the second main question of this paper, area of protecting personal information, regulating the right to access, modify and remove specific kinds of personal information - a form of protecting the right to privacy. There are, however, fields in the Polish legal system, as in any legal system, that need improvement. Some more than others - here are the fields of law that need improvement in order to effectively protect human rights online.

10.2.1. The field of Artificial Intelligence - big questions unanswered.

It is important to state at the very beginning that Artificial Intelligence (AI) is a new area of research not only for law studies but for any studies - from philosophy to robotics.
However, the fact that something is new does not mean it does not need to be explicitly regulated by law. It often means exactly the opposite.

The legal problems of AI are, however, far more fundamental than the lack of complex, comprehensive regulations. The most important question that is still unanswered by the legislator (not only in Poland but in the vast majority of other countries) is the legal definition of Artificial Intelligence and whether it is to be seen as a subject of the law or an object of the law.

We have already started to see the importance of defining the ideas of 'artificial intelligence', 'intelligence' in the forms of legal definitions.

It is best shown in the context of intellectual property - if the property is supposed to be connected directly to its creator, the question of whether we can call AI a subject of law (able to be the carrier of entitlements and responsibilities) or an object of law (not much more than a tool in the perspective of the legal system). Are the creations of AI the

property of the creator of an algorithm - a human? Who is the creator of 'The Day a Computer Writes a Novel' - a human, the creator of AI, or AI itself? Who almost won the Nobel prize - the human, the algorithm, both?

According to the Polish Law on Copyright and Related Rights[475] "Unless the law provides otherwise, author's moral rights protect the author's bond with the work which is indefinite in duration and which may not be waived or transferred."[476] That means only the subject of law, the carrier of entitlements and responsibilities, can be the carrier of the rights to own anything - no matter who or what brought the creation into existence.

Law has always struggled to keep up with reality. Now, in times of rapid development in almost all areas of human activity, it is visible more than ever. The area of AI needs to be regulated soon because there are far too many opinions regarding AI to ensure stability in the system of law if it is left without comprehensive, clear regulations.

The matter that needs to be regulated is complex, first of it's kind to ever exist but we need someone to pioneer the way to regulating the field of AI now when the existing questions pertain to the areas of civil law and not criminal law - yet.

10.2.2. Certain tasks require certain tools to be done well - how to defend our rights effectively.

There is a basic dichotomous division of legal norms. Every norm can be classified as a norm regarding the rights and duties of the subjects of law, the people (substantive law) or the ones that lay down the ways and means by which substantive law can be enforced (procedural law).

The norms regarding procedural law are unfortunately dated because they mostly were created to suit a world without cyberspace, cybercrime and the 'cyberworld' in general. Over time, the ways of infringing the norms of substantive law have changed. There are new spaces in which our rights can be violated. With time, new ways of breaking human rights such as freedom of expression, the right to privacy, the prohibition of discrimination etc. have appeared and the legal system needs to react to them with new laws regarding the procedure of defending them.

Every legal system needs the tools to enforce the law effectively and, whenever possible, easily which has always been a challenging task. Unfortunately, with new ways of breaking the law, it has become even more difficult. That is why there is a visible need to modernise the law, the process of applying the law itself in order to effectively enforce the substantive

[475] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2019 r. poz. 1231 z późn. zm.).
[476] Ewa Kucharska, Michele Le Mauviel, "Ustawa o prawie autorskim i prawach pokrewnych Law on Copyright and Related Rights", Wydawnictwo C.H.Beck, 2017, ISBN: 9788325595562.

law that expresses our rights and freedoms. It can be done both by modernising procedural law and equipping state authorities with the right competencies.

Here are some examples of aspects that need to be modernised when it comes to this area of law:

- regulations on digital evidence,
- electronic communication with the court,
- popularisation of digital signatures,
- acquiring tools and legitimising the use of tools that allow for digital search (based on a valid warrant in certain situations).

Conclusion

As stated above in this report, GDPR, as well as polish provisions in principle, ensure effective protection of personal data. Nevertheless, each breach case has to be considered individually. It is also to highlight that effectiveness of law requires not only precise, clear provisions but also appropriate knowledge of those who apply them. That said, the personal data shall reach the maximum of protection under the condition of the awareness of its importance among administrators, controllers, DPOs and subjects whose rights may be violated. Concerning the matter of antidiscrimination, the necessity of complex regulation shall be noted. The currently applying act does not respond to the expectations. Legal measures available for subjects to pursue claims in the matter of rights violation are appropriate. However, Polish procedures of receiving electronic evidence do not meet expectations and shall lead to closer cross border cooperation in matters of rights violation caused by new technology.

One of the most significant issues with legislators struggling around the globe is the legal status of Artificial Intelligence. The presumably incredible influence of AI in the following decades on every aspect of human life – including human rights – implicates the importance of proper regulations on both international and domestic fields. Until the legal status of Advanced Digital Technologies is stated, the protection of human rights shall be ensured by teleological interpretation of existing provisions.

Table of legislation

Provision in Polish	Corresponding translation in English
Konstytucja Rzeczypospolitej Polskiej, artykuł 32 1. Wszyscy są wobec prawa równi. Wszyscy mają prawo do równego traktowania przez władze publiczne. 2. Nikt nie może być dyskryminowany w życiu politycznym, społecznym lub gospodarczym z jakiejkolwiek przyczyny.	The Constitution of the Republic of Poland, Article 32 1. All persons shall be equal before the law. All persons shall have the right to equal treatment by public authorities. 2. No one shall be discriminated against in political, social or economic life for any reason whatsoever
Konstytucja Rzeczypospolitej Polskiej, artykuł 51 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.	The Constitution of the Republic of Poland, Article 51 1. No one may be obliged, except on the basis of statute, to disclose information concerning his person. 2. Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law. 3. Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute. 4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute. 5. Principles and procedures for collection of and access to information shall be specified by statute.
Konstytucja Rzeczypospolitej Polskiej, artykuł 87 1. Źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia. 2. Źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są na obszarze działania organów, które je ustanowiły, akty prawa miejscowego.	The Constitution of the Republic of Poland, Article 87 1. The sources of universally binding law of the Republic of Poland shall be: the Constitution, statutes, ratified international agreements, and regulations. 2. Enactments of local law issued by the operation of organs shall be a source of universally binding law of the Republic of

	Poland in the territory of the organ issuing such enactments.
Konstytucja Rzeczypospolitej Polskiej, artykuł 176 1. Postępowanie sądowe jest co najmniej dwuinstancyjne. 2. Ustrój i właściwość sądów oraz postępowanie przed sądami określają ustawy.	The Constitution of the Republic of Poland, Article 176 1. Court proceedings shall have at least two stages. 2. The organizational structure and jurisdiction as well as procedure of the courts shall be specified by statute.
Kodeks cywilny, artykuł 23 Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.	Polish Civil Code, Article 23 The personal interests of a human being, in particular health, freedom, dignity, freedom of conscience, name or pseudonym, image, privacy of correspondence, inviolability of home, and scientific, artistic, inventive or improvement achievements are protected by civil law, independently of protection under other regulations
Kodeks cywilny, artykuł 24 § 1. Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny. § 2. Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych. § 3. Przepisy powyższe nie uchybiają uprawnieniom przewidzianym w innych przepisach, w szczególności w prawie autorskim oraz w prawie wynalazczym	Polish Civil Code, Article 24 § 1. Any person whose personal interests are threatened by another person's actions may demand that the actions be ceased unless they are not unlawful. In the case of infringement he may also demand that the person committing the infringement perform the actions necessary to remove its effects, in particular that the person make a declaration of the appropriate form and substance. On the terms provided for in this Code, he may also demand monetary recompense or that an appropriate amount of money be paid to a specific public cause. § 2. If, as a result of infringement of a personal interest, financial damage is caused, the aggrieved party may demand that the damage be remedied in accordance with general principles. § 3. The above provisions do not prejudice any rights provided by other regulations, in particular by copyright law and the law on inventions.
Kodeks cywilny, artykuł 415 Kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia.	Polish Civil Code, Article 415 Fault. Anyone who by a fault on his part causes damage to another person is obliged to remedy it.
Ustawa z dnia 30 czerwca 2000 r. Prawo własności przemysłowej, artykuł 294	Industrial Property Law Act of 30 June 2000, Article 294

Art. 294. 1. Twórca wynalazku może dochodzić roszczenia o wynagrodzenie za korzystanie z jego wynalazku przed sądem okręgowym. 2. W postępowaniu, o którym mowa w ust. 1, stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego, dotyczące postępowania w sprawach o roszczenia pracowników.	1. An inventor may enforce his claims for remuneration for the exploitation of his invention before a district court. He shall not be obliged to pay court costs. 2. In the case referred to in paragraph (1), the provisions of the Code of Civil Procedure governing legal actions involving claims arising out of employment shall apply accordingly.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 8 Administrator i podmiot przetwarzający są obowiązani do wyznaczenia inspektora ochrony danych, zwanego dalej „inspektorem", w przypadkach i na zasadach określonych w art. 37 rozporządzenia 2016/679.	Act on Personal Data Protection of 10 May 2018, Article 8 The controller and the processor shall be obliged to designate a data protection officer, hereinafter referred to as "officer", in the cases and in accordance with the principles set out in Article 37 of the Regulation 2016/679.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 9 Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się: 1) jednostki sektora finansów publicznych; 2) instytuty badawcze; 3) Narodowy Bank Polski.	Act on Personal Data Protection of 10 May 2018, Article 9 The public authorities and bodies obliged to designate the officer referred to in Article 37 para. 1(a) of the Regulation 2016/679 shall mean: 1) entities of the public finance sector; 2) research institutes; 3) the National Bank of Poland.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 27, paragraf 2 Kodeks postępowania przed przekazaniem do zatwierdzenia Prezesowi Urzędu podlega konsultacjom z zainteresowanymi podmiotami.	Act on Personal Data Protection of 10 May 2018, Article 27 paragraph 2 Prior to being forwarded to the President of the Office for approval, the code of conduct shall be consulted with interested entities.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 29 1. Akredytacja podmiotu, o którym mowa w art. 28, jest udzielana na wniosek, który zawiera co najmniej: 1) nazwę podmiotu ubiegającego się o akredytację oraz adres jego siedziby; 2) informacje potwierdzające spełnianie kryteriów, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679. 2. Do wniosku dołącza się dokumenty potwierdzające spełnianie kryteriów, o	Act on Personal Data Protection of 10 May 2018, Article 29 1. Accreditation of the body referred to in Article 28 shall be granted upon request containing at least: 1) the name of the body applying for accreditation and the address of its registered office; 2) information confirming the fulfilment of the criteria referred to in Article 41 para. 1 and 2 of the Regulation 2016/679.

których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679, albo ich kopie. 3. Wniosek składa się pisemnie w postaci papierowej opatrzonej własnoręcznym podpisem albo w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.	2. Documents confirming the fulfilment of the criteria referred to in Article 41 para. 1 and 2 of the Regulation 2016/679 or copies thereof shall be attached to the application. 3. The application shall be submitted in written form on paper or in electronic format, signed with, respectively, a handwritten signature or a qualified electronic signature or a signature confirmed by a trusted ePUAP profile
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 30 1. Prezes Urzędu rozpatruje wniosek, o którym mowa w art. 29 ust. 1, i w terminie nie dłuższym niż 3 miesiące od dnia złożenia wniosku zgodnego z art. 29, po zbadaniu spełniania kryteriów, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679, zawiadamia podmiot ubiegający się o akredytację o udzieleniu lub odmowie udzielenia akredytacji. 2. Wniosek złożony do Prezesa Urzędu niezawierający informacji, o których mowa w art. 29 ust. 1 pkt 1, pozostawia się bez rozpoznania. Jeżeli wniosek nie zawiera informacji, o których mowa w art. 29 ust. 1 pkt 2, lub nie spełnia wymagań, o których mowa w ust. 2 lub 3, Prezes Urzędu wzywa wnioskodawcę do ich uzupełnienia wraz z pouczeniem, że ich nieuzupełnienie w terminie 7 dni od dnia doręczenia wezwania spowoduje pozostawienie wniosku bez rozpoznania. 3. W przypadku stwierdzenia, że podmiot ubiegający się o akredytację nie spełnia kryteriów, o których mowa w art. 41 ust. 1 i 2 rozporządzenia 2016/679, Prezes Urzędu odmawia udzielenia akredytacji. Odmowa udzielenia akredytacji następuje w drodze decyzji	Act on Personal Data Protection of 10 May 2018, Article 30 1. The President of the Office shall consider the application referred to in Article 29 para. 1 and, within a time not exceeding 3 months of the day the application compliant with Article 29 is submitted, after checking whether the criteria referred to in Article 41 para. 1 and 2 of the Regulation 2016/679 have been fulfilled, shall notify the body applying for accreditation about either a successful accreditation or its refusal. 2. An application submitted to the President of the Office, not containing the information referred to in Article 29 para. 1(1), shall not be considered. Should the application lack the information referred to in Article 29 para. 1(2), or should it not fulfil the requirements referred to in para. 2 or 3, the President of the Office shall call upon the applicant to supplement it, together with an instruction that failure to supplement it within 7 days of the day of delivery of the summons shall cause the application to be left unconsidered. 3. Should it be determined that the body applying for accreditation does not fulfil the criteria referred to in Article 41 para. 1 and 2 of the Regulation 2016/679, the President of the Office shall refuse accreditation. The refusal to grant an accreditation shall be made by way of a decision.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 60 Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych, zwane dalej „postępowaniem", jest prowadzone przez Prezesa Urzędu.	Act on Personal Data Protection of 10 May 2018, Article 60 The procedure in case of infringement of the personal data protection provisions, hereinafter referred to as "procedure", shall be conducted by the President of the Office.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 78	Act on Personal Data Protection of 10 May 2018, Article 78

1. Prezes Urzędu przeprowadza kontrolę przestrzegania przepisów o ochronie danych osobowych. 2. Kontrolę prowadzi się zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli lub na podstawie uzyskanych przez Prezesa Urzędu informacji lub w ramach monitorowania przestrzegania stosowania rozporządzenia 2016/679.	1. The President of the Office shall inspect the compliance with the personal data protection provisions. 2. The inspection shall be conducted in accordance with the inspection plan approved by the President of the Office or on the basis of information obtained by the President of the Office or as part of the process of monitoring of compliance with the Regulation 2016/679.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 84 1. Kontrolujący ma prawo: 1) wstępu w godzinach od 600 do 2200 na grunt oraz do budynków, lokali lub innych pomieszczeń; 2) wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli; 3) przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych; 4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego; 5) zlecać sporządzanie ekspertyz i opinii. 2. Kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach, o których mowa w ust. 1 pkt 3. 3. Kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków, o których mowa w ust. 2. W przypadku odmowy potwierdzenia za zgodność z oryginałem kontrolujący czyni o tym wzmiankę w protokole kontroli. 4. W uzasadnionych przypadkach przebieg kontroli lub poszczególne czynności w jej toku, po uprzednim poinformowaniu kontrolowanego, mogą być utrwalane przy pomocy urządzeń rejestrujących obraz lub	Act on Personal Data Protection of 10 May 2018, Article 84 1. The inspector shall have the right to: 1) enter any land, buildings, premises, or other spaces between the hours of 6 a.m. and 10 p.m.; 2) inspect documents and information directly related to the scope of the inspection; 3) inspect places, items, devices, media, IT and ICT systems used in data processing; 4) ask for written or oral clarifications and to question, as witnesses, other persons to the extent necessary to determine the current state of affairs; 5) order that appraisals and opinions be prepared. 2. The inspected party shall provide the inspector and persons authorized to participate in the inspection with conditions and measures necessary to efficiently conduct the inspection, in particular, it shall prepare, on its own, copies or printouts of documents and information contained on data carriers, devices, or systems referred to in para. 1 (3). 3. The inspected party shall confirm that the copies or printouts referred to in para. 2 are true copies of the original. In case of a refusal to make such confirmation, the inspector shall make note of this fact in the inspection protocol. 4. In justified cases the course of the inspection or specific activities performed as part of the inspection, after informing the inspected party, can be recorded using image or audio recording devices. Electronic data carriers within the meaning of the Act of 17 February 2005 on the Computerization of the Business Entities Pursuing Public Tasks (Journal of Laws of 2017, item 570 and of

dźwięk. Informatyczne nośniki danych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848 i 1590), na których zarejestrowano przebieg kontroli lub poszczególne czynności w jej toku, stanowią załącznik do protokołu kontroli.	2018, item 1000), on which the course of the inspection or specific activities performed as part of the inspection have been recorded, shall constitute an attachment to the inspection protocol.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 92 W zakresie nieuregulowanym rozporządzeniem 2016/679, do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 tego rozporządzenia, stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny.	Act on Personal Data Protection of 10 May 2018, Article 92 In matters not regulated in the Regulation 2016/679, the provisions of the Act of 23 April 1964 - Civil Code - shall apply to claims related to the infringement of the personal data protection provisions referred to in Article 79 and Article 82 of that Regulation.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 93 W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 rozporządzenia 2016/679, właściwy jest sąd okręgowy.	Act on Personal Data Protection of 10 May 2018, Article 93 In matters concerning claims related to the infringement of the personal data protection provisions referred to in Article 79 and Article 82 of the Regulation 2016/679, the competent court shall be the regional court.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 94 1. O wniesieniu pozwu oraz prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, o którym mowa w art. 79 lub art. 82 rozporządzenia 2016/679, sąd zawiadamia niezwłocznie Prezesa Urzędu. 2. Prezes Urzędu zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed Prezesem Urzędu lub sądem administracyjnym albo została zakończona. Prezes Urzędu niezwłocznie informuje sąd również o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia.	Act on Personal Data Protection of 10 May 2018, Article 94 1. The court shall immediately notify the President of the Office about the fact of a statement of claim being lodged and about the final ruling ending the proceedings concerning claims related to the infringement of the personal data protection provisions referred to in Article 79 or Article 82 of the Regulation 2016/679. 2. The President of the Office, notified of the pending proceedings, shall immediately inform the court about every case concerning this same infringement of the personal data protection provisions that is pending before the President of the Office or administrative court or that has ended. The President of the Office shall also immediately inform the court about commencement of any proceedings concerning the same infringement.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 95 Sąd zawiesza postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych została wszczęta przed Prezesem Urzędu.	Act on Personal Data Protection of 10 May 2018, Article 95 The court shall stay the proceedings if the action concerning the same infringement of the personal data protection provisions was brought before the President of the Office.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 96 Sąd umarza postępowanie w zakresie, w jakim prawomocna decyzja Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocny wyrok wydany w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, uwzględnia roszczenie dochodzone przed sądem.	Act on Personal Data Protection of 10 May 2018, Article 96 The court shall discontinue the proceedings within the scope in which the legally binding decision of the President of the Office ascertaining an infringement of the personal data protection provisions or a legally binding sentence passed as a result of lodging the complaint referred to in Article 145a § 3 of the Act of 30 August 2002 - Law on Procedures before Administrative Courts - includes the claim being pursued in court.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 98 1. W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, które mogą być dochodzone wyłącznie w postępowaniu przed sądem, Prezes Urzędu może wytaczać powództwa na rzecz osoby, której dane dotyczą, za jej zgodą, a także wstępować, za zgodą powoda, do postępowania w każdym jego stadium. 2. W pozostałych sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych Prezes Urzędu może wstępować, za zgodą powoda, do postępowania przed sądem w każdym jego stadium, chyba że toczy się przed nim postępowanie dotyczące tego samego naruszenia przepisów o ochronie danych osobowych. 3. W przypadkach, o których mowa w ust. 1 i 2, do Prezesa Urzędu stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2019 r. poz. 1460, 1469 i 1495) o prokuratorze.	Act on Personal Data Protection of 10 May 2018, Article 98 1. In matters concerning claims related to the infringement of the personal data protection provisions which can be pursued solely in proceedings before the court, the President of the Office may bring legal proceedings for the benefit of the data subject, upon its consent, and participate in all stages of the proceedings, also upon the plaintiff's consent. 2. In other matters concerning claims related to the infringement of the personal data protection provisions, the President of the Office may participate, upon the plaintiff's consent, in all stages of the proceedings before the court, unless proceedings concerning the same infringement of the personal data protection provisions are pending before this court. 3. In the cases referred to in para. 1 and 2, the President of the Office shall accordingly apply the provisions of the Act of 17 November 1964 - Code of Civil Procedure (Journal of Laws of 2018, item 155, as amended6)) referring to the prosecutor.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 99 Prezes Urzędu, jeżeli uzna, że przemawia za tym interes publiczny, przedstawia sądowi istotny dla sprawy pogląd w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych	Act on Personal Data Protection of 10 May 2018, Article 99 If the President of the Office considers it favourable to the public interest, he shall present to court a view significant for the case in matters relating to the claim for the infringement of the personal data protection provisions.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 100 Do postępowania w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 rozporządzenia 2016/679, w zakresie nieuregulowanym niniejszą ustawą stosuje się przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego.	Act on Personal Data Protection of 10 May 2018, Article 100 In matters not regulated herein, the provisions of the Act of 17 November 1964 - Code of Civil Procedure - shall apply to proceedings in the case of claims related to the infringement of the personal data protection provisions referred to in Article 79 and Article 82 of the Regulation 2016/679.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 101 Prezes Urzędu może nałożyć na podmiot obowiązany do przestrzegania przepisów rozporządzenia 2016/679, inny niż: 1) jednostka sektora finansów publicznych, 2) instytut badawczy, 3) Narodowy Bank Polski – w drodze decyzji, administracyjną karę pieniężną na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679	Act on Personal Data Protection of 10 May 2018, Article 101 The President of the Office may impose on the entity obliged to comply with the provisions of the Regulation 2016/679, other than: 1) entity of the public finance sector, 2) research institute, 3) the National Bank of Poland - by way of a decision, an administrative fine on the basis of and on terms and conditions stipulated in Article 83 of the Regulation 2016/679.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 107 1.Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych	Act on Personal Data Protection of 10 May 2018, Article 107 1. Any person who processes personal data, although processing thereof is not permitted, or is not authorized to process them, shall be subject to a fine, restriction of personal liberty or imprisonment for up two years. 2. If the act referred to in para. 1 pertains to data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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, shall be subject

dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.	to restriction of personal liberty or imprisonment for up three years.
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, artykuł 108 1. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. 2. Tej samej karze podlega kto, w związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej, nie dostarcza danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej lub dostarcza dane, które uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej.	Act on Personal Data Protection of 10 May 2018, Article 108 1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Bibliography

English titles

Legislation

General Data Protection Regulation,

Reports

'Right anti-discriminatory in practice of Polish common courts' Monika Wieczorek and Katarzyna Bogatko, 2013, Polish Anti-Discrimination Society

Digital resources

<https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en>

Case-law

Wesołek v. Poland, ECHR Judgement 13 June 2019, application no. 65860/12

Polish titles

Legislation

Civil Code of 23 April 1964,

Code of Civil Procedure Act of 17 November 1964,

The Constitution of the Republic of Poland of 2 April 1997,

Industrial Property Law Act of 30 June 2000,

The Act of 28 July 2005 on Court Fees in Civil Cases,

Zarządzenia nr 4 Rektora Uniwersytetu w Białymstoku z dnia 9 kwietnia 2014 r. w sprawie wewnętrznej polityki antymobbingowej,

Announcement of the Minister of Justice of 15 February 2016 on list of entities subordinated or supervised by the Minister of Justice,

Act on Personal Data Protection of 10 May 2018,

Decision of the President of the Office of Personal Data Protection of 10 September 2019, no. ZSPR.421.2.2019,

Zarządzenie nr 50/2019 Rektora Politechniki Łódzkiej z dnia 23 września 2019 w sprawie wprowadzenia regulaminu praktyk antydyskryminacyjnych w Politechnice Łódzkiej,

Decision of the President of the Office of Personal Data Protection of 18 February 2020, no. ZSZZS.440.768.2018,

Zarządzenie Rektora UW w sprawie Procedury antydyskryminacyjnej na Uniwersytecie Warszawskim z dnia 31 sierpnia 2020 roku,

Zarządzenie nr 176/2020 Rektora Politechniki Warszawskiej z dnia 22 grudnia 2020 r. w sprawie przeciwdziałania mobbingowi i dyskryminacji w Politechnice Warszawskiej

Reports

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych z 2019 roku

Books

B. Banaszak, Konstytucja Rzeczypospolitej Polskiej. Komentarz, CH Beck 2012,

P. Barta [in:] Ustawa o ochronie danych osobowych. Komentarz, red. P. Litwiński, Warszawa 2018,

A. Dmochowska, M. Zadrożny, Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem wytycznych GR art. 29, ustawy o ochronie danych osobowych z 2018 roku, CH Beck 2018,

A. Gajda, Directions of development of the institution of the Human Rights Defender in Poland, Warsaw 2013,

P. Grzegorczyk, K. Weitz [in:] Leszek Bosek, Marek Safjan, Konstytucja RP. Tom I. Komentarz do art. 1–86, CH Beck 2016

B. Gubernat/S. Szczepaniak [in:] Ustawa o ochronie danych osobowych. Komentarz, red. M. Czerniawski, M. Kawecki, Warszawa 2019,

P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018,

P. Fajgielski [in:] Komentarz do ustawy o ochronie danych osobowych [in:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018,

K. Flaga-Gieruszyńska, A. Zieliński, Kodeks postępowania cywilnego. Komentarz. Wyd. 10, Warszawa 2019,

O. Legat [in:] Ustawa o ochronie danych osobowych. Komentarz, red. B. Marcinkowski, Warszawa 2018,

List and later references to it, M. Kołodziej (red.), Vademecum Inspektora Ochrony Danych, Warszawa 2020,

Paweł Litwiński, Ustawa o ochronie danych osobowych. Komentarz, CH Beck 2018

A. Łazarska/K. Górski [in:] Kodeks postępowania cywilnego. Komentarz. Komentarz. Art. 1–505[39]. Tom I, T. Szanciło (red.), Warszawa 2019,

M. Manowska (red.), Kodeks postępowania cywilnego. Komentarz. Tom I. Art. 1-477(16), wyd. IV,

A. Marciniak [in:] Postępowanie cywilne w zarysie, 13 edition, red. T. Pietrzak, Warszawa 2020,

Z. Radwański, A. Olejniczak, Zobowiązania-część ogólna, CH Beck 2018,

P. Tuleja (red.), Konstytucja Rzeczypospolitej Polskiej. Komentarz,

N. Zawadzka [in:] Ustawa o ochronie danych osobowych. Komentarz, red. D. Lubasz, Warszawa 2019,

Lubasz, D., Chomiczewski, W., "Privacy by design a sztuczna inteligencja", Monitor Prawniczy 20/2020, p. 89,

Periodicals

A. Lach, Problem kryminalizacji naruszenia przepisów rozporządzenia ogólnego w sprawie ochrony danych osobowych, MOP 2017, no. 22

M. Zimna, Odpowiedzialność karna za naruszenie ochrony danych osobowych, Prokuratura i Prawo 2020, no. 1,

Chałubińska-Jentkiewicz K., Karpiuk M. "Prawo nowych technologii. Zagadnienia Wybrane.", Wolters Kluwer, 2015, p.21,

Digital resources

<https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2410>

Case-law

Judgment of Supreme Court of 15 February 2006, case number IV CK 384/05,

Judgment of Supreme Court of 16 May 2006, case number I PK 210/05,

Judgment of the Court of Appeal in Warsaw of 30 June 2020, case number III AUa 870/18

ELSA TURKEY

Contributors

National Coordinator
Nihan Çıtır

National Academic Coordinator
Berin Günay

National Researchers
Ayşe Ezgi Öner
Ebru Metin
Efe Gökdemir
Elif Zengin
Ezgi Ercan
Öykü Subaşı
Yağmur Gündoğdu

National Linguistic Editor
Faik Yetgin

National Technical Editor
Ebru Gümüş

National Academic Supervisor
Dr. Başak Ozan Özparlak

Acknowledgements

This research was supported by the European Law Student Association Turkey (ELSA Turkey). We are grateful to our national academic supervisor Dr Başak Ozan Özparlak, who provided insight and expertise that greatly assisted the research process, although she may not agree with all of the interpretations/conclusions of this paper and any errors are entirely ours and should not diminish her reputation. We would also like to show our gratitude to the reviewers for their comments on an earlier version of the manuscript. However, any errors are our own and should not tarnish the reputations of these esteemed persons.

Introduction

Technology has rapidly changed and developed in the last few decades and became the heart of our lives. It is hard to imagine a life without modern technology that makes our lives undeniably easier. With the development of the Internet, people access knowledge with ease and share their opinions on everything with everyone; with the development of emerging technologies such as robotics, people achieved great success in health, education, finance etc.

While advanced technologies have their fair share in a better quality of life for mankind, they have potential risks of bringing some severe problems globally. This report at hand mainly focuses on the advanced technologies' influence on human rights.

It would be wrong to say today's technology does not have any sound effects on the protection of human rights. For instance, with social media and the Internet, now it is easier to be informed about the violations of human rights all around the world; it is easier to make oneself heard in an unjust situation. With the developing technology, it is easier to monitor people who are facing a breach of their fundamental rights. With all that said, technology also has a capacity to do the exact opposite, from authorities monitoring citizens through surveillance technology to fake news and crimes committed on the Internet such as harassment, unauthored piracy of data and hate speech, and technology has its own way of undermining efforts made in order to identify and protect human rights.

Personal data is now one of the most valuable things; it is used in advertisement and sales, studies in technology and health and in more areas. The concern is, the usage of personal data by companies and government can lead to significant violations of human rights, especially the people's right to private life. Since legal regulations are parallel to humans' needs, it is crucial to enact laws regarding technological developments and data privacy with respect to fundamental human rights.

Since this study primarily establishes its scope by narrowing down the risks in the field of data protection, the right to privacy and data protection will be the focus of this report.

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

Advanced digital technologies pose risks both to society as a whole and to persons' fundamental rights individually. According to an article by Human Rights Watch,[477] The fundamental disruption caused by the advanced digital technologies ('ADT'), such as artificial intelligence, robotics and the Internet of things, are exponential risks, affecting many dimensions of society at once and disabling the policymakers to assess and mitigate risks. On the other hand, Recommendation 2102 (2017) of the Council of Europe also emphasizes that the convergence of specific technologies such as 'nanotechnology, biotechnology, information technology and cognitive sciences' pose risks to the very concept of being a human.[478] In addition to these, artificial intelligence in judiciary systems also pose certain risks for persons who are subject to trial.[479]

In reality, we have already started seeing the ADT's adverse effects with two dimensions: 1- The inequality caused in the society depending on the access to the technology, and 2- Threats to humans' rights due to the misuse of the ADTs.[480] In the first dimension, we see that the first and foremost impact of technology is heightening social inequality.[481] Thus, persons who have access to technology and information have an upper advantage in access to justice over persons who do not have access to technology. On the other hand, misuse of ADT will cause severe human rights violations varying from data privacy violations to excessive energy consumption[482] and even heightening climate change.

The nature and universality of human rights as a subject makes countries share a common confrontation against ADTs. In this regard, inspired by the Council of Europe's ('CoE') study's framework,[483] ADTs pose including but not limited to the following risks on human rights as enacted under the Constitution of the Republic Turkey:

- Equality before the law (Art.10)
- Right to privacy and protection of private life (Art. 20)

---

[477] Human Rights Watch, 'Digital Disruption of Human Rights' (25 March 2016), <https://www.hrw.org/news/2016/03/25/digital-disruption-human-rights,> accessed 4 March 2021.

[478] Recommendation 2102 [2017] 'Technological converge, artificial intelligence and human rights' <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en> accessed 2 March 2021.

[479] Raja Rajput, 'Can AI be fairer than a human judge in the judicial system?' (ReadWrite, 14 May) <https://readwrite.com/2020/05/14/can-ai-be-fairer-than-a-human-judge-in-the-judicial-system/> accessed 3 March 2021.

[480] Stephen P.Marks, 'Science and Engineering Ethics' (Springer, 2014) <https://cdn1.sph.harvard.edu/wp-content/uploads/sites/580/2012/08/Marks-2014-Comment-in-Science-and-Engineering-Ethics.pdf> accessed 4 March 2021.

[481] Phil Bloomer, 'Technology & Human Rights', (Business & Human Rights Resource Centre) < https://www.business-humanrights.org/en/big-issues/technology-human-rights/> accessed 3 March 2021.

[482] Mikko Dufva, 'How can technology be misused?' (Sitra, 9 January 2019) <https://www.sitra.fi/en/articles/can-technology-misused/> accessed 3 March 2021.

[483] Council of Europe, 'A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework' <https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168094ad40>.

- Right to freedom of communication (Art. 22)
- Freedom of expression and dissemination of thought (Art. 26)
- Right to a fair trial (Art. 36)
- Right to protection against discrimination in the exercise of rights and freedoms
- Protection of fundamental rights and freedoms (Art.40)

As mentioned earlier, there are several rights and freedoms of people affected adversely by the misuse of ADTs or the non-regulation of the inequality caused by the ADTs. Thus, states need to take necessary precautions to adapt the human rights mechanisms and take precautions to mitigate human rights violations' risks caused by ADTs.

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?

One method to mitigate risks is to identify human rights issues posed by ADTs by carrying out human rights impact assessments.[484] Under Turkish laws, human rights impact assessments have not been codified under any laws. Despite this fact, Turkey is familiar with human rights impact assessments via self-regulatory mechanisms[485], indirectly via regulations of the Human Rights and Equality Institution of Turkey[486] and related and specific to the right to privacy through the General Data Protection Regulation of the European Union.[487]

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

On the international level, Turkey is a signatory to many international human rights treaties, including the following:

- Universal Declaration of Human Rights (1949)
- European Convention on Human Rights (1954)
- International Covenant on Economic, Social and Cultural Rights (2000)
- Convention on the Elimination on All Forms of Discrimination against Women (1985)

On the national level, the Constitution of the Republic of Turkey is the primary legislation under which human rights are enacted, and the Human Rights and Equality Institution of

[484] United Nations Human Rights Office of the Commissioner, 'Guiding principles for human rights impact assessments for economic reform policies' A/HRC/40/57.
[485] International Labour Organisation, "Rapid Self-Assessment' tool developed to guide companies in human rights practices in Covid-19 times' (2 November 2020) <https://www.ilo.org/ankara/areas-of-work/covid-19/WCMS_759934/lang--en/index.htm> accessed 7 March 2021.
[486] Human Rights and Equality Authority of Turkey, Regulations <https://www.tihek.gov.tr/kategori/yonetmelikler/> accessed 7 March 2021.
[487] Ben Wolford, 'Data Protection Impact Assessment (DPIA) '(GDPR.eu) <https://gdpr.eu/data-protection-impact-assessment-template/ > accessed 7 March 2021.

Turkey is the responsible authority that carries out the mission to protect human rights and equal treatment of persons.

Since this paper establishes its scope by narrowing down the risks in data protection, the right to privacy and data protection will be the focus of the rest of the questions.

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

Personal information is secured under the right to privacy, which is essentially a constitutional right in the Turkish legislative framework. According to the 20(2) of the Constitution, everyone has the right to demand respect for his/her private life. Correspondingly, everyone has the right to request the protection of his/her personal data. Recognizing that technological advancements had paved the way for interventions in the fundamental rights and liberties, which gave rise to multiple questions of law, a sub-article was added to the extent of Article 20 as a result of approving the Law Regarding the Constitutional Amendment No. 5982 in 2010. The right to protection of personal data thereby includes 'being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives.' It was decided that personal data can be processed merely in cases laid down in law or envisaged by the person's explicit consent. The Constitution expressly states that elaborative regulations regarding the protection of personal data shall be made in the form of legislation.

The enactment of a local data protection law had been in progress for more than 35 years in Turkey. The first commission to legislate an exclusive regulation with respect to the protection of personal data was established in 1989. However, it was dissolved without further achievements. Another commission was founded in 2000 and ultimately drafted a law after three years of work. Unfortunately, the draft was not enacted due to several reasons. In 2008 and 2014, although a new law was drafted under the guidance of the Ministry of Justice and introduced to the Turkish National Assembly, it had to become obsolete by virtue of the termination of the legislative year. Until 2016, the regulations regarding the protection of personal data, except for certain specialized sectors, were constituted by a sole provision in the Turkish Constitution and few provisions in the Turkish Penal Code.[488,489] Particularly, Article 135, 136 and 138 of the Penal Code criminalize 'recording on personal data', 'illegally obtaining and disseminating data' and 'destructing data' in the respective order. In addition, Article 140 regulates the security measures that will be applied to the legal persons in the event of committing the

[488] Ozan Karaduman, 'The New Personal Data Protection Law 2019 in Turkey' (Gün+Partners Insights, 14 February 2019) <https://gun.av.tr/insights/articles/the-new-personal-data-protection-law-2019-in-turkey> accessed 5 February 2021.

[489] Initial arrangements for the protection of personal data in Turkey were made with the 5237 Turkish Penal Code on 1 June 2005. The legislator put the rationale for the provisions of the Turkish Penal Code as recognising the validity of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108 of the Council of Europe, which Turkey signed on 28 January 1981.

above-mentioned crimes. Admittedly, none of those provisions was sufficient for responding to the needs of developing technology and the amount of personal data processed and transferred every day. The final step to enact the Law on Protection of Personal Data No. 6698 (The Personal Data Protection Law as in Kişisel Verileri Koruma Kanunu-KVKK) was completed on 7 April 2016, which is several weeks before the EU passed its own General Data Protection Regulation. After the final draft received Presidential approval and the text was published in the Official Gazette, No. 29677, an extensive prohibition was implemented in Turkey on 'processing or storing personal data without explicit consent from the data subject and subject to certain limited exceptions' where such consent is not compulsory. All companies that kept personal data before 7 April 2016 received 'a two-year grace period to ensure the data met the new legislative requirements.'[490] The Turkish Data Protection Authority (TDPA), which has a status of an independent supervisory authority in terms of administration and finance, was established in early 2017.[491] It plays a crucial role in enforcing the provisions of KVKK and raising public awareness about personal data protection.

In this regard, KVKK is the main Turkish national legislation for the protection of personal data and the right to privacy of natural persons with respect to automated or non-automated processing of personal data. It applies to any data controllers and processors that either collect data or process data from Turkey. Not only does its scope include entities located within Turkey, but it also encompasses any foreign natural or legal persons that process the personal information of Turkish data subjects. Turkey executed the Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data ('Convention 108') with the other Member States on 28 January 1981 but delayed its ratification into national law until 2 May 2016, and it entered into force on 1 September 2016.[492] Moreover, the recently published National Cyber Security Strategy Report 2020-2023 underlines the national data strategy in the sense that data deriving from Turkey shall remain in Turkey. The application made by the data controller, TEB Arval Vehicle Fleet Leasing Corporation, for the Commitment regarding the transfer of personal data abroad has been recently evaluated within the scope of Article 9(2) of the Personal Data Protection Law No 6698. The permission for the respective data transfer was granted by TDPA on 9 February 2021.[493] This approach resembles the European Court of Justice's ruling in Schrems II Judgement in 2020 and the decision of the French Data Protection

[490] Burcu Tuzcu Ersin, 'Turkey-Data Protection Overview' (One Trust Data Guidance, April 2020) <https://www.dataguidance.com/notes/turkey-data-protection-overview> accessed 7 February 2021.
[491] Andrada Coos, 'All You Need to Know About Turkey's Personal Data Protection Law (KVKK)' (Endpoint Protector, 30 April 2020) <https://www.endpointprotector.com/blog/everything-you-need-to-know-about-turkeys-personal-data-protection-law/> accessed 5 February 2021.
[492] Burcu Tuzcu Ersin, 'Turkey-Data Protection Overview' (One Trust Data Guidance, April 2020) <https://www.dataguidance.com/notes/turkey-data-protection-overview> accessed 7 February 2021.
[493] KVKK, 'Public Announcement on Application for Commitment' (kvkk.gov.tr, 9 February 2021), <https://kvkk.gov.tr/Icerik/6884/Public-Announcement-on-Application-for-Commitment> accessed 4 March 2021.

Authority (CNIL), which concluded that health data of French nationals shall not be stored in cloud systems that have US-based servers.[494] In spite of its deficiencies, the introduction of the Data Protection Law is a critical development for Turkey and can be considered as a plausible beginning for further improvement in the country's data protection laws.

In addition, secondary legislation in the form of regulations and communiqués outline how Turkey's data protection regime operates in practice.[495] Draft versions of secondary legislation have been published by TDPA. Under these modifications, data controllers have to perform multiple obligations when supervising personal data. In fact, the legislation has a considerable impact on each employee urging the companies operating in Turkey to comprehend the consequences of compliance failure. In this regard, key regulations include Regulation on Deletion, Destruction or Anonymization of Personal Data 2017, Regulation on the Data Controller Registry 2017, Regulation on Working Procedures and Principles of the Personal Data Protection Board 2017, Regulation on Organisation of the Personal Data Protection Authority 2018, Regulation on Promoting and Change of Title of the Data Protection Authority Personnel 2018, Regulation on Personal Data Protection Expertise 2018, Regulation on Disciplinary Supervisors of Personal Data Protection Authority 2019 and Regulation on Personal Health Data 2019. Furthermore, key communiqués include Communiqué on Principles and Procedures for Application to Data Controller 2018 and Communiqué on Procedures and Principles Regarding the Data Controller's Obligation to Inform Data Subjects 2018.

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

According to Article 3(d) of the KVKK, personal data is any information relating to an identified or identifiable natural person. In this respect, it is evident that there are two requirements to distinguish between personal and non-personal data. In order for data to be defined as personal data, the data must be related to a person, and that person must be identified or identifiable. The person to be protected is a 'natural person', as clearly stated in the definitions in the Law. If data of a legal person identifies or makes a natural person identifiable, these data are protected under the Law as well. However, the interest in question to be protected here belongs to the natural person, not to the legal person, since the Law does not cover the processing of personal data concerning legal persons.[496] Before KVKK was enacted, there was a discussion on whether information related to legal entities should be classified as personal data. The new definition of personal data came to the conclusion that only individuals (natural persons) can have personal data. Therefore, the

[494] CNIL, 'The Council of State asks the Health Data Hub for additional guarantees to limit the risk of transfer to the United States' (cnil.fr, 16 October 2020) <https://www.cnil.fr/en/council-state-asks-health-data-hub-additional-guarantees-limit-risk-transfer-united-states> accessed 4 March 2021.
[495] Burcu Tuzcu Ersin, 'Turkey-Data Protection Overview' (One Trust Data Guidance, April 2020) <https://www.dataguidance.com/notes/turkey-data-protection-overview> accessed 7 February 2021.
[496] KVKK, 'Data Protection in Turkey'.

term 'data subject' is used in the Law to refer to a natural person whose personal data are being processed. Article 6 defines 'personal data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing, membership of associations, foundations or trade unions, information related to health, sex life, previous criminal convictions and security measures, and biometric and genetic data as special categories of personal data.' KVKK consists of stricter provisions for special types of personal data that are particularly sensitive as such.

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 the protection of personal information are compatible with EU law, particularly the General Data Protection Regulation (GDPR).

Although the Republic of Turkey is not a Member State of the European Union, as a candidate country, Turkish Laws must be in compliance with the EU *acquis*. In fact, the Data Protection Law is a significant step towards harmonizing Turkish legislation with EU legislation. Accordingly, KVKK outlines a similar framework to the European data protection system within the framework of the Data Protection Directive (Directive 95/46/EC), General Data Protection Regulation (Regulation (EU) 2016/679) and Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680). Fundamentally, KVKK is very similar to the Data Protection Directive, but it is not a complete replica and features various additions and revisions. Therefore, an exhaustive comparison is crucial to elaborate on the intricacies and distinguish between KVKK and the EU legislation. Only if the data controllers that are used to the EU pay careful attention to the differences between the EU legislation and KVKK can they avoid the implications that these differences are most likely to cause in practice. Similarly, data controllers that reside outside of Turkey but process the personal data of Turkish residents must be aware that the obligations of KVKK will apply to them as well as to the data controllers within Turkey.

Even though KVKK constitutes almost all the same fair information practise principles, KVKK does not permit a 'compatible purpose' interpretation, whereas any further processing is restricted. When the data is collected for a purpose in which the subject's consent was taken, the controller may utilize it for another purpose provided that additional consent is further given, or further processing becomes required for legitimate interests.[497] Moreover, there are other regarding the cross-border transport of data and children's data protection, which are not entirely compatible with the EU *acquis*. Unlike the GDPR, KVKK does not have a territorial scope. Taking into account the principle of territoriality applicable under Turkish Law, KVKK applyies to all natural and legal persons who process data originating from Turkey regardless of whether they are located in Turkey

[497] *'Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler'*, Bilgi University (Istanbul, 2020).

or abroad. International transfer of personal data is authorized if the data subject explicitly gives consent and the country's level of data protection is considered adequate by the TDPA.[498] Otherwise, the data controllers are obliged to ensure by writing that they will provide an adequate level of protection in a way TDPA approves. In the essence of what KVKK stipulates through its provision that is 'In cases where interests of Turkey or the data subject will be seriously harmed, personal data shall only be transferred abroad upon the approval of the Authority by obtaining the opinion of relevant public institutions and organizations.', data controllers are obliged to make an evaluation about whether a transfer might result in serious harm. If there appears a possible risk of such harm, they need to obtain the TDPA's approval. While these provisions are similar to those of the GDPR, KVKK further authorizes the TDPA to restrict the cross-border transfer of data even if the explicit consent of the data subject is obtained if the officials conclude that the interests of Turkey or the data subject will be seriously harmed. Unfortunately, how such interests are to be determined remains highly uncertain.

Grounds for data processing under KVKK are mostly corresponding to those which apply for GDPR. On the other hand, KVKK requires explicit consent when sensitive, and non-sensitive personal data is processed, which is a much more time-consuming exercise. One could expect that such a demanding obligation ultimately makes KVKK provide a higher level of data protection than GDPR at first sight. However, a comparison between the definition of explicit consent in KVKK and GDPR's regular consent reveals that KVKK's grounds for processing sensitive personal data are more constricted than GDPR. Both require 'freely given, specific and informed consent, but GDPR further provides that there has to be 'unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[499] Consequently, the majority of data considered sensitive can be processed if it is currently permitted under KVKK, except for any data concerning public health matters.

GDPR requires data controllers to maintain internal records, although there is no general requirement to register with the data protection authorities, whereas KVKK provides a hybrid solution, combining registration and record-keeping requirements.[500] In particular, the most significant difference from the GDPR is the obligation data controllers fulfil under the KVKK to enrol onto VERBIS, the TDPA's Data Controllers' Registry. To elaborate, it is a registration system in which data controllers are registered to and record the data processing activities they engage in. Data controllers must register with the

[498] Burcu Tuzcu Ersin, 'Turkey-Data Protection Overview' (One Trust Data Guidance, April 2020) <https://www.dataguidance.com/notes/turkey-data-protection-overview> accessed 7 February 2020 accessed 6 February 2021.
[499] Duygu Doğan, 'Personal Data Protection in Turkey: The Impact on Business' (GRC World Forums, 8 November 2018) <https://www.grcworldforums.com/gdpr/personal-data-protection-in-turkey-the-impact-on-business/28.article> accessed 9 February 2021.
[500] ibid.

Registry, which is held by the Authority under the supervision of the Board.[501] Obligation to register with VERBIS has the aim of establishing a safer and more transparent environment in terms of clarification of personal data processing and acting in compliance with the legislation for controllers. The procedures and principles related to the Registry are determined in the Regulation on the Data Controllers' Registry.[502] Registration in VERBIS is mandatory for all data controllers prior to processing data of Turkish residents. When registered, data controllers are required to inform about the data processing activities they engage in. Before registering in VERBIS and beginning with processing personal data, organizations must appoint a data controller representative who needs to be a Turkish Legal Entity or a Turkish Natural Person.[503] During registration, they are required to submit a Data Processing Inventory that classifies the various categories of 'data subjects, the types of data they process, their purpose, legal basis, and the technical and administrative measures that an organization is taking to comply with the KVKK'.[504] Additionally, there are several exemptions from registration in VERBIS mentioned in the second paragraph of Article 28 of KVKK.

2.3. How do external instruments (such as the above-mentioned GDPR) influence the data protection in your country (NB can be applicable to non-EU countries as well)?

As a member of the EU Customs Union, Turkey has a long history of commercial relationships with the EU. The EU's GDPR has 'extraterritorial applicability', which signifies that it encompasses all entities collecting and processing personal data of individuals residing in the EU. Consequently, GDPR also applies to private companies based in Turkey. For instance, companies that 'have offices and employees in the EU, offer goods and services to individuals in the EU through their website or app, use cookies to collect the IP address or other personal information from EU citizens and process the personal data of EU individuals' will be subject to the GDPR. In further examining the differences between the Personal Data Protection Law and GDPR, the subtlety is of how they affect businesses operating in Turkey. Any business that is subject to both KVKK and GDPR should take notice of establishing a flexible compliance model that satisfies the demands of regulatory authorities in multiple jurisdictions in order to eliminate duplication of compliance effort.[505]

---

[501] ibid.
[502] ibid.
[503] ibid.
[504] Andrada Coos, 'All You Need to Know About Turkey's Personal Data Protection Law (KVKK)' (Endpoint Protector, 30 April 2020) <https://www.endpointprotector.com/blog/everything-you-need-to-know-about-turkeys-personal-data-protection-law/> accessed 7 February 2021.
[505] Duygu Doğan, 'Personal Data Protection in Turkey: The Impact on Business' (GRC World Forums ,8 November 2018) <https://www.grcworldforums.com/gdpr/personal-data-protection-in-turkey-the-impact-on-business/28.article> accessed 9 February 2021.

Furthermore, the fines that are imposed within the framework of the GDPR serves to raise awareness on data protection in Turkey. It must be mentioned that the Board Decision (No. 2020/481) on 'the right to be forgotten' deriving from the GDPR was adopted by the Turkish Data Protection Board on 23.06.2020 within the framework of Article 20(3) of the Constitution, the regulations in the Articles 4, 7 and 11 of The Personal Data Protection Law and Article 8 of The Regulation on the Erasure, Destruction or Anonymization of the Personal Data. Upon the requests of the individuals on the 'Right to be Forgotten', the above-mentioned Decision requires a balancing test between the fundamental rights and freedoms of the data subject and the interests that the public will obtain from the information in question, observing which of the competing interests outweigh. According to the last paragraph of Article 90 of the Constitution, international treaties on fundamental rights put into effect pursuant to the regulation in Article 90 of the Constitution have the force of law. Therefore, the Council of Europe Convention 108, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, influences data protection in Turkey. However, Turkey has not yet signed the Council of Europe Convention 108+, which is for the protection of individuals with regard to the processing of personal data.

On 8 November 2001, Turkey signed the Additional Protocol No. 181 to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. Published in the Official Gazette No. 29703 on 5 Mayıs 2016, this protocol entered into effect as a part of the domestic rule of law ever since. Moreover, Turkey is among the founding members and signatories of the European Convention on Human Rights, which does not include a direct provision for processing personal data. In fact, Article 8 of the Convention, which encompasses the right to respect for private and family life home and correspondence, essentially addresses the protection of personal data solely under the scope of private and family life. Nevertheless, the court practices of the European Court of Human Rights signify that it has been protecting personal data over the years. Last but not least, as a founding member of the Organisation for Economic Co-operation and Development and a member of the United Nations, Turkey has paid regard to OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980) and United Nations Guideline for the Regulation of Computerized Personal Data Files (14 December 1990).

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

Data protection self-regulation by the industry can be simply described as 'a flexible alternative and complementary to traditional government regulation'.[506] Referring to this self-regulation description herein, Turkey also has a robust government regulation as explained under the previous question. On the other hand, we also see many reflections of the right to privacy in different global human rights advocacy mechanisms (i.e. United Nations Global Compact), which gives businesses the flexibility to enhance data protection compliance requirements as part of their membership requirements.

With respect to human rights, the Turkish private sector is quite familiar with the self-regulatory frameworks for business and human rights due to being a strong trade partner to the European Union.[507] In addition to this, there are several self-regulated bodies operating in Turkey, which fosters compliance to fundamental human rights principles in the scope of corporate sustainability via memberships, such as UN Global Compact Network Turkey promoting the UN Sustainable Development Goals.[508] Another example for self-regulation, which could be considered as co-regulation, would be Turkey's Capital Markets Board Corporate Governance Principles, whereby governs quoted companies to be more sensitive towards social responsibilities via complying with the regulations and ethical rules.[509] Even though the UN Guiding Principles on Business and Human Rights is not a primary framework, it is also advised for companies to adopt these principles in order to show their compliance to human rights when there is a dispute, and a private law liability is upon the company.[510]

Data privacy is another area in human rights where a lot of self-regulatory actions are carried out. Data protection became a hot topic in 2016 with KVKK entering into force and has been an increasingly important agenda item for the private sector since then. Especially after the establishing of The Turkish Data Protection Authority (TDPA), the secondary legislation has broadly expanded with secondary regulations and TDPA Board

---

[506] Siona Listokin, 'Industry Self-Regulation of Consumer Data Privacy and Security' <ftc.gov/system/files/documents/public_comments/2015/10/00031-97822.pdf> accessed 13 March 2021.
[507] Aram Ekin Duran, *'Türkiye'nin ihracatında AB'nin payı artıyor'* (DW, 3 February 2020) <https://www.dw.com/tr/t%C3%BCrkiyenin-ihracat%C4%B1nda-abnin-pay%C4%B1-art%C4%B1yor/a-52243850> accessed 13 March 2021.
[508] Global Compact Network Turkey, <https://www.globalcompactturkiye.org/10-ilke/> accessed 13 March 2021.
[509] Orçun Çetinkaya, Atakan Güngördü, 'Business & Human Rights Series: 01 Why are Human Rights Relevant to Businesses?' (Çetinkaya, 16 November 2020) < https://www.cetinkaya.com/insights/business-human-rights-series-01-why-are-human-rights-relevant-to-business> accessed 14 March 2021.
[510] Altuğ Özgün Çetinkaya, Atakan Güngördü, 'Business & Human Rights Series: 02 An Overview of Turkish Legal Framewor' (ICLG, 26 November 2020) <https://iclg.com/briefing/15144-business-and-human-rights-series-02-an-overview-of-turkish-legal-framework> accessed 14 March 2021.

decisions. However, there are still ongoing uncertainties and ambiguities due to secondary legislation being relatively new. Two very good examples of self-regulatory implementation in data protection would be the binding corporate rules[511] and commitment letters regarding cross border data transfers,[512] which are quite new to Turkish data processors.

There would be many reflections of self-regulatory practices due to rapid technological advancements, complex regulations and the importance of trust between the private sector, public bodies and citizens. In addition to globalization and companies trading more and more in the international markets, the impact of self-regulatory bodies both at the national and international level will also increase. In the scope of this, we expect to see more companies applying human rights due diligence, whereby OECD Due Diligence for Responsible Business Conduct could be a reference as a great source at the international level and Ethics and Reputation Society (TEİD) at the national level.

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 Constitution of the Republic of Turkey defines the right to data privacy distinctly.[513] The relevant article of the Constitution points out that everyone has the right to request the protection of his/her personal data, and it explains the scope of the protection of personal data, which includes being informed of, having access to, and requesting the correction and deletion personal data, and being informed whether the personal data used in consistency with envisaged objectives. It also sets out that personal data can be processed only in cases envisaged by law or by the explicit consent of the individual. However, the principles and procedures regarding the protection of personal data are laid down in the Turkish Personal Data Protection Law, numbered 6698. This code provides the right to data privacy only if the data subject is a natural person and the data is linked with an identified or identifiable natural person.[514] There are five principles to be complied whilst processing personal data: Lawfulness and fairness, being accurate and kept up to date where necessary, being processed for specified, explicit, and legitimate purposes, being relevant, limited, and proportionate to the purposes for which the personal data is processed, being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data is processed.[515]

---

[511] Kişisel Verileri Koruma Kurumu, 'Bağlayıcı Şirket Kuralları Hakkında Duyuru' (KVKK, 10 April 2020) <https://kvkk.gov.tr/icerik/6728/yurt-disina-kisisel-veri-aktariminda-baglayici-sirket-kurallari-hakkinda-duyuru'> accessed 14 March 2021.
[512] Kişisel Verileri Koruma Kurumu, 'Taahhütname Başvurusu Hakkında Duyuru' (KVKK, 9 February 2021) <https://www.kvkk.gov.tr/icerik/6867/taahhutname-basvurusu-hakkinda-duyuru> accessed 14 March 2021.
[513] The Constitution of the Republic of Turkey, Article 20/3.
[514] Turkish Personal Data Protection Law numbered 6698, Article 2.
[515] ibid, Article 4.

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

Personal data cannot be processed without the explicit consent of the data subject.[516] In addition, it is distinctly set out that the data subject has the right to request the erasure or destruction of the personal data if the reasons for the processing no longer exist, to object to the occurrence of a result against himself/herself due to the data processed solely through automated systems and to request correction of the incomplete or inaccurate data.[517] Therefore, if the data subject does not give explicit consent before the processing, personal data cannot be processed. If explicit consent is given before the data processing, the data subject may request a correction at any time or after the reasons for the processing disappears; personal data may be erased, destructed, or anonymized by the data subject's request. The data subject directs the request or objection to the data controller in writing or by other means determined by the Personal Data Protection Board. Thereafter the data controller either takes the necessary actions to fulfil the data subject's request or refuses the request with justified grounds within the shortest time and at the latest within thirty days and free of charge.[518] If the request is refused or the grounds for the refusal are found insufficient, the data subject may lodge a complaint with the Personal Data Protection Board within thirty days after the data controller's response.[519] However, the data subject cannot restrict or object the data processing if; the personal data is processed by natural persons solely for personal activities of the data subject or of family members living together with the data subject provided that it is not to be disclosed to third parties; the personal data is processed for the official statistics provided that the personal data is anonymized; the personal data is processed for the artistic, historical, literary or scientific purposes or within the scope of freedom of expression provided that national defence, national security, public security, public order, economic security, the right to privacy or personal rights are not violated or the process does not constitute a crime; the personal data is processed to maintain national defence, national security, public security, public order or economic security within the scope of preventive, protective and intelligence activities carried out by duly authorized public institutions and organizations; the personal data is processed to prevent a crime or to investigate a crime; for supervision or regulatory duties and disciplinary investigations and prosecution by the duly authorized public institutions and organizations; the personal data is processed to protect economic and financial interests of the state; the processed personal data is made public by the data subject.[520] In addition, there are certain situations where explicit consent is not required before data processing. Explicit consent of the data subject is not required if; it is expressly provided for by the law; the processing is necessary to protect the life or physical integrity of the data subject or of any other individual who is unable to express consent due to the

[516] ibid, Article 5/1.
[517] ibid, Article 11.
[518] Turkish Personal Data Protection Law numbered 6698, Article 13.
[519] ibid, Article 14.
[520] ibid, Article 28.

physical ability or whose consent is not legally valid; the processed personal data is made public by the data subject; the data subject is a party to a contract where it is necessary to process the personal data provided that it is directly related to the establishment of the performance of the contract; the data controller is a subject to a legal obligation where the processing deemed necessary by the law, the processing is necessary for the establishment, exercise or protection of any right; processing is necessary for the legitimate interests of the data controller provided that the processing does not violate the fundamental rights and freedoms of the data subject.[521] In these situations, the data subject will not be able to restrict or object to the data processing because explicit consent of the data subject is not taken before the data processing.

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?

In case of the processed personal data is obtained by others by unlawful means, the data controller is under the obligation to notify the data subject within the shortest time and the Personal Data Protection Board within 72 hours.[522] In this context, the Turkish Data Protection Law adopts a different approach from the General Data Protection Regulation. It does not differentiate the situations that are likely to result in a high risk to the rights and freedoms, and it obliges the data controller to notify the data subject and the Personal Data Protection Board, both.[523] The data subject is notified directly if the communication address of the data subject is determinable. If not, the notification is made through the data controller's website or similar ways.

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

5.1 Which bodies conduct such review?

Turkish Personal Data Protection Authority conducts the review procedure after exhausting the remedy of the application to the data controller under Article 13 of Law No. 6698.[524]

The Authority, which is a public legal entity, has administrative and financial autonomy and is affiliated with the Turkish Ministry of Justice under paragraph 2 of Article 19 of Law No. 6698, notwithstanding being an independent administrative authority.

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

---

[521] ibid, Article 5.
[522] ibid, Article 12/5; The Board Decision No. 2019/10 of 24.01.2019 about Procedures and Principles of Personal Data Breach Notification, <www.kvkk.gov.tr/Icerik/6647/The-Board-Decision-No-2019-10-of-24-01-2019-about-Procedures-and-Principles-of-Personal-Data-Breach-Notification-> accessed 19 February 2021.
[523] General Data Protection Regulation [04.05.2016] OJ L119/52, 53; Turkish Personal Data Protection Law numbered 6698, Article 12/5.
[524] Personal Data Protection Law of the Republic of Turkey No.6698.

Data protection breaches can be reviewed both judicially and non-judicially. Article 13 of Law No. 6698 regulates the request to the data controller in case of a breach, while Article 14 regulates lodging a complaint to the Board with the condition of exhausting the remedy of the request to the data controller and finally, Article 15 regulates the examination to be made *ex officio* if the Board finds out about the alleged breach. However, the option of lodging a complaint to the Board is completely voluntary, and it is also possible for the data subject concerned to apply directly to the judicial authorities without exhausting the remedies specified in Articles 13 and 14.

The data controller can be a natural person, a private or public legal entity, as well as a public administration. Should the data controller fail to comply with their obligations pursuant to Article 13, the data subject can direct their demands with a request to the data controller in Turkish and in writing or other means determined by the Board. Application to the data controller is further elaborated in the Communiqué on Application Procedures and Principles to the Data Controller,[525] by Article 5 of the said Communiqué, the data subject may direct their demands under Article 11 of Law No.6698 by in writing, registered electronic mail address or pre-declared electronic address or a special software signed by an electronic or mobile signature. The data controller shall conclude the demands specified in the request in the shortest possible time at the very latest by 30 days. According to paragraph 2 of Article 13, "The data controller shall act on the request or refuse it together with justified grounds and communicate its response to the data subject in writing or by electronic means.

Should the data controller also fail to comply with its obligations under Article 13, the data subject can entertain their right to lodge a complaint to the Authority under Article 14. In any case, the competent authority for the complaint procedure to the Personal Data Protection Authority is the Personal Data Protection Board, which is the decision-making body of the Authority. In cases where the request is rejected, the response is found to be insufficient, or the response is not given in time after the application made to the data controller by the data subject, the addressee of the allegations of violation of data privacy rights will be the Board.

The data subject can lodge a complaint to the Board in 30 days by the time the data subject learns the data controller's answer of the refusal of the request or the insufficient response of the data controller or the non-response or in any case, 60 days by the date of request application. Article 15 further elaborates the procedures and principles of the examination for both ex officio review and upon complaint.

Paragraph 4 of Article 15 states that, upon complaint, the Board will examine the request and respond to the parties; however, if no response is given to the person concerned within 60 days from the date of the complaint, the request will be deemed rejected.

[525] Communiqué on Application Procedures and Principles to the Data Controller No.30356.

Although it is regulated as a constitutional right for the administration to notify the applicants in writing without delay pursuant to paragraph 2 of Article 74 of the Constitution of the Republic of Turkey, the non-response within this 60-day period regulated in Law No. 6698 is an implied refusal. Thus, after the 60-day period and the administration's silence on the matter, upon parties' desire, the dispute can be transferred to the judicial bodies as it will initiate the application period of the administrative litigation.

Under paragraph 5 of Article 15 of Law No.6698, as a result of the examination made upon complaint or *ex officio*, in cases where it is understood that an infringement exists, the Board shall decide that the identified violations shall be remedied by the relevant data controller and notify this decision to the relevant parties. If the decision taken by the Board is not fulfilled, the administrative fine specified in clause c of paragraph 1 of Article 18 of Law No. 6698 will be applied.

The third non-judicial way is for the Board to examine it ex officio. In the first paragraph of Article 15 of the Law numbered 6698, which includes provisions on the procedures and principles of review upon complaint or *ex officio*, it is stipulated that the Board will carry out the necessary investigations upon complaint or ex officio in case it finds out about the alleged violation. Pursuant to the provision, the Board is obliged to make the necessary examinations within the limits of its duties. The Board may act upon complaint or, if it learns about alleged violations, it will also automatically investigate. Consequently, in order for the Board to initiate an investigation, it is not necessary that a complaint is lodged by the data subject. Third parties who learn about illegal practices will also be able to notify the Board. However, since the Board does not have an automatic general authority by the Law, the examination to be made by the Board will be limited to the subject of the violation informed by the Board.

If it is determined that the violation is widespread as a result of the ex officio examination, the Board has the authority to take a principle decision on this issue. Finally, the Board may decide to stop the processing of data or the transfer of the data abroad. The duration of the ex officio examination should also be mentioned here. Although the obligation to respond to the person concerned by examining the complaint requests within 60 days is stipulated in paragraph 4 of article 15 of Law No. 6698, no period has been stipulated in terms of the examinations to be carried out by the Board. The sanction for non-compliance with the decisions is the same as the complaint procedure to the Board. Board's authority to examine ex officio aims to create a deterrent effect.[526]

[526] Though not a remedy, another important institution within the Authority is the Data Controllers' Registry Information System (VERBIS), pursuant to Article 16 of Law no. 6698 is open to the public under the supervision of the Board. 'Data Protection Authorities should strive not to become machines for laundering the activities of the public sector or a screen to obscure the activities of large private sector controllers. To provide a hollow assurance to individuals will destroy what confidence the public might have in them.' Thus as intended to overcome this, 'VERBIS has designed as a system in which the data and responsibility of the data controllers who are obliged to register in the Registry can be entered into the technical and

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?

Turkish practices and procedures can easily be categorized as strong in the enforcement of data protection law as there are the options of both penalties, administrative fines and pecuniary and non-pecuniary damages and other sanctions. This partly due to the nature of the Turkish Data Protection Authority's as it both acts as an independent administrative institution and as a dispute resolution mechanism for the parties as an alternative; and partly due to the constitutional safeguards provided by Article 20 and Article 74 of the Constitution of the Republic of Turkey.[527]

Law No. 6698 regulated this situation with Article 14 and stated that in case of a complaint to the Board that those whose personal rights were violated reserves the right to demand compensation. '

Similar to the procedure for claiming compensation under general provisions, Articles 135 and 140 of the Turkish Penal Code will be applied if the individuals have been processed illegally and constitute a crime at the same time.

Finally, within the scope of Law No. 6698, administrative fines to be applied by the Board in case of breach of obligations by the data controller are determined.

In terms of the application of administrative fines, there is no distinction between real persons or legal persons as well as private or public legal entities. In the event that the violation is committed within public institutions and professional organizations, disciplinary action is taken against officials working in the said organizations are taken, and the Board is notified accordingly. When compared with the GDPR, said fines are less deterrent as the maximum fine is 2% of the annual return in the case where an enterprise is the data controller. Yet as it can be inferred from the popular decisions of the Board such as Decision on Facebook No. 2019/269[528], Decision No. 2019/144 about Cathay Pasific Airway[529] and Personal Data Protection Board's Decision dated 27/02/2020 numbered 2020/173 on the Application Regarding Amazon Turkey[530] that the sanctions imposed by

---

administrative measures they take in order to ensure the protection of the personal data.' This increases the foreseeability of any potential breach and enables rapid measures to be taken.

[527] 'Article 24 of Directive 9 5/46/EC states that Member States have to 'lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive'. However, the Directive does not clearly and explicitly state that a DPA shall be able to impose fines. This general provision has left it open for the national legislator to determine who can apply the sanctions, following which national law as well as the type of sanctions available. As a consequence, the sanctions for infringing data protection law can be enshrined in criminal or administrative law, they can be applied by courts or national DPAs, and their nature can be pecuniary or non-pecuniary. This led to major differences in their application throughout the EU. The obvious consequence is that some Member State DPAs are stronger' while others are 'weaker' in the enforcement of data protection law.'.

[528] [2019] The Board Decision on Facebook, No. 2019/269.

[529] [2019] The Board Decision on Cathay Pasific Airway, No. 2019/144.

[530] [2020] The Board Decision on the Application Regarding Amazon Turkey, No. 2020/173.

the Board are fairly determined and secured, there are additional sanctions imposed in the case of a failure to comply with the Board's decisions.

To ensure the constitutional right of protection of personal data, the intervention of the criminal law is inevitable. According to the Turkish Penal Code (No.5237), data protection breaches may constitute a crime under the Ninth Chapter of the Code:
— violation of privacy (Art. 134)
— recording of personal data (Art.135)
— illegally obtaining or giving data (Art.136)
—failing to destroy data in accordance with the prescribed procedures before the expiry of the legally prescribed period for destruction (Art. 138)
While Article 134 defines the acts of violating the secrecy of the private life as *actus reus*, Articles 135 and 136 of the Turkish Penal Code defines the acts of unlawful recording, transfer, sharing and seizing of personal data as *actus reus* and finally, Article 138 defines failing to destroy the personal data as *actus reus*.

Any person who violates the secrecy of private life under Article 134 is punished with imprisonment from six months to two years or imposed a punitive fine. Unlawfully recording personal data is also constitutes a crime under Article 135(1) and requires imprisonment from six months to three years. If any of the offences under the Ninth Chapter is conducted by a public officer or by exploiting the advantages of a performed profession and art, the punishment is increased by one half (Art. 137). Also, failure to destroy the data within a defined system despite the expiry of the legally prescribed period requires imprisonment from six months to one year (Art. 138).

All in all, developments in Turkey, a newcomer to the international data protection arena as of 2016, looks highly promising in terms of providing effective remedies for data breaches.

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

The breakthrough was the amendment on one of the articles of the Turkish Constitution with regards to the application of the provisions of the International Conventions into domestic law. Within the scope of the Law of Harmonization Code of the European Union, it is accepted that the international agreements duly put into effect after the aforementioned amendment made in article 90 of the Constitution in 2004 with the law numbered 5170, have the force of law in Turkey.

6.1. Constitution

Discrimination is regulated in various codes and regulations in the Turkish legal system. Firstly, article 10 of the Turkish Constitution stresses equality before the law and forbids any discrimination for any reason, and also has the Turkish Government responsible for ensuring this equality.

Article 122 Turkish Criminal Law regulates the discrimination offence along with hate with the amendment made in 2014. That is, the existence of the discrimination offence was attributed to the motive of hate. The otherwise imputed offence would not come into existence unless it is proven that it is committed with the motive of hate. Therefore, the definition of discrimination that has become a hate crime has been narrowed down. However, pursuant to the preamble of the article, any action might be considered as discrimination depending on the context. By doing this, the lawmaker emphasizes that grounds of discrimination should be interpreted broadly. However, this approach receives criticism on the grounds that it contradicts the principle of legality in crime and punishment. Although it is stated in Article 122 that the perpetrator of the crime can be anyone, Article 20 of the same code states that legal entities cannot be imposed criminal sanction, so the only way to punish the legal entities would be preventive security measures. However, pursuant to Article 60 of the TCL, in order to apply a measure against a legal entity, this measure must be referred to [531]OBJ is that while direct discrimination is regulated as a crime, indirect one is excluded. When it comes to proof of the offence, while the burden of proof may change under certain conditions in the codes or regulations where discrimination is regulated other than the Criminal Code, this situation is not possible in the field of Criminal Law. Contrary to the presumption of innocence, it cannot be expected from the suspect or the accused to prove that the crime has not occurred. As a result, it cannot be said that the intended protection has been achieved with the article.

6.2. Labour Law

Contrary to the previous code, Labour Law No. 857 includes the prohibition of discrimination in Article 5. The aforementioned article is important because that is the first regulation in which discrimination in working life is explicitly prohibited, apart from the provisions in the Constitution. Another factor that makes this law special and important is that it has included the concepts of direct and indirect discrimination in the code for the first time. As clearly stated in the justification of the article, the EU legal acquis was taken into account while drafting the provision. Although this regulation can be seen as progress, the application of the said article takes effect after the beginning of the mutual business relationship. However, in its very first sentence, the justification of Article 5 mentions that employers are obliged to treat workers equally[532] in terms of working conditions from the very beginning. In this sense, it is stated that it can be applied in the recruitment process as well. Besides, thanks to Article 18 of the Labour Law titled 'Termination of the Contract with a Valid Reason', the person has the right to demand the other rights of which he or she is deprived if the labour contract is terminated on the grounds of race, colour, gender, marital status, family obligations, pregnancy, birth, religion, political opinion or similar

[531] Ulaş Karan, 'Prohibition of Discrimination in Turkish Law And Feasibility of Article 122 of Turkish Panel Code', (Union of Turkish Bar Association Journal, (73), 2007)
<http://tbbdergisi.barobirlik.org.tr/m2007-73-373.> accessed 26 February 2021.

[532] Murat Kandemir, Didem Yardimcioglu, 'Equality Principle in Labor Law' (2014) Dicle University Faculty of Law Journal, 19 (30-31)
<https://dergipark.org.tr/en/download/article-file/214048> accessed 27 February 2021.

reasons. Unfortunately, discrimination that minorities may face at the time of employment is excluded from the scope of the article. For this reason, only the people in employment will benefit from the protection of the article. Article 122 of the TCL, on the other hand, punishes certain actions made before the emergence of a business relationship.

6.3. Judicial Review

Victims of the discrimination can file a lawsuit subjected to general provisions within the frame of the Criminal Procedure Code numbered 5271, the Code of Civil Procedure numbered 6100, and the Administrative Judicial Procedure Law numbered 2577. Restorative justice mechanisms that offer non-judicial remedies such as alternative dispute resolution or mediation are very limited in this sense. Since a discrimination offence in criminal proceedings is not regulated as an offence subject to a complaint, a compromise process cannot be carried out.

However, victims of discrimination may demand compensation for their financial damages, deprived earnings, or moral damages arising from their intense pain, or all the remedies having been mentioned above. It is also possible that said criminal, civil or administrative proceedings could take place at the same time. For instance, while victims can simultaneously file a lawsuit for compensation in civil or labour courts, they also have the right to make a complaint about administrative implications or criminal investigation. According to Article 125 of the Constitution, the judicial remedy is available against all acts and proceedings of the administration. Therefore, the administration is obliged to pay for the damage arising from its actions and proceedings. In administrative acts, if an act is considered to be contrary to law by the administrative court, the court may revoke the act and/or rule for indemnity. In the case that the court refuses the application, the applicant must file a lawsuit in the administrative courts within 60 days from the date of refusal. There is also a period of limitation in such cases. Regarding damage, the burden of proof is on the plaintiff in administrative cases. Since the trials are heard through the file, there is no way that the administrative courts hear witnesses. Cases that have been brought before administrative courts are examined by the Council of State upon appeal.

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?

Turkey does not have specific regulations regarding the liability deriving from the development or the usage of Advanced Digital Technologies, such as AI applications, IoT, autonomous weapon systems or autonomous vehicles. However, the above-mentioned data protection legislation[533] has a direct legal impact on the usage of advanced technologies.

Turkey's Digital Transformation Office was established by Presidential Decree No. 1 in 2018, under the Presidency as a public entity with a private budget. The Digital Transformation Office has many competencies, including preparing a road map for digital

[533] ibid.

transformation in the public sector, developing projects for improving information security and cybersecurity, developing strategies for effective use of big data and advanced analysis solutions in the public sector, leading respective implementations and providing coordination, and leading artificial intelligence applications in the public sector with regard to prioritized project areas, and providing coordination.

The Digital Transformation Office has a department dedicated to Big Data and Artificial Intelligence Applications. Competencies of the Department include developing strategies and providing coordination for enabling the effective use of big data and artificial intelligence applications in the public sector, supporting projects and activities necessary for developing big data technologies in the public sector, leading artificial intelligence applications in the prioritized project fields and carrying out big data analytics, security and privacy activities. The Department is also responsible for developing strategies and providing coordination about national-level open data and establishing and running the national Open Data Portal for sharing public data, and determining the procedures, principles and standards on data transfer by public institutions to the Portal.

According to the recent Turkish National Cyber Security Strategic Report, some legislative initiatives might be introduced in the coming years on cybersecurity certification, children's data protection, limiting cross border transfers of Turkish nationals' data. Furthermore, the security criteria of new generation technologies such as artificial intelligence, the Internet of things, blockchain and 5G will be a priority in cybersecurity planning in the near future.[534]

7.1. To what extent are the external legislative developments influential on your country's regulation of this area?

First of all, international agreements, especially the provisions of international law concerning fundamental rights and freedoms, influence Turkish law to a great extent. According to the last sentence of Article 90 of the Constitution: 'International agreements duly put into effect have the force of law. No appeal to the Constitutional Court shall be made with regard to these agreements on the grounds that they are unconstitutional. (Sentence added on 7 May 2004; Act No. 5170) *'In the case of a conflict between international agreements, duly put into effect, concerning fundamental rights and freedoms and the laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail.'*[535]

The Republic of Turkey signed the European Convention on Human Rights in 1950, and it came into force in 1954. In this regard, the judgements of the European Court of Human Rights and the Council of Europe's duly ratified Conventions must be taken into consideration as a national legal tool. The provisions of the Conventions that concern

[534] *'T.C. Ulaştırma ve Altyapı Bakanlığı, Türkiye Cumhuriyeti Ulusal Siber Güvenlik Stratejisi'* (2020-2023), <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/NationalCybersecurityStrategyOfTURKEY.pdf> accessed 1 March 2021.
[535] Constitution of the Republic of Turkey.

fundamental rights and freedoms have great legal importance for Turkey and are considered above domestic laws but below the Constitution. It is significant to note that Turkey is represented at the Council of Europe's ad hoc Committee on Artificial Intelligence (CAHAI).

European Union law influences Turkish law, too, as Turkey is an accession country undergoing the harmonization process. The European Union recently took significant steps to regulate data, starting with the GDPR. The European Union's goal of creating a Single Data Market to ensure data interoperability and the robustness of data sets is likely to influence Turkey as a neighbour and a significant trade partner. The European Union's draft AI regulation, too, is likely to have an influence for the same reason, once adopted by the EU.

The European Union's White Paper on AI is a significant document, followed by the Data Governance Act presented in 2020, which touches upon the reuse of sensitive public data, such as health data from public hospitals, which may be influential for Turkey, too. The European Union's Data Act presented in 2021, which aims to increase fairness in the European Union's data economy, improve data portability rights and review the intellectual property rights framework, is also likely to be a guide for Turkey as an accession country.

The influence of the European Union on Turkey may also be seen from Turkey's E-commerce Law No. 6563, which entered into force in 2015 and is compliant with the European Union's E-Commerce Code. The European Union is currently updating its e-Commerce Code with the Digital Services Act and the Digital Markets Act, and these new legislations will bring significant changes to online platforms which have their business model on collecting and processing data. It is likely that Turkey would bring measures similar to those of the European Union in the future, especially regarding big data and algorithms.

Turkey is also one of the 37 members of the Organisation for Economic Co-operation and Development (OECD), which has initiatives on AI, including the Global Partnership on Artificial Intelligence (GPAI) and the Going Digital project. Turkey is part of OECD's Going Digital Horizontal Project, which helps policymakers understand how digital transformation impacts the economy and society. The project aims to reduce the gap between technology and political development, to provide policymakers with the tools they needed to develop a whole-of-government approach and to advance the measurement of digital transformation.

Furthermore, OECD AI Principles aim to promote responsible stewardship of trustworthy AI, which includes human-centred values, fairness, transparency, robustness, security, safety, and accountability. As a member state, Turkey benefits from OECD's collaborative, multi-stakeholder, interdisciplinary approach. OECD, as an organization, also participates in international initiatives, such as those of the Council of Europe.

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

The increase in technological advancements over the last decades has made it necessary to adopt regulations that provide clear and effective protection of data. Regulations concerning data privacy arising from this need are fairly new all around the world, and Turkey is no exception.[536] Personal Data Protection Law No. 6698 came into effect very recently in 2016. The Constitution of the Republic of Turkey No. 2709 and the Turkish Penal Code No.5237 included provisions to protect the data privacy of individuals before the PDPL entered into force. However, this protection was not sufficient. Data privacy of individuals was protected under Articles 132-140, Part 9, 'Offences Against Privacy and Confidentiality' of the Turkish Penal Code. Article 135 para 1 of TPC provides that unlawfully recording personal data is a crime punishable by imprisonment from one to three years. Illegally obtaining or giving data and destruction of data also constitute crimes as disclosed in Articles 136 and 138.

The 'right to protect personal data' was constitutionally regulated for the first time when Article 20 of the Turkish Constitution governing the 'Privacy of the Individual's Life' was amended in 2010. The added paragraph states that everyone can request that their personal data be protected. Pursuant to this paragraph, individuals may thereby demand to be informed of, have access to and request the correction and deletion of their personal data, and be informed if their personal data has been used in accordance with the intended purpose. The processing of personal data is lawful only when it is envisaged by law, or the individual has given explicit consent. With this provision, the 'right to protect personal data' has been recognized as a fundamental right.[537]

When the Personal Data Protection Law came into force, it did not include penal provisions. Instead, Article 17 of PDPL refers to the relevant provisions (135-140) of the TPC. Thus, if there is a personal data offence in question, the provisions of the TPC will be applied.[538]

Article 12 para 1 of the PDPL states that the data controller has an obligation to take all necessary technical and organizational measures for providing an appropriate level of security to prevent unlawful processing of and access to personal data and safeguard it. Encryption is included among the technical measures described in the Personal Data Security Guideline of the Board. Accordingly, encryption of personal messages must be provided by the controllers pursuant to Article 12 of the PDPL.[539] Although this is the general rule, the decryption of personal messages might be considered lawful and therefore be required under certain circumstances. With the conditions of being relevant and

[536] Oğulcan Özkan, *'Kişisel Verilerin Korunması'* (MSc thesis, Ankara University 2020), 40-43.
[537] ibid. 79-82.
[538] ibid. 241-243.
[539] Turkish Data Protection Board, *'Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'* p 20-28.

proportionate to the purpose and general principles of the PDPL, if it is necessary to process personal data for crime prevention and investigation, personal messages can be decrypted. Article 28 para 2 of the PDPL explains that in the processing of personal data where it is necessary to prevent crime or investigate a crime, provided that it is relevant and proportionate to the purpose and general principles of PDPL, Article 10 regulates the obligation of the data controller to inform; except for the right to request compensation, Article 11 which regulates the rights of the data subject; and Article 16 which regulates the obligation to register with the Data Controllers Registry will not apply.

8.1. The circumstances in which decryption may be conducted and the potential or real consequences of such requirement

When communicating via e-mail or instant messaging, personal messages should be kept private between only the sender and the intended receiver, and no one else should be able to read these messages.[540]

The WP29 allows countries to adopt legislation to protect national security by processing personal data through surveillance measures. Since the 'Guarantees' derive from the jurisprudence of the CJEU and the ECtHR, they apply in and to Turkey as a Member State of the Council of Europe when applying legislation interfering with the fundamental rights to privacy and data protection. Given that data needs to be protected continuously during transfers, the Guarantees need to be taken into consideration when transferring data from the EU to third countries, such as Turkey. The four European Essential Guarantees are as follows:

— Processing should be based on clear, precise and accessible rules,

— Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated,

— An independent oversight mechanism should exist, and

— Effective remedies need to be available to the individual.[541]

Article 22 of the Constitution governing the freedom of communication ensures that the privacy of communication is fundamental. Communication cannot be impeded, or privacy of communication cannot be violated with the exception of a decision duly given by a judge or a written order of an agency authorized by law — in cases where delay is prejudicial — for purposes of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others.[542]

---

[540] Iraklis Symeonidis and Gabriele Lenzini, 'Systematisation of Threats and Requirements for Private Messaging with Untrusted Servers: The Case of E-mailing and Instant Messaging' (International Conference on Information Systems Security and Privacy, Malta, February 2020).

[541] Article 29 Working Party, 'Opinion 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)' (WP 237, 13 April 2016), 1-6.

[542] The Constitution of the Republic of Turkey No. 2709, 22(2).

8.2. Power of decryption of the authorized body

Big Tech companies such as Facebook and Google have extensive access to millions of users' data. The power these companies have over individuals raises privacy concerns. The practices of these companies endanger the confidentiality of data and restrict users' ability to control what the services are doing on their devices.

Cryptography is an important tool that offers secure communication. When applied correctly, no one else should be able to decrypt messages between the sender and the receiver. However, crypto can be switched off unbeknownst to the user; hence he will not be able to seek legal remedies for the lawfulness review of the decryption. Legislation allowing the implementation of surveillance measures, i.e., decryption, gives too much power and control to Big Tech and the authorized body over individuals.[543]

Interfering with the privacy of individuals excessively would restrict persons from sharing their opinions freely and cause a chilling effect, especially on abuse and violence victims. This would also lead to a lack of autonomy. States have an obligation to guarantee individuals that their messages and e-mails will be received only by their intended recipient and that the communication will not be interfered with by the authorities of the State or any third party.[544]

8.3. Level of protection the Turkish legislation provides to the individuals

Under the Turkish Administrative Law, the persons concerned may apply to the Administrative Court for the annulment of an administrative procedure when the procedure is unlawful. If the individual is harmed by this procedure, he can claim compensation.[545] If the Court does not declare the procedure unlawful and rules not in favour of the individual, he retains the right to make an individual application to the Constitutional Court.

According to Article 139 of TPC, individuals have a right to lodge a complaint when their personal messages are unlawfully decrypted. Article 132 para 1 states that while the violation of the secrecy of communication is punishable by imprisonment from one to three years; if this violation occurs through recording, the punishment will be increased by one-fold.

[543] Seda Gürses and Bart Preneel, 'Cryptology and Privacy in the Context of Big Data' in Bart van der Sloot, Dennis Broeders and Erik Schrijver (eds), *Exploring the Boundaries of Big Data,* Amsterdam University Press (Amsterdam, 2016).

[544] Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' UNGA 23rd Session A/HRC/23/40 (2013) paras 23-24.

[545] Procedure of Administrative Justice Act No. 2577.

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

Some believed that there have been three leaps throughout history that human beings have experienced, namely, cognitive revolution, agricultural revolution, and the industrial revolution. Each of them is basically considered to be the most important breakthrough in modern human history. We would be wrong if we thought that they are all a thing of the past because today's foundations lay on them in every way. Thanks to those advancements, recently, we have been living in an era shaped by new cutting-edge technologies such as the Internet of things, AI, robotics, and nanotechnology. Of these, Digitalization, also known as the Digital Revolution, has been taking up too much space for the last decade in our lives. Digitalization is, without doubt, the most significant spread of information since the invention of the printing press, which led to drastic changes in society, so it was one of the key factors that brought about the Renaissance movements, according to prominent historians. Digital transformation is about using digital tools and applications more effectively to improve business agility, productivity and performance.[546]

As it is known, nothing is perfect, so any change or development comes at a price. That is, such improvements cause some challenges needed to be met. In general, digital adoption is the main challenge ahead of this transition period to the new Digital Era. In order to overcome these challenges, first of all, these challenges need to be detected and worked on according to the needs of the public, as well as the market, to keep the society functioning as much as possible; and of course, certain actions should be executed not only by the governments but also by international conventions and domestic legislation in cooperation with the civil society as well.

Following every ground-breaking paradigm shift, it is inevitable that the need for legal arrangements does become the main topic of the conversations. As mentioned above, the Fourth Industrial Revolution changes the way how we live and communicate with each other in an unprecedented way, and there is a decent chance to somewhat adversely affect human rights as well. Firstly, the use of AI and automation have already had an impact on the job markets due to the fact that they are capable of working better than humans. Experts estimate that by 2020, 85% of all customer interactions will be handled without a human agent with the help of chatbots and self-service technologies. Data is the key factor for this change. However, data still possess some humanistic flaws and mistakes such as bias, discrimination, and prejudice. Secondly, access to the Internet and the right to freedom of expression have been interrupted because of the governments' internet crackdowns. The United Nations once said that governments around the globe imposed various bans on the Internet roughly 50 times in 2016 for fear of fake news. This problem should not be underestimated as there are as many as 3 billion internet users around the

[546] Ouritdept.co.uk, 'What is Digital Transformation?'
<https://www.ouritdept.co.uk/what-is-digital-transformation/> accessed 28 February 2021.

world. Yet, along with this excuse, whether or not it is legitimate, this censorship wreak havoc on politics and human rights without a doubt. Lastly, due to the Internet of Things, there has been an imminent threat that a lot of private information and data could become public without the discretion of the owners. According to Business Insider, the number of devices which will be hooked up to the Internet will be as many as 34 billion, and all of them will be able to track personal data.

Science, technology, and development have been at the very centre of people's interests since the age of discovery. In addition, with the industrial revolution, human progress picked up such a pace that had never been before. In the meantime, human rights have always been the case since individual rights become more and more important. From the human rights perspective, the main issue was how human rights should keep up with scientific and technological developments. There is no consensus on how to deal with this challenge, so there are some varying approaches, attempts and thoughts about what to do. However, in *S. and Marper v. the United Kingdom*[547] verdict, the European Court of Human Rights used a term called '*striking a fair balance*' referring to a fine line between the competing public and private interests. In this case, after applicants were charged with a crime, their fingerprints and DNAs were taken. Although they were acquitted at the end of the trial, they asked for their fingerprints and DNA samples to be destroyed, but they were refused. For this reason, the European Court of Human Rights decided that even though the retention of these private data pursued the legitimate purpose of the detection and prevention of crime, there was a violation of Article 8 of the European Convention on Human Rights due to the fact that applicants were just suspects. Also, in the justification, the Court stated that the retention was not time limited. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed. Accordingly, the retention at issue constituted a disproportionate interference with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society.[548] It is clear that with this landmark decision, the Court indicates that there are certain criteria that need to be followed when it comes to interference in private life under Article 8 of the Convention.

A human rights-based approach seems to have been adopted by United Nations to maintain the balance between digital interventions and human rights. Although there is no agreed definition on this approach, in practice, there are certain principles that put the international human rights entitlements, claims of people - *the right-holders*- and the corresponding obligations of the state - *the duty-bearer* - in the centre of the national development debate, and it clarifies the purpose of capacity development. [549]Those principles emphasized by The United Nations Development Programme appear when facing any gender bias, discrimination or misuse of science and technology.

---

[547] *S. and Marper v United Kingdom* [2008] ECHR 1581.
[548] <https://justice.org.uk/s-marper-v-uk-2008/> accessed 28 February 2021.
[549] <https://www.scidev.net/global/features/linking-science-and-human-rights-facts-and-figures/> accessed 28 February 2021.

When it comes to science and technology, according to this approach, scientists are expected to do certain things and make value judgments while doing their profession. Science and technology have reached such a level that cause some major concerns for society, such as the developments in the fields of nanotechnology, tracking technology or geospatial technologies. In other words, besides their main duty, scientists are expected to take human rights into consideration as well. The above-mentioned ethical view could also clearly be seen in some International Declarations and Covenants.

Article 27 of the Universal Declaration of Human Rights guarantee that everyone has the right to be part of the scientific developments and benefit from them. Although scientific advancements and their benefits are considered to be part of cultural life, the World Commission of the Ethics of Scientific Knowledge and Technology (COMEST), an independent advisory body of UNESCO, is assessing the implications of Article 27 in relation to science and technology ethics.

In 2005, UNESCO issued a declaration with regards to ethical matters resulting from modern science. The declaration briefly underlines how to make a law that deals with ethical concerns and human rights in science and technology. The main concern of the declaration is that the wellbeing of the individuals is supposed to be on top priority besides the interests of governments or society. Therefore, the declaration also stresses that just having prior informed consent from the community or third parties in scientific research does not mean that there is no need to get the consent of the individual. Also, it clearly explains that access to scientific and technological information should be provided by the governments that urge the share and circulation of scientific information. The declaration also advises governments to form ethic committees to keep track of the ethical and human rights issues in the fields of science. According to the director of UNESCO's division of ethics of science and technology, Henk ten Have 'it was the first document that comprises these issues in the same document'.

Other than the international efforts concerning human rights matters and ethics in the digitalized world, there are also nationwide efforts as well. In order to embrace the recent digital developments and improvements, some countries already developed and released a method called 'National Artificial Intelligence Strategy' to make a long-standing plan.

Even though Turkey has no National Artificial Intelligence Strategy yet, in 2020, National Artificial Intelligence Strategy Preliminary Report was published. In brief, some suggestions were listed regarding the usage of artificial intelligence in many areas such as education, industry, and everyday life. In parallel with the developing technologies, social demands and reform trends in the public sector, Digital Transformation Office was established on 10 July 2018 in order to collect the studies on digital transformation (e-Government), cybersecurity, national technologies, big data and artificial intelligence,

which are carried out separately under different institutions. [550] Within the scope of the Presidential Decree, various service units of the Digital Transformation Office have been set up. [551]

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?

Turkey, as a member of the Council of Europe, accepts that human rights are the same online and offline. In this respect, all human rights have better protection online in the next five years, starting with the freedom of expression and the right to non-discrimination. Turkey recently brought a new Social Media regulation that aims to overcome difficulties and to hold social network providers accountable towards applications made by public bodies and Internet users. The Law on the Amendment of Law No.5651 on Regulation of Publications on The Internet and Combating Crimes Committed by Means of Such Publication, in its preamble, referred to a Constitutional Court decision that online platforms need to be held accountable in fighting against illegal content, together with governments. With the new law, illegal content on social platforms may be extracted where possible instead of a complete block on access to the platform. In this respect, Turkey may introduce new regulations regarding the responsibilities of online platforms in the near future to safeguard the freedom of speech and to prevent hate speech. Furthermore, the power of algorithms in influencing user behaviour in democratic processes is not to be undermined. Turkey might also introduce new legislation to regulate algorithms. In this respect, it is essential that the law of the European Union influences Turkey, and it will influence Turkey in the next five years as an accession country.

Turkey has still not yet signed the Council of Europe Convention 108+, which is a significant tool for the protection of individuals with regard to the processing of personal data. In the next five years, one might observe new steps in this respect. Furthermore, as enforcement means as much as the legislation itself, the enforcement of the provisions of KVKK remains a priority. As a ground for protecting other human rights online, the right to privacy will gain higher importance. In the coming five years, we will be witnessing a more connected world thanks to the Fifth Generation Communication Technologies (5G), enabling the Internet of Things which will entail more connected devices and the super increase in the flow of data, which brings the question whether the GDPR or KVKK will be able to suffice legal protection of data. As Wachter underlined, since this data protection legislation is focused only on the procedure 'after' the data is collected, this legal scope will be inadequate.

[550] <https://www.resmigazete.gov.tr/eskiler/2018/07/20180710-1.pdf> accessed 28 February 2021.
[551] Cbddo.gov.tr, 'About Us', <https://cbddo.gov.tr/hakkimizda/> accessed 28 February 2021.

The Digital Transformation Office of Turkey has goals such as improving information security and cybersecurity, developing strategies for effective use of big data and advanced analysis solutions in the public sector, leading artificial intelligence applications in the public sector with regard to prioritized project areas. The recent Turkish National Cyber Security Strategic Report stated some legislative initiatives might be introduced in the coming years on cybersecurity certification, children's data protection, limiting cross border transfers of Turkish nationals' data. Furthermore, the security criteria of new generation technologies such as artificial intelligence, the Internet of things, blockchain and 5G will be a priority in cybersecurity planning in the near future. Internet of things systems is to erase the barriers between personal and non-personal data. Therefore, the legislative frameworks focusing only on personal data will become insufficient. Towards 2030, when 6G technology will transform the Internet of Things to the Internet of Smart Things, the human body will be a part of the network as well[552]. Cyber-physical areas will erase the barriers between what is private and what is public; security and privacy gaps in the cyber domain will have greater impacts on the physical domain. In order to be able to protect human rights, the legal framework must first estimate the legal scope of data to define it as a property right or an integral part of being a human. Cybersecurity, big data and artificial intelligence are all areas that are closely linked with human rights. As Turkey aims to bring legislations in these areas of technology in the future, one would expect to see provisions to safeguard the freedom of thought, privacy rights and the right to non-discrimination to complement the law.

Furthermore, women's rights and children's rights remain priorities that need to be underlined. Women, as it can be seen from the pandemic, are vulnerable to human rights breaches, and the effective implementation of the Council of Europe's Istanbul Convention[553] is more significant than ever to provide adequate protection against the new dangers introduced by technology. Children's right to education, in this context, is a crucial point for society. Right to non-discrimination and the protection of children's data needs to be safeguarded better than ever. In its Guidelines on Children's Data Protection in an Education Setting, the Council of Europe underlines the fact that the expansion of educational technology can mean non-state actors routinely control children's educational records. To provide adequate protection of human rights, effective and clear legal protection shall be provided with digital literacy on privacy and security awareness.

Lastly, it is significant to underline the significance of European Union law on Turkish law, as Turkey an accession country with an undergoing harmonization process. Turkey is expected to harmonize its laws with the European Union in regulating AI, too, when the draft AI regulation gets adopted by the European Union.

---

[552] Ylianttila, Mika; Kantola, Raimo; Gurtov, Andrei vd.: *6G White Paper: Research Challenges for Trust, Security and Privacy*, (Oulu University, Oulu, 2020) p. 16.
[553] For an analysis of Turkey's announced withdrawal, see: https://www.ejiltalk.org/withdrawal-from-the-istanbul-convention-by-turkey-a-testing-problem-for-the-council-of-europe/ accessed 28 February 2021.

Conclusion

Turkey, with its population of 80 million, the majority consisting of young people, is a great consumer of newer technology, the Internet and social media. According to the DataReportal's Digital 2020 report, Turkey had 62 million Internet users by January 2020. There is a high chance that the number is much higher today due to the current pandemic, which forces all to study/work at home.

With that high ratio of internet and technology use, it is impossible to ignore the risks of unauthorized storage and processing of personal data. Seeing all these changes and developments in the world regarding the use of technology, Turkey realized the importance of regulating technology law in the scope of human rights.

In 2010, Law Regarding the Constitutional Amendment No. 5982 has entered into the force and added a new sub-article to article 20, Right to Privacy. According to the 20/3 of the Constitution, everyone has the right to request the protection of his/her personal data.

Until April 2020, data privacy was only regulated by the article mentioned above of the Constitution and few articles of the Turkish Penal Code. With the enaction of Law on the Protection of Personal Data No. 6698 (*KVKK*), Turkey finally had a main national legislation regarding protecting personal data and the right to privacy of persons.

Concerning all these amendments and regulations and their compliance with EU regulations, it is safe to point out that Turkey took some important steps to regulate the impact of technology developments on human rights, but has some things to improve as well.

Table of legislation

Provision in Turkish language	Corresponding translation in English
1 Sayılı Cumhurbaşkanlığı Kararnamesi: MADDE 527- (Başlığı ile Birlikte Değişik: RG24/10/2019-30928-CK-48/9 md.) (1) Dijital Dönüşüm Ofisinin görevleri şunlardır: a) Cumhurbaşkanı tarafından belirlenen amaç, politika ve stratejilere uygun olarak kamunun dijital dönüşümüne öncülük etmek, Dijital Türkiye (e-devlet) hizmetlerinin sunumuna aracılık etmek, kurumlar arası işbirliğini artırmak ve bu alanlarda koordinasyonu sağlamak. (1) 24/10/2019 tarihli ve 30928 sayılı Resmî Gazete'de yayımlanan 48 sayılı Cumhurbaşkanlığı Kararnamesinin 6 ncı maddesiyle bu Kararnameye Yedinci Kısmının 'Cumhurbaşkanlığı Ofisleri' başlığından sonra gelmek üzere 'Birinci Bölüm' bölüm numarası ve 'Kuruluş ve Tanımlar' bölüm başlığı eklenmiştir. (2) 24/10/2019 tarihli ve 30928 sayılı Resmî Gazete'de yayımlanan 48 sayılı Cumhurbaşkanlığı Kararnamesinin 9 uncu maddesiyle bu Kararnameye 526 ncı maddesinden sonra gelmek üzere ' İkinci Bölüm' bölüm numarası ve 'Dijital Dönüşüm Ofisi' bölüm başlığı eklenmiştir. b) Kamu dijital dönüşüm yol haritasını hazırlamak. c) Dijital dönüşüm ekosistemini oluşturmak amacıyla kamu, özel sektör, üniversiteler ve sivil toplum kuruluşları arasındaki işbirliğini geliştirerek bunların dijital kamu hizmetlerinin tasarım ve sunum sürecine katılımını teşvik etmek. ç) Görev alanına giren hususlarda kamu kurum ve kuruluşlarınca hazırlanan yatırım	Presidential Decree No. 1: ARTICLE 527- (Amended with Title: OG-24/10/2019-30928-PD-48/9 art.) (1) The duties of the Digital Transformation Office are as follows: a) Leading the digital transformation of the public sector in compliance with the goals, policies and strategies determined by the President, mediating the delivery of Digital Turkey (e-government) services, enhancing inter-institutional cooperation and providing coordination in these fields. (1) Pursuant to Article 6 of the Presidential Decree No. 48 published in the Official Gazette no. 30928 dated October 24, 2019, chapter no. 'Chapter One' and the chapter title 'Establishment and Definitions' have been added to this Decree following the title 'Presidential Offices' of Section Seven. (2) Pursuant to Article 9 of the Presidential Decree No. 48 published in the Official Gazette no. 30928 dated October 24, 2019, chapter no. 'Chapter Two' and the chapter title 'Digital Transformation Office' have been added to this Decree following Article 526. b) Preparing a road map for digital transformation in the public sector. c) For the aim of creating an ecosystem for digital transformation; enhancing cooperation among the public sector, private sector, universities and non-governmental organizations, and promoting their participation in the design and presentation of digital public services. ç) Providing opinion to the Strategy and Budget Directorate with regard to investment project proposals prepared by public

projesi tekliflerine ilişkin Strateji ve Bütçe Başkanlığına görüş vermek ve uygulamaya konan projelerle ilgili gelişmeleri takip edip gerektiğinde yönlendirmek. d) Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek. e) Kamuda büyük veri ve gelişmiş analiz çözümlerinin etkin kullanımına yönelik stratejiler geliştirmek, uygulamalara öncülük etmek ve koordinasyonu sağlamak. f) Kamuda öncelikli proje alanlarında yapay zekâ uygulamalarına öncülük etmek ve koordinasyonu sağlamak. g) Yerli ve milli dijital teknolojilerin kamuda kullanımının artırılması yoluyla geliştirilmesi ve bu kapsamda farkındalık oluşturulması amacıyla projeler geliştirmek. ğ) Kamu kurum ve kuruluşlarının dijital teknoloji ürün ve hizmetlerini maliyet etkin şekilde tedarik etmesine yönelik strateji belirlemek. h) Görev alanına ilişkin proje ve uygulamalara gerektiğinde destek sağlamak. ı) Devlet teşkilatı içerisinde yer alan kurum ve kuruluşların merkez, taşra ve yurtdışı teşkilat birimlerinin elektronik ortamda tanımlanmasına ve paylaşılmasına yönelik çalışmaları koordine etmek. i) Görev alanına giren konularda politika ve strateji önerilerinde bulunmak. j) Cumhurbaşkanınca verilen diğer görevleri yapmak.	institutions and organizations in matters related to its field of duties, and following up and directing where necessary the developments on the projects put into practice. d) Developing projects for improving information security and cyber security. e) Developing strategies for effective use of big data and advanced analysis solutions in the public sector, leading respective implementations and providing coordination. f) Leading artificial intelligence applications in the public sector with regard to prioritized project areas, and providing coordination. g) Developing projects for improving local and national digital technologies by enhancing their use in the public sector and for building awareness in this regard. ğ) Identifying a strategy for the procurement of digital technology products and services by public institutions and organizations in a cost-effective manner. h) Providing support where necessary to projects and implementations related to its field of duties. ı) Coordinating the definition and sharing in an electronic medium of central, rural and foreign organizational units of those institutions and organizations involved within the state organization. i) Proposing policies and strategies in matters related to its field of duties. j) Performing other duties assigned by the President.
30356 sayılı Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ Başvuru Usulü: Madde 5-(1) İlgili kişi, Kanunun 11 inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza,	Communiqué on Application Procedures and Principles to the Data Controller No.30356 Application Procedure: Article 5-(1) The person concerned may request his / her requests within the scope of the rights specified in Article 11 of the Law in written or registered electronic mail (KEP)

mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir. (2) Başvuruda; a) Ad, soyad ve başvuru yazılı ise imza, b) Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, c) Tebligata esas yerleşim yeri veya iş yeri adresi, ç) Varsa bildirime esas elektronik posta adresi, telefon ve faks numarası, d) Talep konusu, bulunması zorunludur. (3) Konuya ilişkin bilgi ve belgeler başvuruya eklenir. (4) Yazılı başvurularda, veri sorumlusuna veya temsilcisine evrakın tebliğ edildiği tarih, başvuru tarihidir. (5) Diğer yöntemlerle yapılan başvurularda; başvurunun veri sorumlusuna ulaştığı tarih, başvuru tarihidir.	address, secure electronic signature, mobile signature or the electronic mail address previously notified to the data controller and registered in the data controller's system by the person concerned. to the data controller by using the software or by means of a software or application developed for the purpose of application. (2) In the application; a) Name, surname and signature, if application is in writing, b) For the citizens of the Republic of Turkey T. C. identification number, nationality for foreigners, passport number or identification number, if any, c) Place of residence or workplace address for notification, ç) E-mail address, telephone and fax number for notification, if any, d) Subject of the request, must be found. (3) Information and documents related to the subject are attached to the application. (4) In written applications, the date on which the document is served to the data controller or its representative is the application date. (5) In applications made by other methods; the date the application reaches the data controller is the application date.
30356 sayılı Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ: Madde 6- (1) Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür. (2) Veri sorumlusu, başvuruyu kabul eder veya gerekçesini açıklayarak reddeder. (3) Veri sorumlusu, cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir.	Communiqué on Application Procedures and Principles to the Data Controller No.30356 Response to the application: Article 6-(1) The data controller is obliged to take all necessary administrative and technical measures to finalize the applications made by the person concerned within the scope of this Communiqué in an effective manner and in accordance with the law and the rule of honesty. (2) The data controller accepts the application or rejects it by explaining the reason.

(4) Cevap yazısının; a) Veri sorumlusu veya temsilcisine ait bilgileri, b) Başvuru sahibinin; adı ve soyadını, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarasını, yabancılar için uyruğunu, pasaport numarasını veya varsa kimlik numarasını, tebligata esas yerleşim yeri veya iş yeri adresini, varsa bildirime esas elektronik posta adresini, telefon ve faks numarasını, c) Talep konusunu, ç) Veri sorumlusunun başvuruya ilişkin açıklamalarını, içermesi zorunludur. (5) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyet gerektirmesi hâlinde, 7 nci maddede belirtilen ücret alınabilir. Başvurunun, veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir. (6) İlgili kişinin talebinin kabul edilmesi hâlinde, veri sorumlusunca talebin gereği en kısa sürede yerine getirilir ve ilgili kişiye bilgi verilir.	(3) The data controller informs the relevant person in writing or electronically. (4) The reply letter must contain; a) Information of the data controller or representative, b) The applicant's; name and surname, for the citizens of the Republic of Turkey T. C. identification number, nationality for foreigners, passport number or identification number, if any, place of residence or workplace for notification, e-mail address for notification, telephone and fax number, if any, c) The subject of the request, ç) The explanations of the data controller regarding the application, (5) The data controller finalizes the requests in the application free of charge as soon as possible and within thirty days at the latest, depending on the nature of the request. However, if the transaction requires an additional cost, the fee specified in Article 7 may be charged. In case the application is caused by the error of the data controller, the fee received will be refunded to the person concerned. (6) In case the request of the relevant person is accepted, the requirement of the request is fulfilled by the data controller as soon as possible and the relevant person is informed.

Title of the legal act	**Provision text in English language**
Labour Act of Turkey Law No. 4857, Article 4	The provisions of this Act shall not apply to the activities and employment relationships mentioned below. a. Sea and air transport activities, b. In establishments and enterprises employing a minimum of 50 employees (50 included) where agricultural and forestry work is carried out.

	c. Any construction work related to agriculture which falls within the scope of family economy, d. In works and handicrafts performed in the home without any outside help by members of the family or close relatives up to 3 rd degree (3 rd degree included), e. Domestic services, f. Apprentices, without prejudice to the provisions on occupational health and safety, g. Sportsmen, h. Those undergoing rehabilitation, i. Establishments employing three or fewer employees and falling within the definition given in Article 2 of the Tradesmen and Small Handicrafts Act, However, the following shall be subject to this Act; a. Loading and unloading operations to and from ships at ports and landing stages, b. All ground activities related to air transport, c. Agricultural crafts and activities in workshops and factories manufacturing implements, machinery and spare parts for use in agricultural operations, d. Construction work in agricultural establishments, e. Work performed in parks and gardens open to the public or subsidiary to any establishment, f. Work by seafood producers whose activities are not covered by the Maritime Labour Act and not deemed to be agricultural work.
Labour Act of Turkey Law No. 4857, Article 5	No discrimination based on language, race, sex, political opinion, philosophical belief, religion and sex or similar reasons is permissible in the employment relationship. Unless there are essential reasons for differential treatment, the employer must not make any discrimination between a full-time

	and a part-time employee or an employee working under a fixed-term employment contract (contract made for a definite period) and one working under an open-ended employment contract (contract made for an indefinite period). Except for biological reasons or reasons related to the nature of the job, the employer must not make any discrimination, either directly or indirectly, against an employee in the conclusion, conditions, execution and termination of his (her) employment contract due to the employee's sex or maternity. Differential remuneration for similar jobs or for work of equal value is not permissible. Application of special protective provisions due to the employee's sex shall not justify paying him (her) a lower wage. If the employer violates the above provisions in the execution or termination of the employment relationship, the employee may demand compensation up his (her) four months' wages plus other claims of which he (she) has been deprived. Article 31 of the Trade Unions Act is reserved. While the provisions of Article 20 are reserved, the burden of proof in regard to the violation of the above – stated provisions by the employer rests on the employee. However, if the employee shows a strong likelihood of such a violation, the burden of proof that the alleged violation has not materialised shall rest on the employer.
Labour Act of Turkey Law No. 4857, Article 18	The employer, who terminates the contract of an employee engaged for an indefinite period, who is employed in an establishment with thirty or more workers and who meets a minimum seniority of six months, must depend on a valid reason for such termination connected with the capacity or

	conduct of the employee or based on the operational requirements of the establishment or service. In the computation of the six-months' seniority, time periods enumerated in Article 66 shall be taken into account. The following, inter alia, shall not constitute a valid reason for termination: a. union membership or participation in union activities outside working hours or, with the consent of the employer, within working hours; b. acting or having acted in the capacity of, or seeking office as, a union representative; c. the filing of a complaint or participation in proceedings against an employer involving alleged violations of laws or regulations or recourse to competent administrative or judicial authorities; d. race, colour, sex, marital status, family responsibilities, pregnancy, religion, political opinion, national extraction or social origin; e. absence from work during maternity leave when female workers must not be engaged in work, as foreseen in Article 74; f. temporary absence from work during the waiting period due to illness or accident foreseen in Article 25 of the Labour Act, subsection I (b). The 'six month' minimum seniority (length of service) of the employee shall be calculated on the basis of the sum of his employment periods in one or different establishments of the same employer. In the event the employer has more than one establishment in the same branch of activity, the number of employees shall be determined on the basis of the total number of employees in these establishments. This Article and Articles 19 and 21 and the last subsection of Article 25 shall not be applicable to the employer's representative

	and his assistants authorised to manage the entire enterprise as well as the employers' representative managing the entire establishment but who is also authorised to recruit and to terminate employees.
Constitution of the Republic of Turkey, Article 10	Everyone is equal before the law without distinction as to language, race, colour, sex, political opinion, philosophical belief, religion and sect, or any such grounds. (Paragraph added on May 7, 2004; Act No. 5170) Men and women have equal rights. The State has the obligation to ensure that this equality exists in practice. (Sentence added on September 12, 2010; Act No. 5982) Measures taken for this purpose shall not be interpreted as contrary to the principle of equality. (Paragraph added on September 12, 2010; Act No. 5982) Measures to be taken for children, the elderly, disabled people, widows and orphans of martyrs as well as for the invalid and veterans shall not be considered as violation of the principle of equality. No privilege shall be granted to any individual, family, group or class. State organs and administrative authorities are obliged to act in compliance with the principle of equality before the law in all their proceedings.
Constitution of the Republic of Turkey, Article 20	Everyone has the right to demand respect for his/her private and family life. Privacy of private or family life shall not be violated. (Sentence repealed on May 3, 2001; Act No. 4709) (As amended on October 3, 2001; Act No. 4709) Unless there exists a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others, or unless

	there exists a written order of an agency authorized by law, in cases where delay is prejudicial, again on the above-mentioned grounds, neither the person, nor the private papers, nor belongings of an individual shall be searched nor shall they be seized. The decision of the competent authority shall be submitted for the approval of the judge having jurisdiction within twenty-four hours. The judge shall announce his decision within forty-eight hours from the time of seizure; otherwise, seizure shall automatically be lifted. (Paragraph added on September 12, 2010; Act No. 5982) Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/ her personal data, and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law.
Constitution of the Republic of Turkey, Article 22	(As amended on October 3, 2001; Act No. 4709) Everyone has the freedom of communication. Privacy of communication is fundamental. Unless there exists a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order of an agency authorized by law in cases where delay is prejudicial, again on the abovementioned grounds, communication shall not be impeded nor its privacy be violated. The decision of the

	competent authority shall be submitted for the approval of the judge having jurisdiction within twenty-four hours. The judge shall announce his decision within forty-eight hours from the time of seizure; otherwise, seizure shall be automatically lifted. Public institutions and agencies where exceptions may be applied are prescribed in law.
Constitution of the Republic of Turkey, Article 60	Everyone has the right to social security. The State shall take the necessary measures and establish the organisation for the provision of social security.
Constitution of the Republic of Turkey, Article 68	(As amended on July 23, 1995; Act No. 4121) Citizens have the right to form political parties and duly join and withdraw from them. One must be over eighteen years of age to become a member of a party. Political parties are indispensable elements of democratic political life. Political parties shall be formed without prior permission, and shall pursue their activities in accordance with the provisions set forth in the Constitution and laws. The statutes and programs, as well as the activities of political parties shall not be contrary to the independence of the State, its indivisible integrity with its territory and nation, human rights, the principles of equality and rule of law, sovereignty of the nation, the principles of the democratic and secular republic; they shall not aim to promote or establish class or group dictatorship or dictatorship of any kind, nor shall they incite citizens to crime. Judges and prosecutors, members of higher judicial organs including those of the Court of Accounts, civil servants in public institutions and organizations, other public servants who are not considered to be labourers by virtue of the services they

	perform, members of the armed forces and students who are not yet in higher education, shall not become members of political parties. The membership of the teaching staff at higher education to political parties is regulated by law. This law shall not allow those members to assume responsibilities outside the central organs of the political parties and it also sets forth the regulations which the teaching staff at higher education institutions shall observe as members of political parties in the higher education institutions. The principles concerning the membership of students at higher education to political parties are regulated by law. The State shall provide the political parties with adequate financial means in an equitable manner. The principles regarding aid to political parties, as well as collection of dues and donations are regulated by law.
Constitution of the Republic of Turkey, Article 70	Every Turk has the right to enter public service. No criteria other than the qualifications for the office concerned shall be taken into consideration for recruitment into public service.
Constitution of the Republic of Turkey, Article 74	(As amended on October 3, 2001; Act No. 4709) Citizens and foreigners resident in Turkey, with the condition of observing the principle of reciprocity, have the right to apply in writing to the competent authorities and to the Grand National Assembly of Turkey with regard to the requests and complaints concerning themselves or the public. (As amended on October 3, 2001; Act No. 4709) The result of the application concerning himself/herself shall be made

	known to the petitioner in writing without delay. (Repealed on September 12, 2010; Act No. 5982) (Paragraph added on September 12, 2010; Act No. 5982) Everyone has the right to obtain information and appeal to the Ombudsperson. (Paragraph added on September 12, 2010; Act No. 5982) The Institution of the Ombudsperson established under the Grand National Assembly of Turkey examines complaints on the functioning of the administration. (Paragraph added on September 12, 2010; Act No. 5982) The Chief Ombudsperson shall be elected by the Grand National Assembly of Turkey for a term of four years by secret ballot. In the first two ballots, a two-thirds majority of the total number of members, and in the third ballot an absolute majority of the total number of members shall be required. If an absolute majority cannot be obtained in the third ballot, a fourth ballot shall be held between the two candidates who have received the greatest number of votes in the third ballot; the candidate who receives the greatest number of votes in the fourth ballot shall be elected. (Paragraph added on September 12, 2010; Act No. 5982) The way of exercising these rights referred to in this article, the establishment, duties, functioning of the Ombudsperson Institution and its proceedings after the examination and the procedures and principles regarding the qualifications, elections and personnel rights of the Chief Ombudsperson and ombudspersons shall be laid down in law.
Constitution of the Republic of Turkey, Article 90/5	International agreements duly put into effect have the force of law. No appeal to the

	Constitutional Court shall be made with regard to these agreements, on the grounds that they are unconstitutional. (Sentence added on May 7, 2004; Act No. 5170) In the case of a conflict between international agreements, duly put into effect, concerning fundamental rights and freedoms and the laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail.
Constitution of the Republic of Turkey, Article 125	Recourse to judicial review shall be available against all actions and acts of administration. (Sentences added on August 13, 1999; Act No. 4446) In concession, conditions and contracts concerning public services and national or international arbitration may be suggested to settle the disputes arising from them. Only those disputes involving an element of foreignness may be submitted to international arbitration. (Sentence added on September 12, 2010; Act No. 5982) (As amended on April 16, 2017; Act No. 6771) Recourse to judicial review shall be available against all decisions taken by the Supreme Military Council regarding expulsion from the armed forces except acts regarding promotion and retiring due to lack of tenure. Time limit to file a lawsuit against an administrative act begins from the date of written notification of the act. (As amended on September 12, 2010; Act No. 5982) Judicial power is limited to the review of the legality of administrative actions and acts, and in no case may it be used as a review of expediency. No judicial ruling shall be passed which restricts the exercise of the executive function in accordance with the forms and principles prescribed by law, which has the quality of an

	administrative action and act, or which removes discretionary powers. A justified decision regarding the suspension of execution of an administrative act may be issued, should its implementation result in damages which are difficult or impossible to compensate for and, at the same time, the act would be clearly unlawful. (As amended on April 16, 2017; Act No. 6771) The law may restrict the issuing of an order on suspension of execution of an administrative act in cases of state of emergency, mobilization and state of war, or on the grounds of national security, public order and public health. The administration shall be liable to compensate for damages resulting from its actions and acts.
Turkish Penal Code No.5237, Article 3	(1) Any penalty and security measure imposed upon an offender should be proportionate to the gravity of the crime. (2) In the implementation of the Criminal Code no one shall receive any privilege and there shall be no discrimination against any individual on the basis of their race, language, religion, sect, nationality, colour, gender, political (or other) ideas and thought, philosophical beliefs, ethnic and social background, birth, economic and other social positions.
Turkish Penal Code No.5237, Article 20	(1) Criminal responsibility is personal. No one shall be deemed culpable for the conduct of another. (2) Penalties shall not be imposed on legal entities. However, security measures prescribed by law to be applied to such in respect of a criminal offence shall be reserved.
Turkish Penal Code No.5237, Article 60	(1) Where there has been a conviction in relation to an intentional offence committed for the benefit of a legal entity, which is

	subject to civil law and operating under the license granted by a public institution, by misusing the permission conferred by such license and through the participation of the organs or representatives of the legal entity it shall cancel this license. (2) The provisions relating to confiscation shall also be applicable to civil legal entities in relation to offences committed for the benefit of such entities. (3) Where the application of the provisions in the above paragraphs would lead to more serious consequences than the offence itself, the judge may not impose of such measures. (4) The provisions of this article shall only apply where specifically stated in the law.
Turkish Penal Code No.5237, Article 122	(1) Any person who (a) Prevents the sale, transfer or rental of a movable or immovable property offered to the public, (b) Prevents a person from enjoying services offered to the public, (c) Prevents a person from being recruited for a job, (d) Prevents a person from undertaking an ordinary economic activity on the ground of hatred based on differences of language, race, nationality, colour, gender, disability, political view, philosophical belief, religion or sect shall be sentenced to a penalty of imprisonment for a term of one year to three years.
Turkish Penal Code No.5237, Article 132	(1) Any person who violates the confidentiality of communication between persons shall be sentenced to a penalty of imprisonment of a term of one to three years. If the violation of confidentiality occurs through the recording of the content of the communication, the penalty to be imposed shall be increased by one fold.

	(2) Any person who unlawfully publicizes the contents of a communication between persons shall be sentenced to a penalty of imprisonment for a term of two to five years. (3) Any person who unlawfully discloses the content of a communication between himself and others without obtaining their consent, shall be sentenced to a penalty of imprisonment for a term of one to three years. (Sentence Added on 2 July 2012 – By Article 79 of the Law no. 6352) Where such conversation is published in the press or broadcasted, the penalty to be imposed shall be the same. (4) (Abolished on 2 July 2012 – By Article 79 of the Law no. 6352)
Turkish Penal Code No.5237, Article 134	(1) Any person who violates the privacy of another person's personal life shall be sentenced to a penalty of imprisonment for a term of one month to three years. Where the violation of privacy occurs as a result of recording images or sound, the penalty to be imposed shall be increased by one fold. (2) (Amended on 2 July 2012 – Article 81 of the Law no. 6352) Any person who unlawfully discloses the images or sounds of another person's private life shall be sentenced to a penalty of imprisonment fro a term of two to five years. Where the offence is committed through the press or broadcasting, the penalty shall be the same.
Turkish Penal Code No.5237, Article 135	(1) Any person who illegally records personal data shall be sentenced to a penalty of imprisonment for a term of one to three years. (2) Any person who illegally records personal data on another person's political, philosophical or religious opinions, their racial origins; their illegal moral tendencies, sex lives, health or relations to trade unions shall be sentenced to a penalty of

	imprisonment in accordance with the above paragraph.
Turkish Penal Code No.5237, Article 136	(1) Any person who illegally obtains, disseminates or gives to another person someone's personal data shall be sentenced to a penalty of imprisonment for a term of two to four years.
Turkish Penal Code No.5237, Article 137	(1) Where the offences defined in the above articles are committed; a) by a public official misusing his power derived form his public post, or b) by benefiting from the privileges derived from a profession or trade. the penalty to be imposed shall be increased by one half.
Turkish Penal Code No.5237, Article 138	(1) Any person who fails to destroy data in accordance with the prescribed procedures, before the expiry of the legally prescribed period for destruction, shall be sentenced to a penalty of imprisonment for a term of one to two years. (2) (Added on 21 February 2014 – By Article 5 of the Law no. 6526) Where the subject of the offence remains within the scope of the information to be removed or eliminated under the provisions of the Code of Criminal Procedure, the penalty to be imposed shall be increased by one-fold.
Turkish Penal Code No.5237, Article 139	(1) Excluding the offences of Recording of Personal Data, Illegally Obtaining or Giving Data and Destruction of Data, the commencement of an investigation and prosecution for the offences listed in this Part are subject to complaint.
Personal Data Protection Law No. 6698, Article 4	(1) Personal data may only be processed in compliance with the procedures and principles set forth in this Law and other laws. (2) The following principles shall be complied within the processing of personal data:

	a) Lawfulness and conformity with rules of bona fides. b) Accuracy and being up to date, where necessary. c) Being processed for specific, explicit and legitimate purposes. ç) Being relevant with, limited to and proportionate to the purposes for which they are processed. d) Being retained for the period of time stipulated by relevant legislation or the purpose for which they are processed.
Personal Data Protection Law No. 6698, Article 9	(1) Personal data cannot be transferred abroad without explicit consent of the data subject. (2) Personal data may be transferred abroad without explicit consent of the data subject provided that one of the conditions set forth in the second paragraph of Article 5 and the third paragraph of Article 6 exist and that; (a) sufficient protection is provided in the foreign country where the data is to be transferred, (b) the controllers in Turkey and in the related foreign country guarantee a sufficient protection in writing and the Board has authorized such transfer, where sufficient protection is not provided. (3) The Board determines and announces the countries where sufficient level of protection is provided. (4) The Board shall decide whether there is sufficient protection in the foreign country concerned and whether such transfer will be authorised under the sub-paragraph (b) of second paragraph, by evaluating the followings and by receiving the opinions of related public institutions and organizations, where necessary: a) the international conventions to which Turkey is a party,

	b) the state of reciprocity concerning data transfer between the requesting country and Turkey, c) the nature of the data, the purpose and duration of processing regarding each concrete, individual case of data transfer, ç) the relevant legislation and its implementation in the country to which the personal data is to be transferred, d) the measures guaranteed by the controller in the country to which the personal data is to be transferred, (5) In cases where interest of Turkey or the data subject will seriously be harmed, personal data, without prejudice to the provisions of international agreements, may only be transferred abroad upon the permission to be given by the Board after receiving the opinions of related public institutions and organizations. (6) Provisions of other laws concerning the transfer of personal data abroad are reserved.
Personal Data Protection Law No. 6698, Article 10	(1) Whilst collecting personal data, the controller or the person authorised by him is obliged to inform the data subjects about the following: a) the identity of the controller and of his representative, if any, b) the purpose of data processing; c) to whom and for what purposes the processed data may be transferred, ç) the method and legal reason of collection of personal data, d) other rights referred to in Article 11.
Personal Data Protection Law No. 6698, Article 11	(1) Each person has the right to apply to the controller and a) to learn whether his personal data are processed or not, b) to request information if his personal data are processed,

	c) to learn the purpose of his data processing and whether this data is used for intended purposes, ç) to know the third parties to whom his personal data is transferred at home or abroad, d) to request the rectification of the incomplete or inaccurate data, if any, e) to request the erasure or destruction of his personal data under the conditions laid down in Article 7, f) to request notification of the operations carried out in compliance with subparagraphs (d) and (e) to third parties to whom his personal data has been transferred, g) to object to the processing, exclusively by automatic means, of his personal data, which leads to an unfavourable consequence for the data subject, ğ) to request compensation for the damage arising from the unlawful processing of his personal data.
Personal Data Protection Law No. 6698, Article 12	(1) The controllers are obliged to take all necessary technical and administrative measures to provide a sufficient level of security in order to: a) prevent unlawful processing of personal data, b) prevent unlawful access to personal data, c) ensure the retention of personal data. (2) In case of the processing of personal data by a natural or legal person on behalf of the controller, the controller shall jointly be responsible with these persons for taking the measures laid down in the first paragraph. (3) The controller shall be obliged to conduct necessary inspections, or have them conducted in his own institution or organization, with the aim of implementing the provisions of this Law.

	(4) The controllers and processors shall not disclose the personal data that they learned to anyone in breach of this Law, neither shall they use such data for purposes other than processing. This obligation shall continue even after the end of their term. (5) In case the processed data are collected by other parties through unlawful methods, the controller shall notify the data subject and the Board within the shortest time. Where necessary, the Board may announce such breach at its official website or through other methods it deems appropriate.
Personal Data Protection Law No. 6698, Article 13	(1) The data subject shall lodge an application in writing to the controller about his demands concerning the implementation of this Law or via other methods specified by the Board. (2) The data controller shall conclude the demands involved in the applications within the shortest time possible depending on the nature of the demand and within thirty days at the latest and free of charge. However if the action in question incurs another cost, the price set by the Board may be collected. (3) The data controller shall accept the application or decline it on justified grounds and communicate its response to data subject in writing or in electronic media. If the demand involved in the application found admissible, it shall be indulged by the data controller. Data subject shall be reimbursed for the application fee provided that the application has been lodged due to a mistake made by the controller.
Personal Data Protection Law No. 6698, Article 14	(1) If the application is declined, the response is found unsatisfactory or the response is not given in due time, the data subject may file a complaint with the Board within thirty days as of he learns about the

	response of the controller, or within sixty days as of the application date, in any case. (2) A complaint cannot be filed before exhausting the remedy of application to the controller under Article 13. (3) The right to compensation under general provisions of those whose personal rights are violated is reserved.
Personal Data Protection Law No. 6698, Article 15	(1) The Board shall make the necessary examination in the matters falling within its scope of work upon complaint or ex officio, where it learnt about the alleged violation. (2) The notices and complaints not meeting the requirements laid down in Article 6 of the Law No. 3071 of 1/11/1984 on the Use of Right to Petition shall not be examined. (3) Except for the information and documents having the status of state secret, the controller shall be obliged to communicate within fifteen days the information and documents related to the subject of examination which the Board has requested, and shall enable, where necessary, on-the-spot examination. (4) The Board shall finalise the examination upon complaint and give an answer to data subjects. In case the Board fails to answer the data subject's application in sixty days as of the application date, it is deemed rejected. (5) Following the examination made upon complaint or ex officio, in cases where it is understood that an infringement exists, the Board shall decide that the identified infringements shall be remedied by the relevant controller and notify this decision to all it may concern. This decision shall be implemented without delay and within thirty days after the notification at the latest, (6) Following the examination made upon complaint or ex officio, in cases where it is determined that the infringement is

	widespread, the Board shall adopt and publish a resolution in this regard. Before adopting the resolution, the Board may also refer to the opinions of related institutions and organisations, if needed. (7) The Board may decide that processing of data or its transfer abroad should be stopped if such operation may lead to damages that are difficult or impossible to recover and if it is clearly unlawful.
Personal Data Protection Law No. 6698, Article 16	(1) The Presidency shall maintain a publicly accessible Registry of Controllers under the supervision of the Board. (2) Natural or legal persons who process personal data shall be obliged to enrol in the Registry of Data Controllers before proceeding with data processing. However, by taking into account the objective criteria set by the Board such as the nature and quantity of the data processed, the legal requirement for data processing, or transferring the data to third parties, the Board may provide exception to the obligation of enrolment in the Registry of Data Controllers. (3) Application for enrolling in the Registry of Data Controllers shall be made with a notification including: a) identity and address of the controller and of his representative, if any, b) purposes for which the personal data will be processed, c) explanations about group(s) of personal data subjects as well as about the data categories belonging to these people, ç) recipients or groups of recipients to whom the personal data may be transferred, d) personal data which is envisaged to be transferred abroad, e) measures taken for the security of personal data.

	f) maximum period of time required for the purpose of the processing of personal data. (4) Any changes in the information provided under the third paragraph shall be immediately notified to the Presidency (5) Other procedures and principles governing the Registry of Data Controllers shall be laid down through a by-law.
Personal Data Protection Law No. 6698, Article 17	(1) Articles 135-140 of Turkish Penal Code No. 5237 of 26/9/2004 shall apply in terms of the crimes concerning personal data. (2) Those who fail to erase or anonymize personal data in breach of Article 7 herein shall be punished under Article 138 of the Law No. 5237.
Personal Data Protection Law No. 6698, Article 18	(1) For the purposes of this Law; a) those who fail to comply with obligation to inform provided for in Article 10 herein shall be required to pay an administrative fine of 5.000 to 100.000 TL, b) those who fail to comply with obligations related to data security provided for in Article 12 herein shall be required to pay an administrative fine of 15.000 to 1.000.000 TL, c) those who fail to comply with the decisions issued by the Board under Article 15 herein shall be required to pay an administrative fine of 25.000 to 1.000.000 TL, ç) those who fail to meet the obligations for enrolling in the Registry of Data Controllers and making a notification as provided for in Article 16 herein shall be required to pay an administrative fine of 20.000 to 1.000.000 TL. (2) The administrative fines listed in this article shall be applicable to natural persons and private law legal persons who are controllers.

	(3) Should the acts listed in the first paragraph be committed within the public institutions and organizations as well as professional associations having the status of public institution, disciplinary procedures shall be applied to the civil servants and other public officers employed in the relevant public institutions and organisations and those employed in the professional associations having the status of public institution upon a notice by the Board and the result is communicated to the Board.
Personal Data Protection Law No. 6698, Article 19	(1) Personal Data Protection Authority which is a public law body with public law legal personality having administrative and financial autonomy has been established to carry out duties provided by this Law (2) The Authority is affiliated to the office of the Prime Minister (3) The Headquarters of the Authority is in Ankara (4) The Authority is composed of the Board and the Presidency. Decision making body of the Authority is the Board.
Personal Data Protection Law No. 6698, Article 21	(1) The Board shall perform and exercise the duties and powers conferred on it by this law and other laws, independently and under its own responsibility. No body, authority, office or person shall give orders and instructions, recommendations or suggestions to the Board on matters falling within the scope of its duties and powers. (2) The Board is composed of nine members. Five members of the Board shall be elected by the Grand National Assembly of Turkey, two members shall be elected by the President of Turkey and two members shall be elected by the Council of Ministers. (3) The following conditions shall be met in order to be elected for the Board:

	a) Being informed on and being experienced in the issues falling within Authority's field of duty. b) Complying with the requirements set forth in points (1), (4), (5), (6) and (7) of subparagraph (A) of first paragraph of Article 48 of the Public Servants Law No. 657 of 14/7/1965. c) Not being a member of any political party. ç) Having been graduated from at least a four-year graduate program. d) Having been employed in public institutions and organisations, international organisations, non-governmental organisations, or professional associations having the status of public institution or in the private sector for at least ten years in total. (4) Those who are elected for the membership should express their consent. Elections are held so as to pluralistical representation of those who are informed on and experienced in the issues falling within Authority's field of duty. (5) Board members shall be elected by the Grand National Assembly of Turkey on the basis of the following procedure: a) Persons twice as many as the number of members to be determined in proportion to the number of deputies of political party groups shall be nominated for election and the members of the Board shall be elected by the Plenary of the Grand National Assembly from among these candidates on the basis of the number of deputies allocated to each political party. However, political party groups shall not negotiate or decide whom to vote for in the elections to be held in the Grand National Assembly of Turkey. b) The Board members shall be elected within ten days after the designation and

	announcement of the candidates. For the candidates designated by the political party groups, a composite ballot in the form of separate lists shall be prepared. Voting shall be cast by ticking of the specific space across the names of the candidates. The votes casted more than the numbers of the members to be elected for the Board from the political party quotas, determined in accordance with paragraph two, shall be deemed invalid. c) Provided that the quorum is ensured, candidates the number of whom corresponds to the number of vacancies and who take most of the votes shall be deemed to have been elected. ç) The election for the renewal of the members shall be held two months before the expiration of their term of office; should there be a vacancy in the memberships for any reason, there shall be an election within one month as of the date of vacancy; or if the date of vacancy coincides with the recess of the Grand National Assembly of Turkey. the election shall take place within one month from the end of the recess, by employing the same procedure. During these elections, the allocation of the vacant memberships to the political party groups shall be made by considering the number of the elected members from the political party groups' quotas in the first election and the current proportions of the political party groups. (6) Forty-five days before the expiration of the term of office or in case of expiration of term of office by any reason of the members elected by the President of Turkey or the Council of Ministers, the Authority shall notify the situation in fifteen days to the office of the Prime Minister so as to be

	submitted to the office of the President of Turkey or the Council of Ministers; A new election shall take place one month before the expiration of term of office of the members. Should there be a vacancy in these memberships before the expiration of term of office, there shall be an election within fifteen days as of the date of notification. (7) The Board shall designate the Head and the Second Head of the Board among its members. The Head of the Board is also the President of the Authority. (8) Term of office of the Board members is four years. Members may be re-elected after expiration of their term of office. The person who is elected instead of the member whose post ends before the expiration of his/her term of office for any reason, shall complete the remaining term of office. (9) Members of the Board shall take the following oath before Court of Cassation's Board of First Presidency: 'I do solemnly swear on my honour and on my dignity that I will carry out my duties with absolute impartiality, bona fides, fairness and with sense of justice in line with the Constitution and the relevant legislation.' Application to Court of Cassation for oath taking is deemed to be one of the pressing matters. (10) Unless provided for by a specific law, the members shall not assume any public or private tasks other than those related with carrying out their official duties in the Board; shall not act as executives in associations, foundations, cooperatives and in similar bodies; shall not engage in commercial activities, shall not engage in self-employment, shall not act as arbitrators and expert witnesses. However, Board members may prepare scientific publications, give lectures and attend conferences so as

	not to hinder their primary duties, and may receive copyrights and fees associated with those. (11) Investigations into the claims about the crimes allegedly committed by the members in connection with their duties shall be conducted as per the Law No. 4483 of 2/12/1999 on Adjudication of Public Servants and Other Public Employees, and permission for investigation shall be granted by the Prime Minister. (12) Provisions of the Law No. 657 shall apply to disciplinary investigations and prosecutions about the members of the Board. (13) Members shall not be removed from their office by any reason before the expiration of their term of office. However, members of the Board may be removed from office by the Board decision if: a) it is found out subsequently that they do not meet the conditions required for their election, b) the verdict, which is rendered for crimes committed by them in connection with their duties, becomes final c) a medical report is issued by board of health to certify that they are not suitable for office, ç) it is ascertained that they were absent from work for fifteen consecutive days or for a total of thirty days within a year, without legitimate permission and excuse. d) it is ascertained that they fail to attend three Board meetings in one month and ten Board meetings in one year without any permission and excuse. (14) Those who are appointed as the members of the Board shall be removed from their previous posts during their term of office in the Board. On the condition that

	they do not fail to meet the requirements of being employed as a civil servant, those who are assigned as Board members whilst on duty shall be appointed to posts that are appropriate for their vested positions and titles in one month, in case their term of office ends or they express their will to resign and lodge an application in this regard to their former institution within thirty days. Until the assignment, Authority shall continue to make any payment they are vested with. Until they take another post or take up another employment, Authority shall continue to make the payment of those who are appointed as Board members despite not being public servants and whose term of office terminated as stated hereinabove; and the payments to be made under this scope shall not exceed three months. With regard to personal and other rights, terms spent in the Authority shall be deemed to have spent in the previous institutions or organisations.
Personal Data Protection Law No. 6698, Article 22	(1) Duties and powers of the Board are as follows: a) to ensure that the personal data are processed in compliance with fundamental rights and freedoms. b) to conclude the complaints of those claiming that their rights with regard to personal data protection have been violated. c) to examine whether the personal data are processed in compliance with the laws, upon complaint, or ex officio where it learnt about the alleged violation, and to take temporary measures, if necessary. ç) to determine the adequate measures which are necessary for the processing of the data of special nature. d) to ensure that Registry of Controllers is maintained.

	e) to draft regulatory acts on the matters concerning the Board's field of duty and operation of the Authority. f) to draft regulatory acts in order to lay out the liabilities concerning data security. g) to draft regulatory acts on the matters concerning duties, powers and responsibilities of the Controller and of his representative. ğ) to decide on the administrative sanctions provided for in this Law. h) to deliver its opinion about the legislation drafted by other institutions or organizations that contain provisions on personal data. ı) to conclude the Strategic Plan of the Authority; to determine the purpose, targets, service quality standards and performance criteria of the Authority. i) to discuss and decide on Strategic Plan and the budget proposal of the Authority which are prepared in compliance with its purposes and targets. j) to approve and publish the draft reports on the performance, financial situation, annual activities and other matters related with the Authority. k) to discuss and decide on the recommendations as regards the purchase, sale and lease of immovable properties. l) to carry out other tasks provided for by laws.
Personal Data Protection Law No. 6698, Article 28	(1) The provisions of this Law shall not be applied in the following cases where: a) personal data is processed by natural persons within the scope of purely personal activities of the data subject or of family members living together with him in the same dwelling provided that it is not to be disclosed to third parties and the obligations about data security is to be complied with.

	b) personal data is processed for the purpose of official statistics and for research, planning and statistical purposes after having been anonymized. (c) personal data is processed with artistic, historical, literary or scientific purposes, or within the scope of freedom of expression provided that national defence, national security, public security, public order, economic security, right to privacy or personal rights are not violated or they are processed so as not to constitute a crime. (ç) personal data is processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorised and assigned to maintain national defence, national security, public security, public order or economic security. (d) personal data is processed by judicial authorities or execution authorities with regard to investigation, prosecution, criminal proceedings or execution proceedings. (2) Provided that it is in compliance with and proportionate to the purpose and fundamental principles of this Law, Article 10 regarding the data controller's obligation to inform, Article 11 regarding the rights of the data subject, excluding the right to demand compensation, and Article 16 regarding the requirement of enrolling in the Registry of Data Controllers shall not be applied in the following cases where personal data processing: a) is required for the prevention of a crime or crime investigation. b) is carried out on the data which is made public by the data subject himself. c) is required for inspection or regulatory duties and disciplinary investigation and prosecution to be carried out by the public

	institutions and organizations and by professional associations having the status of public institution, assigned and authorised for such actions, in accordance with the power conferred on them by the law, ç) is required for protection of State's economic and financial interests with regard to budgetary, tax-related and financial issues.

Bibliography

English titles

Legislation

Act on Restrictions on the Secrecy of the Mail, Post and Telecommunications (1968)

Basic Law (1948)

Code of Civil Procedure No. 5271

Constitution of the Republic of Turkey

Constitution of the Republic of Turkey

Criminal Law Amendment Act 1885

International Convention on the Elimination of all Forms of Racial Discrimination

Labour Law No. 4857

Personal Data Protection Law No. 6698

Personal Data Protection Law No. 6698

Presidential Decree No. 1

Procedure of Administrative Justice Act No. 2577

Turkish Penal Code No. 5237

Reports

'State Council', (2017) Next Generation Artificial Intelligence Development Plan China Science and Technology Newsletter

<http://fi.china-embassy.org/eng/kxjs/P020171025789108009001.pdf> accessed 7 March 2021.

<https://www.insiktintelligence.com/new-fines-on-social-media-platforms/> accessed 7 March 2021.

<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> accessed 7 March 2021.

Burianov M, 'Here'S Why We Need a Declaration Of Global Digital Human Rights' (World Economic Forum 2020)

<https://www.weforum.org/agenda/2020/08/here-s-why-we-need-a-declaration-of-global-digital-human-rights/> accessed 1 February 2021

Article 29 Working Party, 'Opinion 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)' (WP 237, 13 April 2016).

Committee of Experts on the Application of Conventions and Recommendations.

Department of International Cooperation Ministry of Science and Technology (MOST), P.R. China

H. Tankovska, 'Facebook: number of monthly active users worldwide 2008-2020' (2021).

Human Rights Commentary in the United Nations: Human Rights Committee and Committee on Economic, Social and Cultural Rights.

Insikt Intelligence, 'New EU laws that will force social media platforms to remove terrorists' content within 1 hour or face fines'

Kandemir M., Yardimcioglu D., 'Equality Principle in Labor Law' Dicle University Faculty of Law (2014).

Karagoz V, 'Discrimination Compensation at Labour Law' (2010).

Kolombus K 'Artificial Intelligence is preparing for recruitment! And it might be better than you expected (2018).

M. Burianov, 'Here is why we need a Declaration of Global Human Rights' (2020).

Martinez M.R & Gaubert J., 'The sexism of artificial intelligence: female-made algorithms discriminate against women' Euronews, 2020.

Rue F L, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' UNGA 23rd Session A/HRC/23/40 (2013).

Books

Gürses S and Preneel B, 'Cryptology and Privacy in the Context of Big Data' in Bart van der Sloot, Dennis Broeders and Erik Schrijver (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016).

KVKK, 'Data Protection in Turkey' (KVKK Yayınları, 2019).

Symeonidis I and Lenzini G, 'Systematization of Threats and Requirements for Private Messaging with Untrusted Servers: The Case of E-mailing and Instant Messaging'

(International Conference on Information Systems Security and Privacy, Malta, February 2020).

Periodicals

Aldhouse F, 'A Reflection on the Priorities of a Data Protection Authority' (2018) 34 Computer Law & Security Review 816.

Balthasar A, 'Complete Independence' of National Data Protection Supervisory Authorities Second Try: Comments on the Judgment of the CJEU of 16 October 2012, C-614/10, with Due Regard to Its Previous Judgment of 9 March 2010, C-518/07' (2013) 9 Utrecht Law Review 26.

Baumann M-O and Schünemann WJ, 'Introduction: Privacy, Data Protection and Cybersecurity in Europe' [2017] Privacy, Data Protection and Cybersecurity in Europe 1.

Etteldorf C, 'Germany · Data Protection Authorities Try to Fill the Gap between GDPR and e-Privacy Rules' (2018) 4 European Data Protection Law Review 235.

Giurgiu A and A Larsen T, 'Roles and Powers of National Data Protection Authorities' (2016) 2 European Data Protection Law Review 342.

Greenleaf G, 'Independence of Data Privacy Authorities (Part I): International Standards' (2012) 28 Computer Law & Security Review 3.

Gül İ.I., Karan U., 'Prohibition of Discrimination: Concept, Law, Monitoring Documentation' (2011).

Karan U, 'Prohibition of Discrimination in Turkish Law and Feasibility of Article 122 of Turkish Panel Code (2007).

Oğusgil VA, 'Independence of Data Protection and Supervisory Authorities in The EU Member States and Prospective Case of Turkey' (2014) 14 AİBÜ Sosyal Bilimler Enstitüsü Dergisi 203.

Sevinç İ and Karabulut N, 'A Review on The Personal Data Protection Authority of Turkey '(2020) 7 The Academic Elegance 449 <https://dergipark.org.tr/tr/download/article-file/1128175> accessed March 1, 2020.

Digital resources

'Fake News and Cyber Propaganda: The Use and Abuse of Social Media' (2017) <https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media> accessed 7 March 2021.

'Kişisel Verileri Koruma Kurumu: KVKK: Guidelines' (KVKK) <https://www.kvkk.gov.tr/Icerik/6618/Guidelines> accessed March 1, 2021.

'Kişisel Verileri Koruma Kurumu: KVKK: Personal Data Protection Law'(KVKK) <https://www.kvkk.gov.tr/Cache/SetLanguage?returnUrl=%2FIcerik%2F6649%2FPersonal-Data-Protection-Law&langId=2> accessed March 1, 2021.

'Kişisel Verileri Koruma Kurumu: KVKK: Personal Data ProtectionAuthority'(KVKK) <https://www.kvkk.gov.tr/Icerik/6586/Personal-Data-Protection-Authority> accessed March 1, 2021.

'Kişisel Verileri Koruma Kurumu: Right to Lodge a Complaint' (KVKK) <https://kvkk.gov.tr/Icerik/6616/Right-to-Lodge-a-Complaint-with-the-Board-> accessed March 1, 2021.

'Kişisel Verileri Koruma Kurumu: Turkish Journal and Privacy and Data Protection' (KVKK) <https://www.kvkk.gov.tr/Icerik/6648/Turkish-Journal-and-privacy-and-data-protection> accessed March 1, 2021.

Andrada Coos, 'All You Need to Know About Turkey's Personal Data Protection Law (KVKK)' (Endpoint Protector, 30 April 2020) <https://www.endpointprotector.com/blog/everything-you-need-to-know-about-turkeys-personal-data-protection-law/> accessed 7 February 2021.

Ardiyok S, 'Reading Between the Lines of The Turkish Data Protection Law: The Decisions of The Authority - Finance and Banking - Turkey' (Welcome to Mondaq February 2021). <https://www.mondaq.com/turkey/financial-services/1032628/reading-between-the-lines-of-the-turkish-data-protection-law-the-decisions-of-the-authority> accessed March 1, 2021.

Burcu Tuzcu Ersin, 'Turkey-Data Protection Overview' (One Trust Data Guidance, April 2020) <https://www.dataguidance.com/notes/turkey-data-protection-overview> accessed 7 February 2020 accessed 6 February 2021.

Duygu Doğan, 'Personal Data Protection in Turkey: The Impact on Business' (GRC World Forums ,8 November 2018) <https://www.grcworldforums.com/gdpr/personal-data-protection-in-turkey-the-impact-on-business/28.article> accessed 9 February 2021.

Global Law Forum <http://maxlaw.tilda.ws/digitalrights_globalshapers> accessed 7 March 2021.

How are today's biggest tech trends affecting our human rights? <https://www.weforum.org/agenda/2017/12/how-are-today-s-biggest-tech-trends-affecting-human-rights/> accessed 1 March 2021.

Kişisel Verileri Koruma Kurumu: KVKK: Complaint to the Board'(KVKK)<https://www.kvkk.gov.tr/Icerik/6659/Complaint-to-the-Board> accessed March 1, 2021.

Micheal Clarke, 'The Digital Revolution' (2014) <https://www.sciencedirect.com/science/article/pii/B9781843346692500044?via%3Dihub>accessed 1 March 2021.

Ozan Karaduman, 'The New Personal Data Protection Law 2019 in Turkey' (Gün+Partners Insights, 14 February 2019) <https://gun.av.tr/insights/articles/the-new-personal-data-protection-law-2019-in-turkey > accessed 5 February 2021.

S.Romi Mukherjee, 'Linking science and human rights: Fact and figures'(2012) <https://www.scidev.net/global/features/linking-science-and-human-rights-facts-and-figures/> accessed 1 March 2021.

Soyamedia.com, 'The WhatsAppocalypse Continues: Turkish Data Protection Authority Initiates an Investigation against WhatsApp (Detail) - Legal Services Kinstellar' <https://www.gentemizerozer.com/insights/detail/54/the-whatsappocalypse-continues-turkish-data-protection-authority-initiates-an-investigation-against-whatsapp> accessed 1 March 2021.

Case-law

General Assembly of Civil Chambers of the Court of Cassation of the Republic of Turkey, 17 June 2015, No. 2014 / 4-56 2015/1679 K. <http://kazanci.com.tr/gunluk/hgk-2014-4-56.html> accessed 4 March 2021.

Google Spain SL and Google Inc. v *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014, No. C-131/12 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62012CJ0131> accessed 4 March 2021.

Klass and Others v *Germany* (1979) 2 EHRR 214.

Principle Decision of the Personal Data Protection Board of the Republic of Turkey, 16 October 2018, No.2018/118

S and Marper v *United Kingdom* [2008] ECHR 1581

The Board Decision on Cathay Pasific Airway, 16 May 2019, No.2019/144 <https://www.kvkk.gov.tr/Icerik/6597/Board-Decision-about-Cathay-Pasific-Airway> accessed 22 February 2021.

The Board Decision on Facebook, 16 May 2019, No.2019/269 <https://www.kvkk.gov.tr/Icerik/6594/Board-Decision-No-2019-269-on-Facebook>accessed 22 February 2021.

The Board Decision on Procedures and Principles of Personal Data Breach Notification, 24 January 2019, No. 2019/10 <https://www.kvkk.gov.tr/Icerik/6647/The-Board-Decision-No-2019-10-of-24-01-2019-about-Procedures-and-Principles-of-Personal-Data-Breach-Notification> accessed 22 February 2021.

The Board Decision on the Application Regarding Amazon Turkey, 27 February 2020, No.2020/173 <https://www.kvkk.gov.tr/Icerik/6739/2020-173> accessed 22 February 2021.

The Board Decisions regarding minimum elements that should be included in the communication of the breach by the data controller to the data subject, 18 September 2019, No. 2019/271 <https://www.kvkk.gov.tr/Icerik/6599/Board-Decision-on-Minimum-Elements-that-Should-be-Included-in-the-Communication-of-the-breach-by-the-Data-Controller-to-the-Data-Subject> accessed 22 February 2021.

The Decision of the Personal Data Protection Board regarding dated 'the transfer of personal data abroad on the basis of Convention No. 108', 22 July 2020, No. 2020/559 <https://www.kvkk.gov.tr/Icerik/6812/2020-559> accessed 22 February 2021.

The Decision of the Personal Data Protection Board regarding dated 'the transfer of personal data abroad on the basis of Convention No. 108', 22 July 2020, No. 2020/559 <https://www.kvkk.gov.tr/Icerik/6812/2020-559> accessed 22 February 2021.

Zakharov v *Russia* [2015] ECHR, 47143/06 (ECHR)

Turkish titles

Legislation

2577 Sayılı İdari Yargılama Usulü Kanunu.

3071 Sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun.

5237 Sayılı Türk Ceza Kanunu.

6698 Sayılı Kişisel Verilerin Korunması Kanunu.

Türkiye Cumhuriyeti Anayasası.

Reports

KVKK, Kişisel Verilerin Korunması Alanında Ulusal ve Uluslararası Düzenlemeler (KVKK Yayınları 2019) <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/ead8e671-e01e-4ca7-a6a3-bc3c6f79f7c7.pdf> accessed 22 February 2021.

Books

Başar C, Türk İdare Hukuku Ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması (1st edn, On İki Levha Yayıncılık 2020).

Kaya İ and Tolun Y, *Uygulayıcılar İçin Türkiye'de Ve Avrupa'da Kişisel Verilerin İşlenmesi* (Adalet Yayınevi 2020).

KVKK, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi* (KVKK Yayınları No:1, 2019).

KVKK, *Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü* (KVKK Yayınları, 2019).

Öz B, *'Yargı Mercilerinin Görev Alanına Giren Konularla İlgili Kuruma Yapılan Başvurular' Hakkında Kişisel Verileri Koruma Kurulunun 24.12.2018 Tarihli Ve 2018/156 Sayılı Karar Özet,' KVKK Mevzuatı ve Örnek Uygulamaları* (Ekin Yayınevi 2020).

Özkan O, *'Kişisel Verilerin Korunması'* (1st edn,Yetkin Yayınları, 2020).

Üzülmez İ and Mahmut Koca *'Kişisel Verilerin Kaydedilmesi Suçu',* (7th edn Adalet Yayınevi 2020).

Periodicals

Kağıtçıoğlu M, 'Kişisel Verileri Koruma Kurumu'na İdare Hukuku Çerçevesinden Bir Bakış' (2016) 1 Aurum Social Sciences Journal 77 <https://dergipark.org.tr/tr/download/article-file/272994> accessed March 1, 2021.

Digital Resources

Türkiye Cumhuriyeti Dijital Dönüşüm Ofisi <https://cbddo.gov.tr/projeler/#3168> accessed 7 March 2021.

ELSA UKRAINE

Contributors

National Coordinator
Vsevolod Martseniuk

National Academic Coordinator
Ivan Chopyk

National Researchers
Anna-Mariya Luhova
Angelina Spylnik
Bohdan Myronenko
Dariia Donets
Krystyna Lahutina
Nataliia Pavlovych
Viktor Pasichnyk
Vladyslav Sperkach
Yelyzaveta Markova

National Academic Supervisor
Oleksandr Melnyk

Acknowledgements

We would like to express our sincere gratitude to academic supervisor - Oleksandr Melnyk for his continuous support in drafting this report and related research, his patience, motivation and immense knowledge.

Introduction

Ukraine is actively implementing new legislative projects that will regulate advanced digital technologies, as well as changing the legislation of previous years in order to respond to global changes. However, the main problem areas of the state remain the issue of personal data breaches, which have only intensified from the 2000s to the present. From selling papers with collected personal data of voters and bank card holders, or creating the first websites on the Darknet, personal data thieves have moved to online business through anonymous platforms with cryptocurrency payment. Data of Ukrainians are sold for aggressive marketing, mailing spam etc. From time to time, the media accuse state resources of violating user data, and there is evidence of corruption of civil servants who use their status to launder money illegally by selling data. The black data market is thriving, as evidenced by the apparent disclosure of crimes such as Sanix and his profits from data trading and the issuance of online loans by the name of others.

Over the last 5 years, there has been a tendency to increase the precedents of blocking websites: from those that undermine the democracy of the state to GitHub. Some websites have been blocked to date, some of the list of more than 500 sites have been updated, justified with the help of activists, the Ministry of Digital Transformation a.o.

There are cases of criminal prosecution for information posted on the Internet. Incidentally, the imprisonment or fines imposed on violators are not always proportional to the crime and its harm to the society. There are a number of other human rights violations that we cover in our legal research below.

In conclusion, we must admit that in Ukraine there are significant changes in legislation, but also many issues that need to be solved as to why our legal research is focused.

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

To consider the issue of our study, we must first recognize the definition of Advanced Digital Technologies. For the purposes of this Report, we will limit our attention to technologies for collecting, storing, processing, searching, transferring and presenting data in electronic form. These include technologies related to personal data processing, Internet of Things, artificial intelligence, cyber security. Violations, risks and regulatory threats to human rights online in the context of the use of ADTs are widespread in Ukraine, which is why we will now try to reveal the main areas of concern.

1.1. Right to privacy

The issue of personal data protection in Ukraine is regulated by the Law of Ukraine 'On Personal Data Protection'.[554] The Grand Chamber of the Supreme Court has formed the principles of personal data processing (openness and transparency, responsibility, adequacy, non-redundancy of their composition and content in relation to the specified purpose of processing), as well as the grounds for personal data processing. When a person agrees to register on the website, he/she automatically signs for the processing of personal data. Many services provided by public authorities also consent to the processing of personal data. Unfortunately, it is almost impossible to remember to whom and what personal data is provided, as well as to predict the possible leakage of provided data. There are many problems in this matter, so we propose to dwell on the most common.

Firstly, the text of the consent to the processing of personal data is always the same, does not involve changes and has only one option - to agree. Failure to sign such an agreement makes it impossible to obtain the necessary services. However, it is important to take into account the consequences of giving consent in a certain situation. The Grand Chamber of the Supreme Court in the exemplary case[555] pointed out that the law does not regulate the consequences of a person's refusal to process his personal data, in fact there is no alternative to such a choice, which leads to poor law and violation of constitutional rights of a person. In addition, the implementation of state functions should be carried out without forcing a person to consent to the processing of personal data. Such processing, as before, should be carried out within and on the basis of those laws and regulations of Ukraine, in accordance with which there are legal relations between the citizen and the state. In this case, technologies should not be unalterable and coercive. Individuals who have refused to process their personal data must have an alternative - the use of traditional methods of identification.

Secondly, the person does not know where and to whom his/ her personal data may be transferred in the future. Article 8 of the Law of Ukraine 'On Personal Data Protection'[556] stipulates that the personal data subject may receive information on the conditions of access to personal data, information about third parties to whom his/her personal data is transferred, have access to his/her personal data and even withdraw consent to personal data processing. According to the number of consents given by a person in today's world, it is impossible to track the transfer of their data to third parties. In this regard, the exercise of the rights granted by law is ineffective. In most cases, individuals are often unaware of the dissemination of their data and therefore cannot properly protect it. The issue of

[554] The Law of Ukraine 'On Personal Data Protection' 2010 № 2297-VI <https://zakon.rada.gov.ua/laws/show/2297-17> accessed 1 June 2021.
[555] Case №806/3265/17 (26 March 2018) (Grand Chamber of the Supreme Court) <https://supreme.court.gov.ua/supreme/inshe/zrazkovi_spravu/zr_rish_806_3265_17> accessed 1 June 2021.
[556] The Law of Ukraine 'On Personal Data Protection' (n 554), art 8.

revocation of consent was considered by the Ministry of Justice of Ukraine in Letter,[557] which stated that the consent can be revoked only for future data processing, as a result of which the person cannot be sure of, therefore, how and who has already processed its data. In this regard, there is a question of security of already processed data.

In view of the above, it will be appropriate to pay attention to the possibility of deleting already provided personal data. The Law of Ukraine 'On Personal Data Protection' provides for such a possibility, but it cannot be done at the request of a person. This requires a court decision or an order from the Commissioner. In case №127/13877/19[558] The court of first instance, satisfying the plaintiffs' claims for the obligation to delete personal data by Ukrposhta Company, indicated that the identification of a person during the provision of services can be carried out on passport data without the need for automation. Despite the fact that the plaintiffs in this case did not consent to the processing of their personal data and entry in electronic databases, the defendant did not prove that he did not carry out such processing.

The owner of the largest amount of personal data is the state, so it is to meet the strictest requirements for their preservation and avoidance distribution in cases where it is not provided by the consent of the person. It is obvious that the leakage of information from state databases only increases distrust of the state and creates a feeling of insecurity against internal and external threats. Thus, we cannot talk about the protection of personal data by individuals, even if public databases are under threat. Ukrainian practice in this matter is characterized by a much smaller number of cases, but not due to the lack of violations, but due to the low legal culture of citizens regarding their own personal data and inefficient system of their protection.

Illegal trade in private data has existed in Ukraine for ten years. Back in the early 2000s at the capital's book market 'Petrovka' you could buy CDs with databases of voters, customers of bank officials or mobile operators. Currently, such information is sold mainly on specialized sites in the darknet. In addition, the recently popular platform for this performance Telegram - a messenger that can maintain anonymity and accept payments in cryptocurrency. Recently, there was a large-scale leak of personal data of Ukrainian citizens, mostly on driver's licenses, so the suspicion immediately fell on the application 'DIYA'.[559] Some time later, the authorities denied involvement in the statement. The true cause of the data leak has not yet been established. However, the rights of not only the users of this program, but also millions of others were violated. In any case, this is a problem of data

[557] Ministry of Justice of Ukraine in Letter №5543-0-33-13 / 6.1 dated 26.04.2013 <https://zakon.rada.gov.ua/laws/show/v5543323-13#Text> accessed 1 June 2021.
[558] Case № 127/13877/19 (24 June 2020) (Vinnytsia Court of Appeal) <https://reyestr.court.gov.ua/Review/90109587> accessed 1 June 2021.
[559] DIYA is a mobile application, web portal and brand of the digital state in Ukraine developed by the Ministry of Digital Transformation of Ukraine.

leakage from the authorities from IT systems created and maintained by the state.[560] People needed to use Tor to visit the site anonymously. Now the telegram bot has been combined with the Bitcoin anonymous payment service, which allows database owners to accept money safely. Privacy allows cybercrime to grow rapidly, but is a big plus for investigators and journalists.

Sean Townsend[561] said in his interview that on hacker forums people can buy e-mail accounts of Ukrainians for less than $ 1 per unit - both wholesale and retail. The cost of data collection, for example, for spam, ranges from a few tens to several hundred dollars per set. Targeted attacks on specific people or customers of companies are much more expensive. Information is traded not only by hackers. According to Townsend, this is often done by unscrupulous officials and insiders of companies that have access to personal databases - addresses, telephone numbers, passport numbers. Last year a former police colonel was exposed for purchase nine apartments in Kyiv by leaking data[562] from the Ministry of Internal Affairs and the National Police of Ukraine for years.

1.2. Freedom of opinion, expression, speech

In Ukraine, the Internet has no separate legal regulation. The Constitution guarantees the right to freedom of thought and speech, free expression of views and beliefs, whilst prohibiting censorship.[563]

At the same time, the Constitution of Ukraine provides for the possibility of restricting the right to freedom of speech on the basis of law in the interests of national security, territorial integrity or public order in order to prevent riots or crimes, to protect public health, to protect the reputation or rights of others, information obtained in confidence or to maintain the authority and impartiality of justice.[564]

---

[560] Vsevolod Nekrasov, 'State registers have leaked: who is 'merging' the personal data of Ukrainians and what to do about it' (Economic truth, 13 May 2020)
<https://www.epravda.com.ua/publications/2020/05/13/660405/> accessed 1 June 2021

[561] Volodimir Kondrashov, 'Battle on two fronts. Great interview with the founders of the Ukrainian Cyber Alliance' (New Time Business, 3 March 2020)
<https://biz.nv.ua/ukr/tech/zasnovniki-ukrajinskogo-kiberalyansu-mi-ne-nouneymi-yakis-neisnuyuchi-obraz i-chi-agenti-sbu-50073238.html> accessed 1 June 2021.

[562] National Police of Ukraine, A group of people led by a former National Police official was detained in Kyiv for unauthorized use of official information, Official Website of the National Police (Official website of the National Police, 20 February 2019)
<https://www.npu.gov.ua/news/korupcziya/u-kijevi-za-nesankczionovane-vikoristannya-sluzhbovoji-inform acziji-zatrimano-grupu-osib-na-choli-z-kolishnim-posadovczem-naczpolicziji/> accessed 01 June 2021.

[563] Constitution of Ukraine 1996 art 15
<https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> accessed 1 June 2021.

[564] ibid, art. 37.

In the previous ILRG ELSA Ukraine[565] mentioned that an indirect continuation of the protectionist policy against potential informational threats from the Russian Federation as envisaged by particular policy papers, Ukrainian authorities enforced blocking to restrict access to several Russian websites in order to fight hybrid war and propaganda.[566] The instrument was enforced through the Law of Ukraine 'On Sanctions' allowing the National Security and Defence Council of Ukraine (NSDC), a presidential coordination body in the area, to impose particular restrictions. The Law does not explicitly provide for blocking as one of the permissible instruments. Although, it allows for 'other sanctions in accordance with the principles of their application as established by this Law, [567] which may vaguely be interpreted to allow for any imaginable sanctions if they correspond to certain criteria. With that being said, such decisions are applicable only to executive authorities.[568] The NSDC can impose sectoral and personal sanctions for the purpose of national interests, national security, sovereignty and territorial integrity of the state protection, counteraction of terrorist activity, as well as prevention of violation, restoration of violated rights, freedoms and legitimate interests of Ukrainian citizens.[569] The freedom of speech restriction in the interests of national security, territorial integrity, or public order is one of the derogations allowed under the Constitution of Ukraine.[570] Therefore, the balance between protecting the fundamental freedoms and observing the state's own integrity deserves attention, even more so considering the current situation in Ukraine. Experts stress that as the information can be weaponized it creates difficulties in creating proper counter-action mechanisms to deal with Russian disinformation.[571] The lack of proper internet environment regulation leaves certain decisions to be taken on a case-by-case basis.[572] In this aspect it is necessary to consider the notorious Decree of the President of Ukraine №133/2017[573] and № 109/2021.[574] The Decree enacted the Decision of NSDC

[565] 'International Report on Internet Censorship. Final Report of the International Legal Research Group on Internet Censorship (eds)' (ELSA International, 2020) <https://files.elsa.org/AA/LRG_Internet_Censorship/Final_Report.pdf> acessed 1 June 2021, pp. 1195-1198.

[566] Alec Luhn, 'Ukraine blocks popular social networks as part of sanctions on Russia' (16 May 2017) <https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war> accessed 8 May 2020.

[567] The Law of Ukraine 'On Sanctions' 2014 №1644-VII art 4, §1(25) < https://zakon.rada.gov.ua/laws/show/1644-18#Text> accessed 2 April 2020.

[568] ibid, art 10, §4.

[569] ibid, art 1, §1.

[570] Constitution of Ukraine (n 563), art 34, §3.

[571] 'Freedom of speech vs. information security? Key quotes from UkraineWorld's event at Kyiv Security Forum 2019' (Ukraine world,18 April 2019) < https://ukraineworld.org/articles/infowatch/freedom-speech-vs-information-security-key-quotes-ukraineworlds-event-kyiv-security-forum-2019> accessed 24 February 2020.

[572] Sources and data on digital participation in Ukraine (DW Akademie, 1 July 2019) <https://www.dw.com/en/sources-and-data-on-digital-participation-in-ukraine/a-49430929> accessed 21 February 2020.

[573] Decree of the President of Ukraine 'On the decision of the National Security and Defence Council of Ukraine of 28 April 2017 'On the application of personal special economic and other restrictive measures (sanctions)' 15 May 2017 №133/2017 <https://www.president.gov.ua/documents/1332017-21850> accessed 3 April 2020.

[574] Decree of the President of Ukraine 'On the decision of the National Security and Defense Council of Ukraine of 2 March 2021 'On the application, abolition and amendment of personal special economic and

under which several Russian websites, such as VKontakte and Odnoklassniki social network, Mail.ru email service provider, Kaspersky Lab cybersecurity and antivirus provider and Dr. Web anti-malware provider, and Yandex search engine company (39 websites in total) were blocked.[575]

Freedom House, the international human rights organization, notes that blocking of websites in Ukraine 'significantly limited the digital rights of Ukrainians and caused significant damage to freedom of speech, information space and Ukraine's economic interests' in its latest Freedom on the Net review.[576] According to the National Coordination Center for Cyber Security of Ukraine under the NSDC: 'VK Unblock extension for Chrome browsers, Edge contained malicious code to steal data from Google accounts (including mobile activity, geolocation, etc.)'.[577] In total, more than 3 million users have installed such malicious applications; the main countries targeted were France, Ukraine, and Brazil. Malicious extensions are currently blocked by Google and Microsoft. Therefore, the issue of sanctions and blocking of websites can be considered from different points of view.

In the so-called Enigma case № 757/38387/19-к,[578] the imposition of an arrest on 19 websites was considered. The case involved law enforcement officials and civil society activists who published a series of investigations on blogging platforms challenging the court's decision. The blockade has caused outrage because the law only allows sites to be blocked completely if they distribute child pornography. The owner of the Enigma website notes that the project was developed as an element of information counteraction to Russian information operations and a website that was to become an alternative source of information for the Ukrainian audience of information of such an organization. Such case law opens up opportunities for extremely serious abuses and violations of freedom of expression and freedom of the media.

The Holosiivskyi District Court of Kyiv has ruled to block access to 426 sites in Ukraine. The relevant decision, which must be implemented by Internet providers and mobile operators, was announced on Thursday, February 25, by the National Commission for State Regulation of Communications and Informatization. Among the blocked - the site of

---

other restrictive measures (sanctions)' 23 March 2021 №109/2021 <https://www.president.gov.ua/documents/1092021-37481> accessed 3 April 2020.

[575] Decision of the National Security and Defence Council of Ukraine 'About application of personal special economic and other restrictive measures (sanctions)' 28 April 2017 <https://zakon.rada.gov.ua/laws/show/n0004525-17#n2> accessed 3 April 2020.

[576] Adrian Shahbaz, Allie Funk, 'Freedom House official website link: Pandemics digital shadow, article' (Freedom House) <https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow#footnote12_9h7bed5> accessed 1 June 2021.

[577] National Cyber Security Coordination Center, 'The application for bypassing Vkontakte locks stole personal data' (National Cyber Security Coordination Center of Ukraine official Facebook page, 5 February 2021) <https://www.facebook.com/ncsccUA/posts/227197159022642> accessed 1 June 2021.

[578] Case № 757/38387/ 19к (18 February 2020) (Kyiv Court of Appeal) <https://reyestr.court.gov.ua/Review/87671973> accessed 1 June 2021.

the Vinnytsia edition of '20 minutes', the Russian news agency RBC, the Russian blog platform LiveJournal and part of the platform for software developers Github gist.github.com. In addition, the list of blocked also included the telegram-statistics service TGStat. Police and prosecutors do not support the decision of the Holosiivskyi District Court of Kyiv to block 426 sites and will appeal. After the media response, the police withdrew the letter to the NCCIR. The prosecutor's office also initiated an investigation into the incident: in the absence of corpus delicti, the case was closed.

1.3. The right to fair trial

According to the innovations in the legislation of Ukraine, website owners are obliged to post information about themselves or contact information on their own websites and / or in the WHOIS service.[579] Despite this rule, not all site owners follow it. In defamation cases, finding an alleged infringer can be difficult if the domain name is registered abroad and / or hosting services are ordered from abroad. In case № 910/16699/19 [580] [the website owner was accused of posting inaccurate, untrue and discrediting the business reputation of the LLC with information that degraded the honor, dignity and business reputation of the plaintiff, which was disseminated on the website. However, the registrar and hosting provider of the domain name are foreign entities - non-resident legal entities.] Thus, the plaintiff lost the case, as it was not possible to prove the guilt of the defendant due to insufficient evidence, taking into account foreign registration. However, there is also case law when the court immediately refuses to initiate proceedings on the application for establishing the fact of inaccuracy of the information and its refutation, referring to the fact that the applicant does not have evidentiary information to establish a proper defendant in court. The main violation of human rights in the context of such issues is the right to privacy and family life.[581]

Since 2014, 118 court verdicts have been handed down in cases of actions on the Internet that may threaten the state.[582] The largest number of court decisions concerned statements that affected national security. Thus, 69 sentences were handed down for undermining territorial integrity, and 54 for actions aimed at forcible change or overthrow of the constitutional order. The fairness of the decisions is questionable, as the judges relied on evidence relating to specific knowledge. Instead of examining in detail the content and context of such positions, the judges based their decisions on some expertise. Here, forensic experts analyzed the semantic and textual examinations of messages on the social network. This was argued as a violation of the right to a fair trial, as the owners of

[579] The Law of Ukraine 'On Copyright and Related Rights' 1993 № 3792-XII p. 11, art. 52-1 <https://zakon.rada.gov.ua/laws/show/3792-12#52-1> accessed 1 June 2021.
[580] Case № 910/16699/19 (4 August 2020) (Economic Court of Kyiv) <https://reyestr.court.gov.ua/Review/89739526> accessed 1 June 2021.
[581] Case № 369/1469/19 (19 September 2019) <http://www.reyestr.court.gov.ua/Review/79701294 > accessed 01 June 2021.
[582] Mykola Myrnyi, 'Analytical report 'Freedom of Speech on the Internet' (Human Rights Platform, 19 April 2020). <https://www.ppl.org.ua/yak-ukra%D1%97na-karaye-za-nezakonnu-informaciyu-v-interneti.html> accessed 1 June 2021.

Facebook groups with several members and thousands of active audiences were punished equally. Judicial decisions in such cases lack clear mechanisms for dealing with criminal content. If it is proved that the information poses a danger to the state and society, then legal instruments should be in place that would have an impact on such information. But Ukraine does not have such tools at the moment.

However, pro-Russian and separatist sympathizers are not the only ones on the dock under Article 109 of the Criminal Code. Thus, in February 2016, the court considered the case of a 22-year-old student who reposted a post on one of the nationalist groups on his VKontakte page under the nickname 'Bogdan Mazepa.'[583] This and several other letters were considered by the court as calls to overthrow the current constitutional order. Even comments in public posts become the subject of the investigation. An example is the case of Uzhhorod musician Yuri B., who in January 2017 commented on a post in the Facebook group 'Peresichka' Uzhhorod' calling to gather for a rally near the Transcarpathian Regional State Administration.[584]

The public sector and experts in this field should be involved in the development of new Internet standards to compete for knowledge and explain the basic principles of cooperation in technology and human rights.

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

2.1 External instruments of data protection in Ukraine

For the first time, the protection of personal data in Ukraine received its regulatory consolidation with the ratification in 1973 of the International Covenant on Civil and Political Rights 1966.[585] In addition to universal international treaties, the relevant rules are contained in Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms 1950.[586] These regulations became the source of personal data protection rules in Ukraine.

Then, the practice of the European Court of Human Rights should be mentioned. For example, Zaichenko v. Ukraine case describes an infringement into private life by receiving personal data about applicant's mental health by law enforcement agencies.[587] In Surikov v. Ukraine case the applicant's employer unlawfully collected, stored and used personal data

[583] Case № 591/442/16-к (4 March 2016) (Zarichny District Court of Sumy) <https://reyestr.court.gov.ua/Review/55398181> accessed 1 June 2021.
[584] Case № 308/1221/17 (10 February 2017) (Uzhhorod City District Court) <https://reyestr.court.gov.ua/Review/64585422> accessed 1 June 2021.
[585] The International Covenant on Civil and Political Rights 1966 <http://www.un.org.ua/images/International_Covenant_on_Civil_and_Political_Rights_CCPR_eng1.pdf> accessed 1 June 2021.
[586] Convention for the Protection of Human Rights and Fundamental Freedoms 1950 <https://zakon.rada.gov.ua/laws/show/995_004#Text> accessed 1 June 2021.
[587] Zaichenko v Ukraine App no 45797/09 (ECtHR, 6 July 2015) <http://hudoc.echr.coe.int/rus?i=001-152598> accessed 1 June 2021.

about his mental health in connection with the latter's application for promotion, and also disclosed this information to the public at large.[588]

EU association process presupposes conformity of the Ukrainian data privacy regulations with the European standards.[589] Ukraine's priority is to get the EU's recognition of an adequate level of its personal data protection in accordance with "the highest European and international standards, in particular the relevant documents of the Council of Europe'.[590] Therefore, as of today, one of the most modern documents in the field of personal data protection is the GDPR.

According to experts, the extraterritorial effect of GDPR is of significant importance to Ukraine since it applies to companies anywhere in the world which come into contact with EU residents' data.[591] For instance, GDPR may extraterritorially apply to a Ukrainian company developing a fitness application that monitors user activity in the EU. This may illustrate 'monitoring the behavior of data subjects, if such behavior takes place in the EU'[592] rule. Another example, when developing a SaaS platform for a restaurant or a vet clinic, software developers get access to personal data of people who sign up (waiters, doctors, or pet owners). According to the GDPR, getting access to any personal data, even if this data is not stored on any device, means personal data processing.[593]

2.2 The concept of 'personal data' under the Ukrainian law

Ukrainian legislation provides for more than one type of information related to personal data. The Law of Ukraine 'On Personal Data Protection' defines personal data as any information about an individual who is identified or can be identified.[594] The Law of Ukraine 'On Information' uses the term 'information about person'.[595] As such, the Ukrainian legislation fixes several different terms for information related to an individual. Researchers stress that given the same definition and the premise that all information capable of individualizing and identifying a person as a participant in public relations

[588] Surikov v Ukraine App no 42788/06 (ECtHR, 26 April 2017) <https://jurisprudencia.mpd.gov.ar/Jurisprudencia/Surikov%20vs%20Ukraine.pdf> accessed 01 June 2021.
[589] Sayenko Kharenko, 'Analysis of Data Privacy Laws and Legislation in Ukraine' Final Report (the 'Memorandum')' (Sayenko Kharenko, 14 September 2020) p. 47 <https://ecpl.com.ua/wp-content/uploads/2020/09/ENG_09142020-_CEP_Final-Report.pdf> accessed 1 June 2021.
[590] The Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part: <https://zakon.rada.gov.ua/laws/show/984_011#Text> accessed 1 June 2021.
[591] Tatiana Gordienko, 'GDPR in Ukraine: who is covered by the new regulations?' (Detector Media, 4 February 2019) <https://detector.media/infospace/article/144571/2019-02-04-gdpr-v-ukraini-khto-pidpadaie-pid-diyu-norm-novogo-reglamentu/> accessed 1 June 2021.
[592] Complete guide to GDPR compliance <https://gdpr.eu> accessed 1 June 2021.
[593] Lida Klymkiv, 'GDPR — how it affects Ukrainian companies' (Dead Lawyers Society, 15 March 2018) <https://medium.com/dead-lawyers-society/gdpr-how-it-affects-ukrainian-companies-ce9ed3d0dc8> accessed 1 June 2021.
[594] The Law of Ukraine 'On Personal Data Protection' (n 554).
[595] The Law of Ukraine 'On Information' 1992 № 2657-XII <https://zakon.rada.gov.ua/laws/show/2657-12#Text> accessed 1 June 2021.

belongs to 'personal data', it should be recognized that the concepts of 'personal data' and 'information about person' are identical.[596] However, it is not as simple as it might see at first sight.

The Law of Ukraine 'On Information' propose another type of information, namely confidential, and distinguishes confidential information from other information to which access is restricted by an individual or legal entity.[597] Certain information is treated as confidential *per se* and does not require to be additionally protected. These can be nationality, education, marital status, religious beliefs, state of health, as well as address, date and place of birth.[598] Any other information about a person is not treated as confidential. As such, a person may deliberately restrict access to such information. Importantly, even if such information does not refer to personal data.

Thus, the Constitutional Court pointed out that there is also confidential information which should not be treated as personal data.[599] The Law of Ukraine 'On Access to Public Information' provides for additional rules on access to such information[600]. For example, confidential information may contain information of public interest and thus may be disclosed and provided upon request, in the case of information about a person nominated for election to a position in government or another significant public position, holds such a position.[601] The public need in this case stems from the fact that only with access to this information the voter will be able to obtain complete information about the candidates and make an informed and conscious choice.[602] Thus, not all information about a person which is personal data can be treated as confidential and enjoy the same level of legal protection.

2.3 Liability for violation of legislation in the field of personal data protection

The right to privacy is one of the most important rights in any democratic society. The limits of lawful interference with private life at the legislative level are ensured by measures of legal responsibility.

To begin with, a person can independently protect their personal data through non-jurisdictional forms of protection. Such self-defence provides for the possibility of using certain means of counteracting violations and unlawful encroachments, which are not prohibited by law and do not contradict the moral principles of society, without recourse to

[596] Romanyuk I.I., 'Protection of the right to personal data in Ukraine (civil law aspect)' (Kyiv, 2015), 267 p.
[597] The Law of Ukraine 'On Information' 1992 (n 595).
[598] Resolution of the Constitutional Court of Ukraine 2012 No 2-рп/2012 <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text> accessed 1 June 2021.
[599] ibid.
[600] Law of Ukraine 'On access to public information' Scientific and practical commentary Kyiv, 2012. 38 p.
[601] ibid, 39 p.
[602] Zakharov E. Yu., 'Violation of freedom of expression during the 2006 election campaign 2006'(Kharkiv Human Rights Group, 7 March 2006) <http: //www.khpg.org/index.php? Id = 1141752068> accessed 1 June 2021.

the competent authorities. The state also ensures the protection of personal data through the institution of the Ombudsman.

The mechanism of judicial protection of a person's right to privacy and direct protection of violated rights in the field of personal data occurs in the process of judicial proceedings: civil, administrative, criminal.

The legal basis of civil liability should be considered within the set of personal non-property rights of an individual, enshrined in the Civil Code of Ukraine,[603] as well as a number of articles that determine the general procedure for protection of civil rights and interests. In the system of legal liability, civil liability is primarily restorative and compensatory, its priority is to return the position of the person whose rights have been violated, to the state it was at the time of the civil offense. That is, a person whose rights have been violated as a result of a civil offense will, first of all, have the right to compensation for moral damage, and having established a causal link between the violation of personal non-property rights and negative property consequences - and compensation for material damage.

Administrative liability in the field of personal data protection is established by Articles 188-39, 188-40 of the Code of Ukraine on Administrative Offenses.[604] However, the subject of an administrative offense is special - a person who, in accordance with the law, can process the personal data of the personal data subject.

The most severe punishment is provided in Article 182 of the Criminal Code of Ukraine[605] for violation of privacy, namely for illegal collection, storage, use, destruction, dissemination of confidential personal information or illegal alteration of such information.

After using all national remedies, person has the right to apply to the relevant international organizations of which Ukraine is a member or participant.

It follows from the above that a personal data is protected at the legislative level. Moreover, every person also has the right to judicial protection of his/her rights. However, experts say, that Ukrainian law, in fact, is not amended with key requirements for data processing and protection, defined by the Convention 108 and GDPR, therefore the protection of personal data in Ukraine is far from corresponding to European standards.[606]

---

[603] The Civil Code of Ukraine 2003 № 435-IX <https://zakon.rada.gov.ua/laws/show/435-15#Text> accessed 21 June 2021.
[604] The Code of Ukraine on Administrative Offenses 1984 № 8073-X< https://zakon.rada.gov.ua/laws/show/80731-10#Text> accessed 1 June 2021.
[605] The Criminal Code of Ukraine 1984 №2341-III <https://zakon.rada.gov.ua/laws/show/2341-14#Text> accessed 1 June 2021.
[606] Data Protection Day: Does Data Protection in Ukraine Meet International Standards? (Council of Europe, 27 January 2021)
<https://www.coe.int/en/web/kyiv/-/data-protection-day-does-the-personal-data-protection-in-ukraine-meet-international-standards-> accessed 21 June 2021.

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 necessity of self-regulation of data protection arises from a number of international commitments of Ukraine and recommendations of international bodies, probably the earliest one being the Recommendation № 32 of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) that, back in 2001, set some general recommendations that would establish trustful relations between the government and the independent data processors and controllers in the mentioned sphere.[607] Probably the most publically well-known one, however, is the Association Agreement with the European Union. Bringing the data protection legislation in compliance with the requirements of the General Data Protection Regulation ((EU) 2016/679) is one of Ukraine's important commitments which is encouraged by the Council of Europe.[608] In general, self-regulation corresponds with the principle of subsidiarity.[609] However, the independent watchdogs of the Ukrainian European integration express concerns about the rates of improvement of current legislature: for instance, the experts of the 'Pulse of the Agreement' monitoring agency note that no progress has been made so far to implement the necessary amendments - it means Ukraine has missed the mentioned aspect of legislature harmonization. In fact, no draft of the law containing the amendments has been registered in the Parliament so far.[610]

In the EU, companies share the responsibility of data protection under the General Data Protection Regulation of 2016 while the US jurisdiction has no such comprehensive document on the federal scale. In Ukraine, the Law 'On Personal Data Protection' regulates these details.[611] It provides, inter alia, that the Parliament Commissioner for Human Rights ('Ombudsperson') shall prepare and approve the model rules for personal data processing for the businesses' usage.[612] These rules do not differ in their wording from one data controller to another. However, the above-mentioned Law provides the opportunity for the professional communities, civil associations and other legal entities to

---

[607] Recommendation No. 32, adopted by seventh session of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) (1st edn, ECE/TRADE/277, 2001) <https://unece.org/fileadmin/DAM/cefact/recommendations/rec32/rec32_ecetrd277.pdf > accessed 30 January 2020.

[608] 'New data protection legislation of Ukraine is being developed with the expert support of the Council of Europe' (Council of Europe, 30 January 2020) <https://www.coe.int/en/web/national-implementation/-/new-data-protection-legislation-of-ukraine-is-being-developed-with-the-expert-support-of-the-council-of-europe> accessed 30 January 2020.

[609] Glossary of summaries (Eur-Lex) <https://eur-lex.europa.eu/summary/glossary/subsidiarity.html> accessed 1 June 2021.

[610] Monitoring the improvement of legislation on personal data protection in order to bring it in line with Regulation (EU) 2016/679 (European integration portal) <http://pulse.eu-ua.org/ua/streams/human-rights-justice-and-anticorupption/2020-substream5-95> accessed 27 January 2021.

[611] The Law of Ukraine 'On Personal Data Protection' (n 554).

[612] ibid, art. 6, § 10.

draft, taking into consideration the special nature of personal data they deal with, own codes regulating data protection unless the terms of these drafts contravene the Law.[613] Such an opportunity was used, for instance, by the All-Ukrainian Association of the Administrative Service Centres that has adopted such a code in cooperation with the Ombudsperson.[614] It urges, inter alia, the administrative service centres to delete or de-personalize personalized data after the person stops using their services.[615] The Ombudsperson or the entitled officials may as well demand the deletion of personal data.[616]

Speaking about the cooperation of the two sectors in Ukraine, the above-mentioned Law provides that, generally, the Ombudsperson is responsible for the coordination of such cooperation. The Ombudsperson is entitled to collaboration and consultations, inter alia, with the representatives of data processors to determine the best decisions on the way data is handled. Also, the Ombudsperson is to communicate the final decisions regarding the state policy to the controllers of personal data.[617]

Generally, most of the major Ukrainian businesses have their own terms of privacy. The latter often warn that the data may be transmitted to the government officials solely for the legitimate purposes and on the legitimate grounds.[618] They also warn the users entrusting their personal data of the purposes of its usage and the explicit reasons of saving some details after the owner of personal data stops using the provided services (e.g. for the scientific or statistical purposes).

The controllers and processors of the personal data which is considered sensitive for the rights and freedoms of subjects of personal data are also obliged by the law to establish a separate division responsible for the personal data policy and to communicate the decision on establishment to the Ombudsperson who, in the future, will interact with the respective division or a responsible employee.[619] The 'sensitive' information includes that regarding race and ethnicity, health and sexual life, biometric and genetic data, membership in religious, politic or other organizations etc.[620] Once the business is accused of the violation

---

[613] ibid, art. 27, § 2.
[614] All-Ukrainian Association of Centers for Administrative Services, 'Code of Conduct for Processing and Protection of Personal Data in Centers for Administrative Services' (All-Ukrainian Association of Administrative Service Centers, 2020) <https://drive.google.com/file/d/1J3HEaBbgwvqv9rVUtk41vI7El1wtTB-2/view?fbclid=IwAR2D-fr-kypIcdba-gOGtcJe3mt_RhXPs7TUst0ClAyZCvveLqakLCiF33M> accessed 1 June 2021.
[615] ibid, art. 2.1.
[616] The Law of Ukraine 'On Personal Data Protection' (n 554), art. 15, § 3.
[617] ibid, art. 23, § 1, 6, 12.
[618] See, for example, Kyivstar privacy policy. 'STAR GUARD family' services (Kyivstar, 29 May 2019) <https://cdn.kyivstar.ua/sites/default/files/about/privacy_policy_star_guard_family_eng.pdf> accessed 1 June 2021.
[619] The Law of Ukraine 'On Personal Data Protection' (n 554), art. 24, § 2.
[620] Decree of the Ukrainian Parliament Commissioner for Human Rights 'On approval of documents in the field of personal data protection' 08.01.2014 № 1/02-14 <https://zakon.rada.gov.ua/go/v1_02715-14> accessed 1 June 2021, art. 1, § 1.2.

of law concerning personal data, the Ombudsperson organizes an audit concerning allegations.

The state online platform 'Diia' (lit. 'Action') organizes consultations with the representatives of the private sector for the exchange of ideas and opinions on the safety of data. It has recently introduced the Data Protection Self-Assessment Tool designed to help the organizations understand the legislative basis better as well as set an individual plan of actions on data protection created in the cooperation with the United Nations Development Program, the Ministry of Foreign Affairs of Denmark and the Privacy Hub, one of Ukraine's top non-governmental organizations in the privacy sphere.[621]

From another side, the self-regulation of data protection is not flawless. In the 2019 annual report, the Ombudsperson noted the violation of privacy rules by multiple institutions, mostly the state ones. For example, one of the district administrations of the city of Kyiv posted on its official website a report containing a data of some individuals as personal as birth date, passport number and place of registration while the number of schools and recreational institutions demanded from parents eager to admit their children thereto the reports on vaccination.[622] The conclusion can be made that the private and public sectors 'peacefully coexist' in the Ukrainian field of personal data protection. Still, some issues of concern remain; for example, as the IAPP researchers noted, the notion of 'consent' for data processing 'has become such a big thing that it is almost worshiped': this processing ground is used so widely that it leaves almost no place for other ones (e.g. legitimate interests, contract) - so, the concept of consent is, according to the researchers, gradually becoming underestimated.[623]

But probably the most important notion of the experts pertains to the necessity of establishing an independent authority responsible for data policy in Ukraine. The institution of Ombudsperson should, experts believe, be dealing more with human rights, for which it actually was established, and its overload with extrinsic, in character, functions causes concerns it might fail to work efficiently in the future in the above-mentioned capacity.[624] It seems more likely that the transition of Ukraine to the 'American' (decentralized) scenario of data protection will take place once the data commissioner assumes the duties - however, a level of governmental control (at least the modest one) is likely to remain present. This is likely to be practically implemented under the auspices of the Ministry of Digital Transformation: as Mykhailo Fedorov, head of the mentioned

[621] Diia.Business, Data protection self-assessment tool (Diia.Business) <https://business.diia.gov.ua/en/selftesting/data-protection-tool> accessed 1 June 2021.
[622] Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in 2019 (Secretariat of the Commissioner, 2020) <http://www.ombudsman.gov.ua/files/Dopovidi/zvit%20za%202019.pdf> 22 May 2020.
[623] Artem Kobrin, Dmytro Korchynskyi, Vladislav Nekrutenko, 'Ukrainian GDPR: The reality and future of privacy legislation in Ukraine' (IAPP, 28 September 2020) <https://iapp.org/news/a/ukrainian-gdpr-the-reality-and-future-of-privacy-legislation-in-ukraine/> Accessed 1 June 2021.
[624] ibid.

Ministry, noted, it may become a driving force for strengthening privacy culture and regulatory policy in Ukraine.[625] Also, this version may be supported by the fact that many companies are forced by their European customers and their expectations to already comply with GDPR standards - without any coercion from the state authorities. As the 'Analysis of Data Privacy Laws and Legislation in Ukraine' 2020 report by the Sayenko Kharenko law firm noted, the majority of Ukrainian-based businesses having personal data processing as a core requirement for running their business feel the obligation to raise their internal standards to successfully comply with the GDPR - *inter alia*, for competitive reasons. Furthermore, Ukrainian businesses which offer services and goods to EU residents or which monitor the behaviour of data subjects located in the EU automatically fall into the scope of the GDPR according to its Article 3(2).[626]

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 under the national law?

Under the Ukrainian law, the right to privacy covers mainly the right to privacy of personal and family life. This, by definition, includes rights to confidentiality of personal information (e.g. any identifying or sensitive information) and correspondence, as well as personal data protection.

The right to data privacy emanates from the right to personal and family life enshrined in the Constitution of Ukraine. Article 32 of the Constitution provides that 'an interference with these rights is possible only if provided by law, in the interests of national security, economic prosperity and the protection of human rights'. Article 32 of the Constitution also grants 'the right to refute and withdraw inaccurate information about oneself and family members, as well as the right to compensation of damages, including morals, that occurred as a result of collection, processing, usage and dissemination of such information'.[627] These provisions are also enshrined in the Civil Code of Ukraine.[628] The Constitution of Ukraine also protects the confidentiality of the correspondence, including phone calls and mail.[629]

The Constitutional Court of Ukraine in its decision in case № 1-9/2012 defined the scope of personal life as one including personal, family, sexual, friendly, professional, business

[625] ibid.
[626] Sayenko Kharenko, 'Analysis of Data Privacy Laws and Legislation in Ukraine: Final Report (the 'Memorandum')' (Sayenko Kharenko, 14 September 2020) <https://ecpl.com.ua/wp-content/uploads/2020/09/ENG_09142020-_CEP_Final-Report.pdf> accessed 1 June 2021.
[627] Constitution of Ukraine (n 563), art 32.
[628] The Civil Code of Ukraine 2003 №435-IV <https://zakon.rada.gov.ua/laws/show/435-15#Text> accessed 28 February 2021, arts 301 - 302.
[629] Constitution of Ukraine (n 563), art 32.

and other forms of relationships and activities.[630] The Court further underlined that it is impossible to determine all forms of activities constituting personal and family life since they are part of natural human rights that are not exhaustive.[631]

The scope of the privacy of personal and family life was further extended, and now includes the privacy of confession,[632] adoption,[633] correspondence,[634] notary actions,[635] health,[636] attorney-client privilege,[637] bank secrecy.[638]

The Code of Criminal Procedure also protects the rights to privacy. Non-interference with private life is one of the key principles of criminal procedure enshrined therein.[639] Article 15 of the Code of Criminal Procedure prescribes that information regarding the private life, obtained in the course of investigation, shall not be used for the purposes not prescribed by the Code.[640]

The Law of Ukraine 'On information' defines confidential information as one allowing the identification of a person. The law does not provide an exclusive list of information regarded as confidential. Instead, it provides that information about the ethnical origin, education, family, religion, health, address, date and place of birth shall be regarded as confidential per se.[641]

In this regard, the Law 'On information' followed an approach[642] set in the decision of the Constitutional Court of Ukraine in case № 18/203-97, in which the Court stressed that it is prohibited not only to collect, but also to store, use and disseminate confidential information about a person without his/her prior consent.[643]

The Constitutional Court of Ukraine played an important role in the development of data protection regulations. For instance, in its decision in case № 1-9/2012, the Constitutional

---

[630] The Resolution of the Constitutional Court of Ukraine of 20 January 2012, case № 1-9/2012, <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>, accessed 28 February 2021, § 3.1.

[631] Ibid, § 3.1.

[632] The Law of Ukraine 'On freedom of conscience and religious organizations' 1991 № 987-XII, <https://zakon.rada.gov.ua/laws/show/987-12#Text> accessed 28 February 2021, art 3.

[633] The Family Code of Ukraine 2002 № 2947-III <https://zakon.rada.gov.ua/laws/show/2947-14#n11> accessed 28 February 2021, arts 226 – 231.

[634] The Civil Code of Ukraine 2003 № 435-IX , <https://zakon.rada.gov.ua/laws/show/435-15#n1651> accessed 28 February 2021, art 306.

[635] The Law of Ukraine 'On notary' 1993 № 3425-XII, <https://zakon.rada.gov.ua/laws/show/3425-12#n66> accessed 28 February 2021, art 8.

[636] Civil Code of Ukraine 2003 № 435-IX <https://zakon.rada.gov.ua/laws/show/435-15#n1651> accessed 28 February 2021, art 286.

[637] The Law of Ukraine 'On Bar' 2013 № 5076-VI, <https://zakon.rada.gov.ua/laws/show/5076-17#n173> accessed 28 February 2021, art 22.

[638] The Law of Ukraine 'On banks and banking' 2001 № 2121-III, <https://zakon.rada.gov.ua/laws/show/2121-14#n983> accessed 28 February 2021, art 60.

[639] The Code of Criminal Procedure 2012 № 4651-VI, <https://zakon.rada.gov.ua/laws/show/4651-17#n431>, accessed 28 February 2021, art 7.

[640] Ibid, art 15.

[641] The Law of Ukraine 'On information' 1992 № 2657-XII, <https://zakon.rada.gov.ua/laws/show/2657-12#n84> accessed 28 February 2021, art 11.

[642] Ibid, art 11.

[643] The Resolution of the Constitutional Court of Ukraine 2012, № 18/203-97, <https://zakon.rada.gov.ua/laws/show/v005p710-97#Text> accessed 03 February 2021, § 1 of the resolutive part.

Court provided that it is necessary to obtain a data subject's consent for the collection, storage, use and dissemination of such information by any person, including state and local bodies, and that the collection, storage, use and dissemination of such information constitutes a violation of the right to privacy granted with the Article 32 of the Constitution.[644] Moreover, the Court stressed that a natural person to whom confidential information relates has the right to freely determine the procedure for acquaintance with such information, as well as the right to keep it in secret.[645]

The right to data privacy was further expanded with the adoption of the Law 'On Personal Data Protection', which implemented the Constitutional Court's approach. The Law defines personal data as data relating to an identified or specifically identifiable natural person.[646] It provides that such data is protected by law.[647] This law provides data subjects with a possibility to not only protect their rights in court, but also to file complaints to the Commissioner for Human Rights of the Verkhovna Rada (Parliament) of Ukraine ('Ombudsman').[648]

During 2020 (the most recent data available), the Ombudsman considered 2 031 complaints concerning privacy violations (two times more than in 2019), conducted 67 inspections and rendered 9 protocols on privacy violations.[649] The Ombudsman underlined that most complaints were related to unlawful personal data processing by debt recovery agencies.[650]

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

Unlike GDPR, Ukrainian legislation does not formally distinguish the rights to restrict data processing and to object to it.

Data subjects have a right to restrict the processing of their personal data when providing consent for such processing as well as to withdraw their consent[651] if the only basis for processing is the consent of the personal data subject.[652]

Data subject may also make a request to the controller of personal data with an objection to processing, or request to change the scope or content of processed data.[653] The data controller must consider such a request within 10 days of receipt. If the data controller

---

[644] The Resolution of the Constitutional Court of Ukraine 2012, case № 1-9/2012, <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>, accessed 28 February 2021, § 1 of the resolutive part.
[645] Ibid, § 3.
[646] The Law of Ukraine 'On Personal Data Protection' (n 554), art 2.
[647] Ibid, art 5.
[648] Ibid, art 8.
[649] Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2020 (Secretariat of the Commissioner, 2021) <https://www.ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf> accessed 01 June 2021, p. 21 - 22.
[650] Ibid, p. 22.
[651] The Law of Ukraine 'On personal data protection' (n 554), art 8 §2.
[652] Decree of the Ukrainian Parliament Commissioner for Human Rights "Typical procedure for processing personal data" 2014 № 1/02-14, <https://zakon.rada.gov.ua/laws/show/v1_02715-14#n11> accessed 03 February 2021, art. 2.15.
[653] The Law of Ukraine "On personal data protection" (n 554), art. 2.12.

finds that personal data of a data subject is processed illegally, the controller is obliged to stop processing of such personal data and notify the data subject.[654] If the data controller will find that personal data of the subject is unreliable, the controller must stop processing such personal data or change its scope or content and notify the data subject.[655]

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?

Unlike as set under the GDPR, there is no general obligation to notify the data subject in case of data protection breach. This, consequently, causes significant problems, especially considering numerous data protection breaches involving the leakage of personal data during recent few years in Ukraine. For example, in September 2020, SoftServe, one of the largest Ukrainian software outsourcing companies, suffered a cyber-attack, in result of which a leak of personal data of about 200 employees were leaked, including scanned copies of passports.[656] Another example is a personal data leakage from career.gov.ua – Ukrainian governmental job portal. As a result, scan-copies of passports, diplomas and graduation certificates of numerous people become publicly available.[657]

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

5.1. Which bodies conduct such review?

'The review' (or 'control') means establishing the compliance of personal data processing with the requirements of the Constitution of Ukraine, the Law of Ukraine 'On Personal Data Protection', the Standard Procedure for Personal Data Processing, and effective international treaties of Ukraine on personal data protection.[658]

With the amendments made in 2014 to the Law of Ukraine 'On Personal Data Protection', the courts and the Ombudsman are responsible for the review.[659]

The courts exercise their review function during judicial proceedings (civil, criminal, administrative and during hearings of administrative offences cases).[660] Also, the control is

---

[654] ibid, art. 2.13.
[655] ibid, art. 2.13.
[656] Maya Yarovaya, 'New "spill" of SoftServe data: client projects and, probably, employee data' (Ain, 16 September 2020) <https://ain.ua/2020/09/16/softserve-utechka-2/> accessed 20 February 2021.
[657] 'Cisomag, 'NSDC Acknowledges Data Leak in Ukrainian Government Job Portal' (Cisomag, 20 January 2020) <https://cisomag.eccouncil.org/nsdc-acknowledges-data-leak-in-ukrainian-government-job-portal/> accessed 20 February 2021.
[658] The Ukrainian Parliament Commissioner for Human Rights, 'Control over compliance with the requirements of the legislation on personal data protection' <https://ombudsman.gov.ua/ua/page/zpd/kontrol/> accessed 20 February 2021.
[659] The Law of Ukraine 'On Personal Data Protection' (n 554), art. 21.
[660] Letter of explanation of the Ukrainian Parliament Commissioner for Human Rights for Human Rights as of 3 March 2014 № 2/9-227067.14-1/НД-129 <https://zakon.rada.gov.ua/laws/show/v7067715-14#Text> accessed 20 February 2021 (Ombudsman's Letter of explanation).

carried out through the activities of the Plenum of the Supreme Court[661], which provides clarifications on the application of the law by courts.[662]

The credentials of the Ombudsman include reviewing the complaints of data subjects, carrying out the inspections of controllers and processors, and issuing prescriptions to eliminate the detected violations, addressing proposals to the state bodies on the adoption or amendment of personal data protection regulations, cooperating with foreign actors on personal data protection etc.[663]

In order to carry out the wide range of functions described, the Ombudsman established a Department for Personal Data Protection within its Secretariat[664] and introduced the position of Ombudsman's representative for Personal Data Protection.[665]

One of the main Ombudsman's functions in the area of review is carrying out personal data controllers and/or processors' investigations. The grounds for launching an investigation could be individuals and legal entities' complaints or the Ombudsman's initiative. Inspections can be of different types, for example, scheduled or unscheduled, which are also classified as on-site or off-site.[666] The responsibilities and rights of inspection participants and other aspects related to the inspections process are regulated by the 'Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection'.[667]

Based on the inspection results, the Ombudsman and/or the authorised official[668] draws up an act of verification of compliance with personal data protection legislation. This document contains information on non-compliance or improper compliance with the personal data protection legislation or the absence of such violations.[669]

If the violation is detected, the Ombudsman or the authorised official draws up an order to eliminate the violations revealed. The order shall specify the measures to be taken by the

---

[661] Originally, the Letter referred to the 'Plenum of the High Specialized Court' instead of the 'Plenum of the Supreme Court'. However, as a result of judicial reform in 2016, high specialized courts were liquidated and the Supreme Court was established as a single court of cassation.
[662] Ombudsman's Letter of explanation (n 660).
[663] Law of Ukraine 'On personal data protection' (n 554), art. 23.
[664] The Ukrainian Parliament Commissioner for Human Rights, 'Information about the Department for Personal Data Protection'
<https://ombudsman.gov.ua/ua/page/zpd/info/> accessed 20 February 2021.
[665] M. V. Bem, I. M. Gorodisky, G. Sutton, O. M. Rodionenko, 'Personal data protection: Legal regulation and practical aspects: scientific and practical manual' 131. (Bem M. V.).
[666] Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection as of 8 January 2014 № 1/02-14
<https://zakon.rada.gov.ua/laws/show/v1_02715-14#n92> accessed 20 February 2021, par. 1.2. (Procedure).
[667] ibid.
[668] As mentioned in the par. 2.2 of the Procedure, the inspection may also be carried out by authorized officials on the basis of Ombudsman's order. Such officials may be the head of the Secretariat and his/her deputy, Representatives of the Ombudsmen, heads of structural subdivisions of the Secretariat and their deputies, employees of the Secretariat of the Ombudsmen.
[669] ibid, par. 5.1 – 5.3.

controller and/or processor, the period of execution of the order, and informing about the elimination of the violations.[670] In case of noncompliance, the Ombudsman or authorised official draws up a report on an administrative offence, as envisaged in Article 188-40 of the Code of Administrative Offenses of Ukraine.[671]

Also, the Ombudsman or authorised official draws up a report on the administrative offence if the violation specified in Articles 188-39 or Article 188-40 of the Code of Administrative Offenses was revealed during the inspection. [672]

In 2019, ten protocols on administrative offences were submitted to the court. Most violations were in financial and banking services, insurance, housing and communal services, healthcare, social protection, education, personal data processing during video surveillance, accounting of administrative and criminal offences.[673]

If the inspection reveals a criminal offence, the Ombudsman sends the investigation materials to law enforcement agencies (for details, please see Question 9).[674]

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

The data subject may file a complaint to the data controller and/or processor, the Ombudsman Office, or apply to court.[675] Such appeals shall take place in the manner prescribed by law on the Ombudsman's credentials in the field of data protection or the relevant procedural codes.

The Ombudsman may also initiate the administrative legal proceeding. As described earlier, it is done in case the violation of legislation on personal data protection is detected during the Ombudsman's inspections. In case such violation was revealed, the Ombudsman or authorised official draws up a report or an administrative offence protocol. A copy of this protocol is sent to the court of the first instance at the place of the offence.[676]

The case on an administrative offence is usually reviewed within 15 days from the date of receipt by the court of the administrative offence protocol. Based on the case outcome, a decision is made. In case of disagreement with the decision, the prosecutor, processor, controller or data subject may appeal it in the court of the second instance within ten days from the date of issuance of the decision.[677]

---

[670] ibid, par. 5.10, 5.11.
[671] Ibid, par. 5.15.
[672] Ibid, par. 5.16.
[673] Annual Report 2019, op cit, p. 193.
[674] Ibid, par. 5.17.
[675] The Law of Ukraine 'On Personal Data Protection' (n 554), art. 8.
[676]The Code of Ukraine on Administrative Offenses №80731-X <https://zakon.rada.gov.ua/laws/show/80732-10#Text> accessed 20 February 2021, art. 257.
[677] Ibid, art. 294.

If there are signs of a criminal offence, the Ombudsman must also send the investigation materials to law enforcement agencies (for details, see Question 9).[678]

The measures provided by the personal data protection legislation are aimed at stopping or correcting violations and do not envisage compensation to the data subject.[679] Therefore, the data subject has the right to sue for damages caused by a violation of its right to personal data protection according to the established civil procedure.[680]

5.3. What kind of sanctions are imposed as penalties for the violation of the personal data protection legislation?

Article 28 of the Law 'On Personal Data Protection' provides for penalties for violations of the personal data protection provisions under the current legislation of Ukraine.[681] Such liability may be administrative or criminal, both of which are applied to natural persons only (e.g., managers or DPOs of data controllers or processors). A data subject also has the right to claim compensation for material or moral damage.[682]

Provisions on administrative liability are provided by Articles 188-39 and 188-40 of the Code of Ukraine on Administrative Offenses. In particular, sanctions in the form of fines up to UAH 34,000 (approx. EUR 1,000) for the following violations are envisaged:[683]

Failure to notify or untimely notification of the Ombudsman on the processing of personal data or the change of information subject to the notification, notification of incomplete or inaccurate information;

Non-compliance with legitimate requests of the Ombudsman or authorised officials regarding the prevention or elimination of violations of the legislation on personal data protection;

Non-compliance with the procedure for the protection of personal data established by law, which has led to illegal access to this data or violation of the rights of the data subject;

Non-compliance with legitimate requests of the Ombudsman or the authorised officials. For example, denial of access to documents or information necessary for the inspection, etc.

Regarding criminal liability, Article 182 of the Criminal Code of Ukraine provides for sanctions in the form of fines, corrective labour, arrest, restriction of freedom, or

---

[678] O. O. Tikhomirov and others, 'Law, society, state, security: information dimension' <http://zpd.inf.ua/page19.html#top> accessed 20 February 2021.
[679] Bem M. V. (n 665), 146.
[680] Ombudsman's Letter of explanation (n 660).
[681] The Law of Ukraine 'On Personal Data Protection' (n 554), art. 28.
[682] Ombudsman's Letter of explanation (n 660).
[683] The Code of Ukraine on Administrative Offenses №80731-X <https://zakon.rada.gov.ua/laws/show/80732-10#Text> accessed 20 February 2021, art.188-39, 188-40.

imprisonment for illegal collection, storage, use, destruction, dissemination of confidential personal information or illegal alteration of such information.[684]

5.4. Conclusion regarding the effectiveness

During the analysis of review measures and related aspects, we concluded that the review mechanism does not provide effective protection of data privacy in its current state.
First, the articles on liability for violations of legislation on personal data protection due to certain inaccuracies in the terminology and practical mechanism of their application may narrow the scope of responsibility of the data controller and may also call into question the occurrence of liability in general.[685]

Second, the amount of sanctions specified in the above articles of the Code of Administrative Offenses and the Criminal Code are unlikely to deter processors and controllers from committing violations: the minimum amount of fine equals approx. 50 EUR, while the highest fine does not exceed 1,000 EUR.[686]

Thirdly, the experts also note the significant workload on the Ombudsman and his Secretariat, as well as the lack of staff in his apparatus, which does not allow to respond effectively to requests from individuals and legal entities for violations of personal data protection, conduct inspections and other activities provided by law.[687]

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

Generally, the Constitution of Ukraine secures fundamental anti-discrimination principles, inter alia, addressing equality before the law. This principle means that any subjects of administrative and legal relations must be recognized as equal, and they must be provided with an opportunity for the realization of equality. This is manifested in the fact that during the consideration of a case against a person and a citizen, the same legal acts are applied for all (substantive norms and administrative procedural rules). Favourable or positive conditions are not created for any person during the consideration of cases.

The Law of Ukraine 'On Principles of Preventing and Combating Discrimination in Ukraine' determines who is protected against discrimination and may apply to court.

The Commissioner for Human Rights of the Verkhovna Rada of Ukraine in her 'Strategy for Prevention and Combating Discrimination in Ukraine for 2014-2017' - addressed the following issues:

---

[684] The Criminal Code of Ukraine 2001 №2341-III <https://zakon.rada.gov.ua/laws/show/2341-14#Text> accessed 20 February 2021, art. 182.
[685] Bem M. V. (n 665), 143.
[686] Alina Pravdychenko, "Personal data online: regulation problems and protection prospects" (Center of democracy and the rule of law, 21 November 2019) <https://cedem.org.ua/articles/personalni-dani-onlajn/> accessed 27 February.
[687] Bem M. V. (n 665), 144; Pravdychenko (n 686).

- the general low level of understanding of their rights by Ukrainians, their inability to objectively assess violations and demand the restoration of their rights;
- distrust of citizens in the judicial system and unwillingness to file complaints to the court in case of violation of their rights;
- misunderstanding by judges of the essence, tasks and specifics of anti-discrimination legislation;
- non-application of Art. 60 of the Civil Procedure Code of Ukraine on the reversed burden of proof in discrimination cases;
- inaccessibility of most courts for people with disabilities;
- predominant activity in the use of the judicial mechanism to protect their rights by only one protected group - people with disabilities.
Furthermore, the laws of civil and criminal procedures stipulate general non-discrimination before the code principles.

The Code of Civil Procedure of Ukraine stipulates that in cases of discrimination, the plaintiff is obliged to provide factual data confirming that discrimination has taken place. In the case of such data, proof of their absence is entrusted to the defendant.

The statement of claim must substantiate the existence of discrimination, and in accordance with the second part of Article 81 of the Code of Civil Procedure of Ukraine, the burden of proof in this category of cases is reversed.

The Law on Principles of Prevention and Counteraction of Discrimination in Ukraine dated 06.09.2012 № 5207-VI, provides many basic things to protect against discrimination and to understand its essence (for example, the law specifies the definition and types of discrimination). But, in addition, it provides for the process of identifying discriminatory actions and a number of actors responsible for the protection of human rights in this area.

Finally, there is a piece of secondary legislation issued by the Ministry Justice of Ukraine - Order of 12.03.2019 № 33 On approval of Guidelines for the identification of cases of gender discrimination and the mechanism for providing legal assistance. This act provides a test for the detection algorithm and disqualification actions in the event of it, which leads to legal action.

As a summary of the court appeal procedure, this order provides for trials in various areas of the Ukrainian process: As a summary of the recourse procedure, this order provides for processes in different areas of the Ukrainian process, which are depicted in different algorithms of action on different types of discrimination. This act also emphasizes that cases of discrimination in Ukrainian courts are a special priority, so the court in considering such cases tries to create practice on the basis of such cases and explain aspects of such offences in its decisions.

Paying attention to the above order, we can conclude that in the process for discrimination cases the following is important:

- the plaintiff must use social and law algorithms to determine whether his right has been violated due to discrimination;
- prove that the discrimination was not the defendant's responsibility;
- this category of cases is a priority for courts, so they are considered with special care in order to build judicial practice: prescribe explanations of various terms and mechanisms of protection against discrimination, which are provided in the relevant acts on this topic;
- courts and laws often draw attention to Western experience in resolving such disputes, in particular the case law of the European Court of Human Rights and international anti-discrimination acts.

From the above it can be concluded that Ukraine does not provide a large number of rules governing equality and anti-discrimination. Most norms and profile laws are designed for substantive law and the actual norm of creativity, paying less attention to the process. There are some rules that provide for equality in the process - for example, Art. 81 of the Civil Procedure Code, but mainly in practice and in the opinion of the legislator, equality in the Ukrainian process exists through the fundamental principles and norms enshrined in the Constitution of Ukraine, relevant and international acts.

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. Artificial intelligence (AI) and Big Data

Currently there is no legislation or specific proposals to regulate AI or big data. However, there was an AI policy paper adopted, a Concept on the development of AI in Ukraine, proposed on 2 December 2020 by the Cabinet of Ministers of Ukraine, which has a section on legal regulation.[688] The Concept promotes the implementation of rules maintained in the Recommendation on Artificial Intelligence.[689]

7.2. Encryption

Current legislation on encryption consists of the Law 'On Electronic Commerce', the Law 'On Electronic Trust Services', the Law 'On Electronic Documents and Electronic Document Flow', the Law 'On Information Protection in Information and Telecommunication Systems', and the Presidential Decree on Regulations on procedure of cryptographic information protection. According to the 2019 Freedom of the Net report in Ukrainian legislation places no restrictions related to the encryption tools[690]. The

[688] Order of the Cabinet of Ministers of Ukraine 'Concept on the development of artificial intelligence in Ukraine' 2020 № 1556-p, <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> accessed 1 June 2021.
[689] ibid.
[690] Freedom of the Net, 2019 Report on Ukraine, <https://freedomhouse.org/country/ukraine/freedom-net/2019> accessed 1 June 2021, § C4.

legislation on encryption may be divided into the laws on e-commerce, e-signatures and cryptography.

- E-commerce

The Law 'On Electronic Commerce' was adopted on 3 September 2015. It defines and regulates electronic transactions and formation of e-contracts.[691] The Law specifies that electronic signature shall be used to enter into contract.[692] In accordance with the Law, Internet service providers enjoy immunity from liability if they fulfil the following requirements: do not initiate information sharing ('mere conduits'), do not select recipients of the transaction, and do not change the information shared.[693]

- E-signature

In Ukraine, the specific regulation on electronic signatures consists of the Law 'On Electronic Trust Services', the Law 'On Electronic Documents and Electronic Document Flow'. The Law on Electronic Trust Services defines the key principles of electronic identification,[694] determines the rights and obligations of legal entities,[695] and establishes a specific procedure for state supervision.[696] In the Law three types of signatures are defined: the advanced electronic signature, the qualified electronic signature and the simple electronic signature.[697] The Law on Electronic Documents and Electronic Document flow establishes the legal principles of document flow and contains rules on the usage of e-documents.[698]

Cryptographic protection of information

On cryptographic protection of the information Ukraine has a Law 'On information protection in information and telecommunication systems'. It defines the cryptographic protection of information as 'a type of information protection implemented by converting information using special data in order to hide / restore the content of information, confirm its authenticity'.[699] The Law also defines the conditions of information processing in the system and establishes that the system owner bears responsibility for information protection.[700] Moreover, the Law vests the state agents with the power of issuing requirements for the protection of state information.[701] As to the secondary legislation a Presidential Decree About Regulations on procedure of cryptographic information

---

[691] The Law of Ukraine 'On Electronic Commerce' 2015 №675-VII, <https://zakon.rada.gov.ua/laws/show/675-19> accessed 1 June 2021, art. 1, art. 10.
[692] ibid, art. 3.
[693] ibid, art. 9, § 4.
[694] The Law of Ukraine 'On Electronic Trust Services' 2017 2155-VIII <https://zakon.rada.gov.ua/laws/show/2155-19?lang=uk#Text> accessed 1 June 2021, art. 1.
[695] ibid, Art. 12, 13.
[696] ibid, Art. 33.
[697] ibid, Art. 1.
[698] The Law of Ukraine 'On Electronic Documents and Electronic Document flow' 2003 №851-IV <https://zakon.rada.gov.ua/laws/show/851-15> Section 3.
[699] The Law of Ukraine 'On information protection in information and telecommunication systems' 1994 №80/94-ВР <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80> accessed 1 June 2021, Art. 1.
[700] ibid, Art. 9.
[701] ibid, Art. 10.

protection in Ukraine was issued in 1998, and amended in 2009. The decree provides definitions on the terms such as cryptographic system, systems and means of cryptographic information protection.[702] It determines that persons which have access to state secrets following a specific procedure are entitled to use cryptosystems of the classified information.[703] The Decree specifies that certified testing by having recourse to the means of encryption shall be carried out to determine the level of security from illegal access.[704]

7.3. IoT

The Internet of Things is a broad concept and involves a large number of subjects such as physical objects—that are embedded with high technology software for the purpose of exchanging data with other systems. On the Internet of things Ukraine has the Strategy for the development of the information society in Ukraine, The Concept on e-government development in Ukraine, the Law on information protection in information and telecommunication systems.

The Concept on e-government development provides for the modernization of public services and development of interaction between government and citizens with the help of information and communication technologies as well as e-government development management.[705] Moreover, the Concept calls for the development of open data infrastructure on the basis of a single state web portal, publication and regular updating of data sets in the form of open data in accordance with the public interest.[706] The Concept establishes the main areas in e-government initiative, which are the introduction of the system of electronic interaction of state electronic information resources, as well as development of cross-border electronic interaction.[707]

Other important spheres of development include the introduction of telemedicine, introduction of the electronic water balance system of Ukraine.[708] In the field of social protection it stands for the introduction of electronic hospital and in the field of human rights the Concept provides for the introduction of a national system of calls to emergency services and other life support services on a single toll-free telephone number.[709] The Strategy for the development of the information society in Ukraine indicates the need to improve the regulatory framework for ensuring proper coordination of actions of all

[702] Decree of the President of Ukraine 'On the regulations on procedure of cryptographic information protection in Ukraine' 1998 № №505/98 <https://zakon.rada.gov.ua/laws/show/505/98#Text> accessed 1 June 2021, § 2.
[703] ibid, § 7.
[704] ibid, § 6.
[705] The Decree of the Cabinet of Ministers of Ukraine 'On approving the concept on e-government development in Ukraine' 2017 № 649-2017-p <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text> accessed 1 June 2021.
[706] ibid.
[707] ibid.
[708] ibid.
[709] ibid.

stakeholders during the implementation of e-democracy tools; increasing the level of information representation of Ukraine in the Internet space, and increasing at the state level the importance of the Ukrainian segment of the Internet.[710] Moreover, Ukraine has a draft Law on cryptocurrency. Article 13 requires licensing of cryptocurrencies.[711] Article 16 places restrictions on cryptocurrency transactions. According to the provisions of the Article cryptocurrency transactions can be carried out exclusively through cryptocurrencies and cryptocurrency exchange offices.[712] The Draft Law also establishes responsibility for breaching provisions by the revocation of the license to conduct activities in the cryptocurrency market.[713]

Cybersecurity is also a part of the Internet of things as it governs the protection issue. On cybersecurity, Ukraine has a Law on the basic principles of cybersecurity in Ukraine. The main principles of cybersecurity listed in Article 7 include ensuring the national interests of Ukraine; accessibility, stability and security of cyberspace, public-private cooperation, broad cooperation with civil society in the field of cybersecurity by exchanging information on cybersecurity incidents, proportionality and adequacy of cyber defence measures to real and potential risks, realization of the inalienable right of the state to self-defence in accordance with the norms of international law in case of aggressive actions in cyberspace; the inevitability of punishment for committing cybercrimes; international cooperation in order to strengthen mutual trust in the field of cybersecurity and develop joint approaches to counter cyber threats, consolidate efforts in the investigation and prevention of cybercrime, prevent the use of cyberspace for terrorist, military and other illegal purposes; ensuring democratic civilian control over military formations and law enforcement agencies formed in accordance with the laws of Ukraine, carrying out activities in the field of cybersecurity.[714]

7.4. To what extent are the external legislative developments influential on national regulation of this area

The most influential external legislative developments would be the initiatives from the EU, as Ukraine is obligated under the EU-UA Association Agreement to harmonize its legislation with the legislation of the EU.

On the AI, the EU does not have any specific regulations, but intends to further developments in 2021. In 2020, the EU adopted a White Paper on Artificial Intelligence - A European approach to excellence and trust which contains legislative proposals. The

[710] The Decree of the Cabinet of Ministers of Ukraine 'On approving the strategy for the development of the information society in Ukraine' 2013 № 386-2013-p <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text> accessed 1 June 2021.
[711] Draft Law 'On the cryptocurrency in Ukraine' 2017 № 7183 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684> accessed 1 June 2021, art. 13.
[712] ibid, art. 16.
[713] ibid, art. 21.
[714] The Law of Ukraine 'On the basic principles of cybersecurity in Ukraine' 2017 №2163-VIII <https://zakon.rada.gov.ua/laws/show/2163-19#Text> accessed 1 June 2021, Art. 7.

White Paper is very similar to the Ukrainian Concept of Development. The difference is that the EU-initiative includes more focus on the international cooperation.[715] On the Internet of Things, the EU adopted the Cybersecurity Act, which maintains rules on individual schemes of certification on certain IP-products.[716] The Ukrainian Law on the basic principles of cybersecurity by comparison to the EU legislative framework is more declaratory and does not include a section on the certification of the IP-products. Ukrainian legislation. One of the best examples to show the influence of the EU legislation on the Ukrainian is the regulation of electronic signatures. The EU has adopted in 2014 a new Directive on the electronic identification, authentication and trust services. The main amendment was that personal keys of qualified electronic signatures should be stored only tokens on and should receive the certification from the government-approved certification authorities. The Law on Electronic Trust Services was adopted to harmonize the Ukrainian legislation with this Directive.

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

8.1. Circumstances under which such decryption can be carried out

Generally, as we previously mentioned, unlawful decryption is not allowed. What is more, unlawful decryption is punishable. According to the Constitution of Ukraine, the right to private life of every citizen is one that is protected by the state. (see Q 4.1)
The only possible way to legally decrypt personal messages is criminal proceedings. Not all criminal proceedings, but only covert.

Criminal procedure law envisages covert investigation as a part to evidence gathering actions of pre-trial investigation.

In criminal procedure, covert criminal investigations are understood as measures are carried out covertly, that is without the knowledge of an owner, possessor or keeper of personal data or message.[717]

Criminal procedure law provides for the right of a prosecutor or investigator to authorise decryption of otherwise encrypted person's personal messages received through transport

[715] White Paper on Artificial Intelligence - A European approach to excellence and trust (2020), COM(2020) 65 final, <https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 1 June 2021, p. 8.
[716] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 <http://data.europa.eu/eli/reg/2019/881/oj> accessed 1 June 2021.
[717] Since criminal procedure law does not operate the same notions as personal data protection law, for the purposes of this part of the Ukrainian Report the terms of the latter were used to maintain unification of the legal framework.

telecommunications networks or through electronic information systems, the Internet within measures of covert criminal investigation.[718]

Such authorization for the decryption within covert investigations of private messages from transport telecommunication networks, from electronic information systems can be implemented under the ruling of an investigating judge at the request of the prosecutor, or investigator agreed with the prosecutor.[719]

Criminal procedure law does not set out specific grounds on which the prosecutor or investigator may request the investigating judge for a ruling to allow decryption of personal data as a separate covert investigative measure.

Researches state that the data can be recorded if necessarily needed to gather evidence to transfer criminal proceeding for a serious or particularly serious crime[720] to the court.[721]

In practice, these measures are used to prevent the commission of a serious or especially serious crime, the cessation of terrorist acts and encroachments into internal affairs of State by the secret services of foreign states and organizations.[722]

Transport telecommunication networks are networks which provide transmitting of any signs, signals, written texts, images and sounds or messages between telecommunication access networks connected.[723] For example, decryption of a mobile operator's network.

Collecting information from electronic information systems means accessing the electronic information system or its parts to search, identify and record the information contained in them. [724]

Decryption of information is done through the use of software and special equipment that provides copying of information from means of communication that is relevant to criminal proceedings.[725]

---

[718] The Criminal Procedure Code of Ukraine 2012 №4651-VI <https://zakon.rada.gov.ua/laws/show/4651-17> accessed 26 February 2021, part 4 art. 258.
[719] ibid, part 2 art. 246.
[720] Criminal law of Ukraine provides for the division into minor, serious and especially serious crimes. 'A serious crime is punishable by a fine of no more than twenty-five thousand non-taxable minimum incomes or imprisonment for a term not exceeding ten years. Particularly serious is a crime punishable by a fine of more than 25,000 tax-free minimum incomes, imprisonment for more than ten years, or life imprisonment.'.
[721] D Sergeeva 'Withdrawal of information from transport telecommunications networks: problematic issues of legal regulation' ('Kh .: Arsis LTD', 2009) p. 286.
[722] The law of Ukraine 'On operational and investigative activities' 1992 № 2135-XII <https://zakon.rada.gov.ua/laws/show/2135-12#Text> accessed 26 February 2021, art. 8.
[723] ibid, part 1 art. 263.
[724] E. Iskenderov 'Withdrawal of operational units of information from transport telecommunications networks: problematic issues' ('Actual problems of law enforcement', 2016) p. 137 <http://vkslaw.knu.ua/images/verstka/4_2016_Iskenderov.pdf> accessed 26 February 2021.
[725] N. Goldberg 'Withdrawal of information from transport telecommunications networks: problems of criminal procedure regulation' ('Bulletin of the AMSU. Series: 'Law'', 2015) p. 151.

For the purposes of this section 8, we will further refer to TTN and EIS collectively as transport telecommunication networks and electronic information systems.

Decryption of the information provides control over telephone conversations, SMS-messages, collecting information from communication channels. [726]

8.2. Does this requirement (in general or in practice) give the authority too much power?

Criminal procedural law limits the scope of powers of law enforcement officials related to decrypting information and establishes guarantees to prevent unjustified restriction of personal rights and freedoms. In particular, the information about the crime and the perpetrator can be decrypted if impossible to obtain otherwise. [727]

As we described above, decryption can be carried out under extra circumstances: only within the limit of covert investigation, only if grounds are met, only the decision of a judge. Only the investigating judge has the right to decide on the decryption of personal information. [728] The investigator must inform the prosecutor about the decision to carry out actions that interfere in private communication, and their results.[729] The received information must be recorded in the protocol, and persons who have the right to get acquainted with it are warned about criminal liability for disclosure of the received information.[730] Furthermore, it is not possible to make extracts or copies from the protocols of the received information.[731] It is clearly defined that law enforcement and security agencies may decipher personal messages by a decision of the investigating court.[732]

8.3. What level of protection does your country's law provide for individuals in the above circumstances?

Furthermore, decrypted data is protected. Criminal procedure law provides for the disclosure of pre-trial investigation information only with the permission of the prosecutor or investigator.

Criminal liability is provided for illegal disclosure of such information.[733]

---

[726] Order of the Prosecutor General's Office of Ukraine, Ministry of Internal Affairs of Ukraine, Security Service of Ukraine, Administration of the state border service of Ukraine, Ministry of Finance of Ukraine, Ministry of Justice of Ukraine 'Instruction on Covert Investigative (Search) Actions' 2012 № 114/1042/516/1199/936/1687/5 <https://zakon.rada.gov.ua/laws/show/v0114900-12> accessed 26 February 2021, § 1 subsection 1.11.5.
[727] The Criminal Procedure Code of Ukraine 2012 №4651-VI <https://zakon.rada.gov.ua/laws/show/4651-17> accessed 26 February 2021, part 2 art. 246.
[728] ibid, part 3 art. 246.
[729] ibid, part 3 art. 246.
[730] ibid, part 2 art. 254.
[731] ibid, part 3 art. 255.
[732] ibid, part 2 art. 41.
[733] ibid, art. 222 (2).

The content of information transmitted to persons through the transport telecommunications networks from which the information is collected shall be preserved.[734]

Information concerning the personal life of the person in respect of whom such actions are carried out is not subject to disclosure. [735] That is, the person who was tapped has the right to receive a protocol of personal information, except for information that is classified. The obligation to inform the person, in respect of whom decrypted measures were taken, but always after their completion, is enshrined in criminal procedure law.[736] In practice, this makes it possible to claim damages for wrongful measures, as well as to declare the evidence inadmissible.[737]

From the date of termination of such actions Persons whose data was decrypted shall be notified of the fact of interference.

The person shall be notified within twelve months, but before being charged with an alleged crime in the court of law by the state prosecution.[738]

In material of a covert investigation record information about both: the person being listened to and the private lives of other people with whom communication has taken place.[739] If such information does not pertain to a crime, it is destroyed. Researchers note that the legislation of our country provides an average level of protection for persons whose personal information is decrypted.[740]

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

According to statistics compiled by the State Statistics Service of Ukraine in 2020, Ukrainian companies exported IT services abroad, totalling $ 2.11 billion.[741] In 2020,

---

[734] ibid, art. 263.
[735] D Sergeeva 'Withdrawal of information from transport telecommunications networks: problematic issues of legal regulation' ('Arsis LTD', 2009) p. 287.
[736] Order of the Prosecutor General's Office of Ukraine, Ministry of Internal Affairs of Ukraine, Security Service of Ukraine, Administration of the state border service of Ukraine, Ministry of Finance of Ukraine, Ministry of Justice of Ukraine 'Instruction on Covert Investigative (Search) Actions' dated 16.11.2012 № 114/1042/516/1199/936/1687/5 <https://zakon.rada.gov.ua/laws/show/v0114900-12> accessed 26 February 2021, § 1 subsection 1.11.5.
[737] Overview of the case law of the Supreme Court of Ukraine on the inadmissibility of evidence obtained as a result of a significant violation of human rights and freedoms <https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Ogljad_KKS_VS.pdf> accessed 26 February 2021.
[738] The Criminal Procedure Code of Ukraine 2012 №4651-VI <https://zakon.rada.gov.ua/laws/show/4651-17> accessed 26 February 2021, part 1 art. 253.
[739] ibid, art. 254
[740] Z. Udovenko 'Problems of security and protection of private households before the hour of knowledge of information from transport telecommunications' ('Scientific notes of NaUKMA. Legal sciences', 2019.) p. 123.
[741] The State Statistics Service of Ukraine, 'Express Issue' (The State Statistics Service of Ukraine, 13 November 2020) <https://ukrstat.org/uk/express/expr2020/11/136.doc> accessed 3 May 2021.

exports of IT services from Ukraine accounted for 25.9% of all Ukrainian services.[742] 75.1% of IT services exports were computer services (by $ 1.58 billion), 21.8% were information services exports ($ 459.4 million).[743] The rest was the export of telecommunications services, which brought $ 65.3 million in revenue to the country's economy.[744] Another feature of Vodafone's NB-IoT network is power-saving modes in Power Saving Mode, DRX, eDRX.[745] So, the service IT industry seems to be rather significant in Ukraine.

Digital advancements are fairly represented in Ukraine. Such advancements are represented by a number of technological projects in the AI, Big Data, Internet of Things and encryption areas. As such, AI among one of the most prominent companies established in Ukraine, there are: Grammarly, Aitheon, GitLab, Preply, RefaceAI, People AI.[746] Furthermore, in the IoT area, Vodaphone, one of the Ukrainian mobile operators, launched commercial operation of the NB-IoT network.[747] Devices connected to the NB-IoT network can communicate with each other at a dedicated frequency of 1800 MHz.[748] Another feature of Vodafone's NB-IoT network is the support of power saving modes in Power Saving Mode, DRX, eDRX.[749] Also, Vodafone provides a wide range of corporate clients with such products based on Big Data technologies as targeting promotion, clients' analysis, look-a-like model, accurate geoanalytics.[750] Another big Ukrainian mobile operator, Kyivstar, also offers to use Big Data tools for similar purposes.[751]

Although digital advancements are represented in Ukraine, most of them are represented by start-ups established in Ukraine. Among the areas that are actively developing and implementing technologies, there are bank servicing, mobile operators, logistics companies, marketplaces, ticket services, online cinemas.

Such a huge number of Ukrainian companies engaged in technological advancements presupposed that there might be a significant disbalance in protecting human rights online. As such, our analysis suggests that the balance between the development of digital

[742] ibid.
[743] ibid.
[744] ibid.
[745] ibid.
[746] 7 most prominent tech companies born in Ukraine (Silicon Canals, 18 June 2020) <https://siliconcanals.com/news/most-prominent-tech-companies-born-in-ukraine/> accessed 17 February 2020.
[747] The Ukrainian mobile operator has launched the Internet of Things into commercial operation (Economic truth, 21 January 2020) <https://www.epravda.com.ua/news/2020/01/21/656038/> accessed 17 February 2020.
[748] ibid.
[749] ibid.
[750] Big Data for business from Vodafone <https://business.vodafone.ua/produkty/big-data?utm_source=Search&utm_medium=CPC&utm_campaign=Vodafone_Analytics_Search_BRD&utm_term=vodafone%20big%20data&gclid=CjwKCAjwhMmEBhBwEiwAXwFoEb9D7XwnVipjdyCOGimKeImFcmCj4a6Y8SpRkz-xab0AHuhjf1cjwhoCnUAQAvD_BwE> accessed 3 May 2021.
[751] Big Data Decisions <https://bit.ly/2ZClVCD> accessed 17 February 2020.

advancements and the protection of citizens' rights online was not achieved to a bigger extent in Ukraine today.

To begin with, almost all Ukrainian companies that provide access to their services online use a public agreement (offer) which suggests that its provisions are not mutually agreed by both the individual and the company.[752]
The company, in this case, has more advantages as the potential user cannot change or even suggest changing the terms of services. Thus, a client wishing to use the company's services has only one option: either to refuse to use the service entirely or accept all the conditions listed in the user agreement, whatever these conditions may be. Thus, it is difficult to say that the user provides voluntary consent as it is non-alternative consent. Moreover, it should be noted that often in the relationship of consent to the processing of personal data, unequal economic entities are taking part (for example, an individual citizen on the one hand, and a mobile operator, who provides services to millions of customers- on the other). There are no provisions in the legislation that establish conditions and safeguards for abuse by the more economically strong party (e.g., unfair contract terms), similarly to agreements with natural monopolies, etc.

The only workaround is possible is a user can prove that, by agreeing to the terms of the accession agreement, they forfeit their rights that they would normally have otherwise[753]. In this case, a user shall prove (possibly in court) that their rights were actively violated.

In the light of the above, it is reasonable to consider the issue with the debt collection business in Ukraine. The condition that companies can transfer personal data of debtors to third parties is included in the Kyivstar Code.[754] A similar provision, is in the Vodafone Terms of Use[755]. The existence of this problem is noted by the Ukrainian Parliament Commissioner for Human Rights. According to the Report, in 2019, the Ombudsman's Office received more than 500 complaints from citizens.[756] In 2020, from 2031 complaints, almost 1,500 concerned the violation of the human right to non-interference in private and family life in the course of debt collection activities on the monetary obligations of individuals (collection activities).[757]

---

[752] The Civil Code of Ukraine 2003 № 435-IX <https://zakon.rada.gov.ua/laws/show/435-15#Text> accessed 1 June 2021, art. 634.
[753] ibid.
[754] The Code of Good Practice for Personal Data Processing of 'Kyivstar' <https://bit.ly/3kinkrG> accessed 17 February 2020, § 3.4.4.
[755] Vodafone Terms of use <https://www.vodafone.ua/terms-of-use> accessed 19 February 2020, § 5.11.
[756] The National Bank and the Commissioner for Human Rights of the Verkhovna Rada of Ukraine will work together to protect the personal data of Ukrainians <https://bank.gov.ua/ua/news/all/natsionalniy-bank-ta-upovnovajeniy-verhovnoyi-radi-ukrayini-z-prav-lyudini-spilno-pratsyuvatimut-nad-zahistom-personalnih-danih-ukrayintsiv> accessed 19 February 2020.
[757] Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2020 (Secretariat of the Commissioner, 2021) <https://www.ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf> accessed 1 June 2021, p. 21.

Current laws prescribe no considerations regarding such data transfers. Thus, even though this may lead to certain drastic consequences, the company still legally obtains personal data but uses this data to bother and spam people.

Moreover, the User Agreement of the online cinema services, Megogo, which consists 40 million users per month,[758] contains a provision under which a user consents to cross-border data transfer, covering countries that may not provide an adequate level of personal data protection.[759] However, paragraph 1 part 3 of article 29 of the Law of Ukraine 'On the protection of personal data' set out that access to personal data shall not be granted to a third party if the said person refuses to undertake obligations to ensure compliance with the requirements of this Law or is unable to provide them. The transfer of personal data by the controller to third parties - foreign subjects of relations related to personal data, is carried out on the general basis of personal data processing defined by the Law 'On the protection of personal data' and relevant international acts. Personal data may be transferred to processors situated in foreign countries if a subject grants their unambiguous consent to such transfer.[760] However, to transfer data legally, the controller should provide a person with information concerning grounds and conditions of cross-border data transfer, requirements to the recipient of information he should comply with, his obligation to store it.

Thus, the Megogo User Agreement does not provide information about who the recipient of the information is, so the data can be transferred to wherever. There is no possibility to understand if a processor provides an adequate level of personal data protection. Even though none of this is complied with, consent is still given which places the data subject in a very disproportionate position as they do not know where their data is transferred to and how it is further processed.

To conclude, the abovementioned give reason to consider the rights of users of the service to be violated. Especially given the fact that the customer does not have the technical ability to refuse the cross-border transfer of his personal data at the time of the conclusion of the user agreement.

At the same time, Ukrainian courts' practice does not go through the application of financial sanctions for such violations. However, it is possible to apply to the Ukrainian Parliament Commissioner for Human Rights, who can conduct an inspection and, as mentioned in one of the earlier questions, draw up an order. If the subject of inspection does not comply with the order within the period specified, the Commissioner can draw up protocols on bringing the subject to administrative responsibility and send them to court.[761]

---

[758] Nina Glushchenko, 'Who pays for legal video and how: statistics from Megogo' (Ain, 24 November 2016) <https://ain.ua/2016/11/24/kto-i-kak-platit-za-legalnoe-video-megogo-oct-2016/> accessed 4 March 2021.
[759] Megogo User Agreement <https://megogo.net/ru/rules> accessed 19 February 2020.
[760] The Law of Ukraine 'On Personal Data Protection' (n 554), art 29, § 4 (1).
[761] ibid, art 23, § 1 (10).

In Ukraine, administrative responsibility is provided for failure to comply with the procedure for protecting personal data established by the legislation on personal data protection, which led to illegal access to them or violation of the rights of the personal data subject.[762] The fine for officials, legal entities vary from EUR 50 to EUR 1,000 for repeated violation.[763]

It is worth mentioning that there is no responsibility for the misuse of personal data. Illegal processing of personal data, namely mobile phone numbers of individuals who have no relationship to the monetary obligation (family members, neighbours, friends and employees), is a common phenomenon during the implementation of collection activities.[764] It is a common practice when a financial company makes calls and sends SMS messages to people regarding the repayment of the debt on another person's credit obligations. [765] Thus, only after such a person applied to the Commissioner and the latter took actions, the contact number of the person's mobile phone can be removed from the database of the financial company.[766]

It is worth mentioning that there is no direct criminal responsibility for intentional illegal collection and usage of personal data. Article 182 of the Criminal Code only covers criminal responsibility for illegal collection, storage, use, destruction, dissemination of confidential information or illegal alteration of such information.[767] However, this article is applicable only if personal data can be determined as confidential information. Because of this and the low administrative sanctions, one of the most widespread issues in protecting personal data in Ukraine is an issue with personal data trade. Judging by the number of incidents, databases' trade with Ukrainians' personal information is on stream. In 2017, a tax officer from Sumy traded the database of tax service.[768] In 2017, the personal data of Privatbank's customers were copied to Russian servers.[769] In 2018, the database of 18,000 Nova Poshta users was selling on the darknet.[770] In 2018, sellers of data from the customs

---

[762] Code of Ukraine on Administrative Offenses 1984 № 8073-X, <https://zakon.rada.gov.ua/laws/show/80732-10#Text> accessed 1 June 2021, art 188-39, § 4.
[763] ibid, § 4.
[764] Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2020 (Secretariat of the Commissioner, 2021) <https://www.ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf> accessed 1 June 2021, p. 22.
[765] ibid.
[766] ibid.
[767] The Criminal Code of Ukraine 1984 №2341-III <https://zakon.rada.gov.ua/laws/show/2341-14#Text> accessed 01 June 2021, art 182.
[768] Dmytro Weber, 'In the center of Sumy, a tax officer was caught selling personal data' (Segodnya, 31 September 2017) <https://criminal.segodnya.ua/criminal/v-centre-sum-poymali-nalogovika-torgovavshego-personalnymi-dannymi--1051731.html> accessed 20 February 2020.
[769] How did the data of private clients of PrivatBank end up in Moscow? (Zakon i Business, 7 December 2017) <https://zib.com.ua/ru/print/131103-kak_dannie_chastnih_klientov_privatbanka_okazalis_v_moskve.htm> accessed 20 February 2020.
[770] In 'dark Internet' the customer base of 'Nova poshta' sells (Economic truth, 6 February 2018) <https://www.epravda.com.ua/rus/news/2018/02/6/633794/> accessed 20 February 2020.

database were caught in Zaporizhia.[771] In 2019, a Kharkiv resident was convicted of trafficking in data of tax services.[772] In 2020, in Dnipro cyber specialists of the Security Service of Ukraine blocked the sale of personal data of citizens at the hacker forum, which in many respects coincides with the information stored in the State Register of Voters.[773]

Also, as the Commissioner highlighted in the Report, numbers of complainants concern the illegal dissemination of personal data via the Internet, illegal dissemination of personal data in messengers and social networks, violation of the right to protect personal data during the implementation of electronic services.[774] Among the complaints as for illegal spreading of personal data on the Internet, the Commissioner mentioned in Reports those that concern publishing information that includes personal data by state agencies, companies, and state universities.

As for the illegal dissemination of personal data in messengers, paid illegal distribution of personal data through bots in the Telegram messenger has become an extensive problem in recent years in Ukraine. In May 2020, several bots appeared on Telegram that offered to find a person by name, phone number, taxpayer registration card number, car number, e-mail address and even provide passwords from the e-mail itself.[775] So, all these occasions are evidence of the insufficient level of personal data protection. In Ukraine, there is no legislation on the protection of personal data in case of its leakage. The only mechanism to protect one's data as a result of breaches is to appeal to the Ukrainian Parliament Commissioner for Human Rights. Court protection might not be as widespread.

Digital advancements are developing in the modern world, but Ukrainian legislation on data protection does not correspond to the contemporary state of digital advancements and is not stable, so the stable law enforcement practice can provide the balance; however, in Ukraine, there is no proper judicial protection. The Commissioner notes that in 2016, 45 protocols were sent to the court, which concerned violations of legislation in the field of personal data protection, 40 protocols were considered by the court, while the number of cases in which a person was found guilty and imposed an administrative penalty is 15, the remaining cases were closed due to the expiration at the time of the term of the imposition

---

[771] 'Cyberpolice exposes office for sale of personal databases' (Cyberpolice National Police of Ukraine, 5 April 2018) <https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-ofis-z-prodazhu-baz-personalnyx-danyx-1858/> accessed 20 February 2020.

[772] Kharkiv citizen who illegally sold customs databases sentenced to fine and special confiscation (Interfaks-Ukraine, 21 March 2019) <https://interfax.com.ua/news/general/574332.html> accessed 20 February 2020.

[773] The sale of the voter personal database was blocked in Dnipro - SSU (Media Sapiens, 24 October 2020) <https://ms.detector.media/kiberbezpeka/post/25811/2020-10-24-u-dnipri-blokuvaly-prodazh-bazy-personalnykh-danykh-vybortsiv-sbu/> accessed 20 February 2020.

[774] Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2020 (Secretariat of the Commissioner, 2021) <https://www.ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf> accessed 1 June 2021, p. 22.

[775] Vsevolod Nekrasov, 'State registers have leaked: who is 'merging' the personal data of Ukrainians and what to do about it' (Economic truth, 13 May 2020) <https://www.epravda.com.ua/publications/2020/05/13/660405/> accessed 20 February 2020.

of the administrative penalty.[776] During 2017, the Office for Personal Data Protection drew up and sent to court 34 protocols.[777] In only 2 cases, the persons were found guilty and imposed an administrative penalty; in 13 cases, the person was found guilty, but the proceedings were closed due to the term's expiration for the imposition of an administrative penalty.[778] In 2019, 10 protocols on administrative offences concerning violations of the legislation requirements in the field of personal data protection were submitted to the court.[779]

The court cases analysis makes it possible to establish that in the period from 2012 to the present, only 143 decisions regarding administrative violations of legislation in the field of personal data protection can be found in the system[780]. At the same time, the number of considered cases by year is distributed as follows: in 2012, the court considered 4 cases that concerned protection of the personal data; in 2013 – 7 cases; in 2014 – 3 cases; in 2015 – 10 cases; in 2016 – 48 cases; in 2017 – 49 cases; in 2018 – 21 cases; in 2019 – 1 case, in 2020 – 0 cases. These figures indicate that preventing violations of personal data protection in Ukraine has a downward trend.

As we can see, in Ukraine, there is an issue with basic legislation and judicial protection. It is problematic to reach the balance between allowing digital advancements and protecting human rights online because of the formal approach of companies to privacy policies, low sanctions established by the legislation for violation of the legislation on personal data, regular illegal disclosure of personal data by companies and government officials and the negligible number of court decisions due to violation of legislation on the protection of personal data.

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?

Prospects for the development of human rights on the Internet in Ukraine have many issues that have not yet been resolved. This can be argued for the following reasons:

- outdated legislation;
- unresolved issues of existing legislation and how to ensure protect human rights online.

[776] Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2016 (Secretariat of the Commissioner, 2017) <https://ombudsman.gov.ua/files/Dopovidi/Dopovid_2016_final.pdf>accessed 1 June 2021, p. 91.
[777] Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2017 (Secretariat of the Commissioner, 2018) <http://www.ombudsman.gov.ua/files/Dopovidi/Report-2018-1.pdf> accessed 1 June 2021, p. 485.
[778] ibid.
[779] Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in 2019 (Secretariat of the Commissioner, 2020) <http://www.ombudsman.gov.ua/files/Dopovidi/zvit%20za%202019.pdf> accessed 1 June 2021, p. 191.
[780] The search was carried out according to the following parameters: cases about administrative offenses, violations of legislation in the field of personal data protection

First, law, technology and social interactions are constantly evolving to ensure the legal design and regulation of the ongoing design in legislation. The Ukrainian legislation in this sphere and the ratified international treaties are not superfluous or outdated, but the development of technology and social ties has taken a step forward, so this is not enough. Already in 2021, there are many new international acts that need to be ratified, for example The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), or at least tried to take a vector to modernize national legislation similar to the example of Western countries, but Ukraine has not yet taken such action, even with a number of problems in protecting personal databases.

Secondly, according to the Law of Ukraine 'On Amendments to Certain Legislative Acts of Ukraine on Improving the System of Personal Data Protection', which entered into force on January 1, 2014 to ensure the independence of the authorized body for personal data protection, as required by the Council of Europe Convention persons in connection with the automated processing of personal data, the authority to monitor compliance with the legislation on personal data protection is vested in the Commissioner of the Verkhovna Rada of Ukraine for Human Rights. From 2014 to 2019, annual reports were issued on the status of legislation, its compliance and ensuring the implementation of personal data protection. The reports also added information on problems of legislation, conflicts, lack of institutions for the implementation of rights and their protection, and recommendations on how to improve legislation and the process of protecting and enforcing rights. But every year the problem areas in the reports are repeated, the recommendations only increase, but there are no changes. The Commissioner for Human Rights of the Verkhovna Rada of Ukraine, in particular, often notes the following problems in the private information sector:[781]

- in the field of personal data protection related to medical secrecy, as well as in the problems of registration and accounting of such information;
- in the storage of personal data related to law enforcement and official activities;
- in the field of personal data protection concerning local governments and other owners of personal data that ensure the processing of personal data stored in personal files;
- ensuring the possibility of exercising the right of personal data subjects to access information about themselves, in general, the incomprehensibility and non-transparency of the state's actions regarding personal data;
- the lack of an effective mechanism for the implementation of sanctions for human rights violations in this area and control over the actions of entities that use and have access to personal data.

[781] Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in 2019 (Secretariat of the Commissioner, 2020) <http://www.ombudsman.gov.ua/files/Dopovidi/zvit%20za%202019.pdf> accessed 01 June 2021.

These issues, as already mentioned, have not been resolved since 2014, and with the development of technology, especially in a pandemic, the virtualization of society and human rights will deepen and multiply. Therefore, we can say that the prospects for the development of protection of personal databases in Ukraine are not positive.

Although there are some trends that may suggest otherwise. In order to improve the situation with the implementation of protection and realization of human rights in this area, it is necessary for the executive and legislative bodies to listen to the recommendations of the Commissioner. Her reports contain many relevant comments, examples and ideas that would improve the process of human rights protection.

Thirdly, the legislation needs: the Ukrainian legislative process is currently being revived, a large number of new bills are being introduced, no less laws are being passed, and several new codes of Ukraine from various fields of law are being drafted. In the wake of this update, it is possible to improve legal acts related to personal databases, to draw attention to the experience of foreign partners, to ratify some international acts. For example: the General Data Protection Regulation of 25 May 2016, 'Recommendation CM / Rec (2020) 1 of the Committee of Ministers to member states on the impact of algorithmic systems on human rights' was adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of deputies ministers,

Third, you need to turn to the doctrine and try to add certain methods and ways to improve this legal issue from it. In fact, in practice and in the scientific community, the field of personal data has come a long way. For example, scientific and practical manual 'Personal data protection:' Legal regulation and practical aspects 'by Bem MV, Gorodisky IM, Satton G., Rodionenko OM,' Legal analysis of the main models of institutionalization of the state supervision with regard to personal data and access to public information in by Volodymyr Venher and Oleh Zaiarnyi. If the legislator pays attention to the trends that exist in practice and pays attention to the already developed doctrine, it will be possible to supplement the existing legislation, closing a large number of its gaps.

The recent scandals of private companies also testify to the forced changes in the protection of human rights online. There is a lack of accountability and control over situations where people's rights are violated online due to work and lack of preparedness for attacks by private companies. Although the legislator does not comment on his actions in this area, it is difficult to calculate his actions, but the scandal with one of the largest Ukrainian IT outsourcers - SoftServe and other large companies should have been the reason for the legislator's actions, so I believe that certain actions will be taken in the future. direction.[782]

[782] 'Maya Yarovaya, 'New "spill" of SoftServe data: client projects and, probably, employee data' (Ain, 16 September 2020) <https://ain.ua/2020/09/16/softserve-utechka-2/> accessed 1 June 2021.

Therefore, as a result, it is necessary to state a positive future for changes in this area, the legislator ignores the renewal of the sphere and the problems that have existed in it since 2014, ignores the recommendations of the doctrine and the Verkhovna Rada Commissioner for Human Rights, international experience and trends. Although there are hopes that changes will be made in the wake of a general overhaul of the legislation, as there are already international legal acts that need to be adopted, there is a ready practice and scientific basis. Therefore, everything depends only on the desire of the legislator, because all other aspects of updating the protection of personal databases are ready. But it is possible that the current problems and the number of cases of human rights violations on the Internet will increase under the conditions of quarantine and development of technologies and access to them, so the legislator will no longer have time to think about the critical situation in this area. In such a situation, regulations and executive institutions will be rapidly updated, but the quality of such an update and its effectiveness will soon be forgotten, so even such actions will not solve human rights violations in the future. So look forward to the option when the legislator Ukraine gradually reasonable, citing international legal and practical experience in the wake of legislation update and improve legislation in the field of human rights on the Internet, and at least this many reasons small acts creator desires. If we take into account the immersion of Ukrainian law in international experience and a large number of young figures in the field outside the state apparatus, we can say about the prospects for scientific development in the field of personal data protection. Then, under such conditions, which are real in modern times, as indicated during the study earlier, science and international experience will create an opportunity for the legislator to draw new proven international experience and domestic scientific theory solutions to existing problems. Under conditions that are quite realistic for our time, prospects for the protection of personal data and human rights in Ukraine look much more successful. Therefore, reviewing the research and analysis of the topic and presentation of different ways of development of Ukrainian law, we can predict that the result is a high probability of innovations, but how they will be introduced and implemented only time will tell, but as stated earlier, Ukraine draws on international experience and draws on national doctrine, which improves the enforcement mechanism, which should result in positive trends in the protection of personal data and human rights on the Internet in the face of such active protection.

Conclusion

The right to protection of personal data in Ukraine is a wide area. There is a widespread practice of exercising these rights in various segments of society: from personal rights to the protection of medical secrecy to the protection of the confidentiality of database data in large companies. There is a development and a multifaceted scientific doctrine that considers the approaches, purpose, principles, goals and general fundamental aspect of the protection and implementation of this right. The doctrine of content includes new-fangled revisions, the experience of foreign scholars and years of national work. When it comes to

legislation, there is a constitutionally recognized recognition of such a right, its implementation and protection. Some international legal acts have been ratified, which further protect and improve legislation in this area. There are a number of relevant laws, which were mentioned earlier, the indication of norms in the Civil, Administrative, Criminal Codes of Ukraine, which protect and offer the right to protection of personal data, in addition, there are sanctions for their violation. Judicial practice has a number of examples of the application of legislation that set precedents that improve the justice process and the protection of personal data protection rights. In addition, there is a special state body that expands information and promotes protection in this area: the Verkhovna Rada of Ukraine Commissioner for Human Rights - an official who monitors compliance with the requirements of constitutional rights and freedoms of man and citizen in Ukraine. Having the apparatus and composition for efficient and complete performance of their duties. Therefore, under all these conditions, the rights of Ukrainian citizens must be protected and realized.

But this is not the case at all, because there are a number of problems that have not been solved and there has been no progress in this field for years. Note the following problems:
- Sanctions are disproportionate to the damage, the bark is borne by those whose rights have been violated. Criminals have no reason not to commit offenses. Insufficient fines and liability;
- There is not enough case law: few cases come to consideration, so it is impossible to form a fully effective system of justice on this issue;
- Legislation not updated: there are a number of international legal acts that Ukraine has not yet adopted and ratified - this makes its legislation obsolete in relation to foreign partners;
- Lack of national innovations: powerful innovations in the field of personal data protection have not occurred since 2014, as this area is developing rapidly due to the technical evolution of the world and the problems in this area are increasing. Therefore, the current legislation of Ukraine is no longer a problem;
- There is no interaction between the doctrine and the legislator: in Ukraine there is indeed a deep theoretical basis, it is diverse and well-developed, but the legislator does not pay any attention to it. The work of scientists is not used to update legislation, which creates unpromising conditions for the development of both legislation and science. After all, why develop science if it is not used and it is not listened to;
- Compliance with the law is inefficient and incomprehensible to the population. There are few factors that explain to the public how to protect their rights in the digital age, and when they do, they encounter law enforcement agencies that are not technically, theoretically and practically ready to perform their duties due to a lack of institutions, knowledge and tools. This means that it is very difficult to ensure the right and its implementation in Ukraine, which means its actual violation.

These problems are the result of years of inaction in the field of protection, development and ensuring the right to protection of personal data in Ukraine. Of course, the legislator is to blame for this, but we need to understand why this situation happened. The newest sphere is always a problem for the legislator, in addition, it is accompanied by technical progress and the international aspect. It is likely that the legislator simply does not know how best to resolve this issue, although at the same time these rights and their regulation exist in a purely practical application with frequent recourse to international experience and international courts. That is, it is possible to understand why such a legal situation occurred, but this does not mean that it should remain so.

Now the legislation of Ukraine in various spheres is being updated in the wake of such an update, perhaps the legislator will dare to touch on this topic. For example, to introduce new acts, regulate the field of artificial intelligence, cryptocurrency and its confidentiality, the circulation of personal data in the international digital space. Since Ukraine already has some practice and a broad scientific base, the foundation for such changes already exists, which will facilitate work in this field.

Therefore, the right to protection of personal data in Ukraine is protected and implemented: the institutions, acts, methods of implementation and restoration of the violated right are provided. But protection and implementation are incomplete, imperfect and in need of major upgrades. This is possible, because the prospects of such actions on the part of the legislator are seen, so over time changes and improvements are possible, although so far the area needs to be recognized as problematic, and the rights as not fully protected and difficult to implement.

Table of legislation

Provision in Ukrainian language	Corresponding translation in English
Стаття 2 Закону України «Про захист персональних даних»: персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;	**Article 2 of the Law of Ukraine 'On Personal Data Protection':** personal data - information or a set of information about an individual who is identified or can be specifically identified;
Стаття 11 Закону України «Про інформацію»: 1. Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. 2. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.	**Article 11 of the Law of Ukraine 'On Information':** 1. Information about a natural person (personal data) - information or a set of information about a natural person who is identified or can be specifically identified. 2. The collection, storage, use and dissemination of confidential information about a person without his or her consent is not permitted, except in cases specified by law and only in the interests of national security, economic well-being and protection of human rights. Confidential information about an individual includes, in particular, information about his or her nationality, education, marital status, religious beliefs, state of health, as well as address, date and place of birth.

Стаття 7 Закону України «Про доступ до публічної інформації»: 1. Конфіденційна інформація - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Не може бути віднесена до конфіденційної інформація, зазначена в частині першій і другій статті 13 цього Закону.	**Article 7 of the Law of Ukraine 'On Access to Public Information':** 1. Confidential information - information to which access is restricted by a natural or legal person, except for subjects of power, and which may be disseminated in the manner prescribed by them at their request in accordance with the conditions provided by them. The information specified in parts one and two of Article 13 of this Law may not be classified as confidential.
Стаття 15 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Сторони домовились співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи. Співробітництво у сфері захисту персональних даних може включати, inter alia, обмін інформацією та експертами.	**Article 15 of the Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part:** The parties agreed to cooperate in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards, in particular the relevant documents of the Council of Europe. Cooperation in the field of personal data protection may include, inter alia, the exchange of information and experts.
Стаття 22 Закону України "Про захист персональних даних": 1. Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють такі органи: 1) Уповноважений; 2) суди.	**Article 22 of the Law of Ukraine 'On Personal Data Protection':** 1. The following bodies shall exercise control over the observance of the legislation on the protection of personal data within the powers provided by law: 1) the Ombudsman; 2) the courts.

Стаття 23 Закону України "Про захист персональних даних":	**Article 23 of the Law of Ukraine 'On Personal Data Protection':**
1. Уповноважений має такі повноваження у сфері захисту персональних даних: 1) отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду; 2) проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних; 3) отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом; 4) затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених цим Законом; 5) за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі,	1. The Ombudsman has the following powers in the field of personal data protection:1) receive proposals, complaints and other appeals from individuals and legal entities on the protection of personal data and make decisions based on the results of their consideration; 2) conduct scheduled or unscheduled, on-site or off-site inspections of the data controllers and processors in the manner prescribed by the Ombudsman, ensuring the access to premises where personal data is processed, as prescribed by law; 3) receive at the request and have access to any information (documents) from data controllers and processors that are necessary to control the protection of personal data, including access to personal data, relevant databases or files, information from restricted access; 4) approve regulations in the field of personal data protection in the cases provided by this Law; 5) based on the results of inspection, consideration of the application, to issue mandatory requirements (instructions) for the prevention or elimination of violations of personal data protection legislation, including changes, deletion or destruction of personal data, providing access to it, providing or prohibiting access to a third party, suspension or termination of personal data processing; 6) provide recommendations on the practical application of legislation on personal data protection, explain the rights and responsibilities of relevant persons at the request of personal data subjects, processors or controllers, departments responsible for the

зупинення або припинення обробки персональних даних; 6) надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб; 7) взаємодіяти із структурними підрозділами або відповідальними особами, які відповідно до цього Закону організовують роботу, пов'язану із захистом персональних даних при їх обробці; оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб; 8) звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних; 9) надавати за зверненням професійних, самоврядних та інших громадських об'єднань чи юридичних осіб висновки щодо проектів кодексів поведінки у сфері захисту персональних даних та змін до них; 10) складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом; 11) інформувати про законодавство з питань захисту персональних даних,	organisation of personal data protection, other persons; 7) interact with structural subdivisions or responsible persons who, in accordance with this Law, organise work related to the protection of personal data during its processing; publish information about such structural subdivisions and responsible persons; 8) address proposals to the Verkhovna Rada of Ukraine, the President of Ukraine, the Cabinet of Ministers of Ukraine, other state bodies, local governments, their officials on the adoption or amendment of regulations on personal data protection; 9) provide, upon the request of professional, self-governing and other public associations or legal entities, conclusions on draft codes of conduct in the field of personal data protection and changes to them; 10) draw up protocols on bringing to administrative responsibility and send them to court in cases provided by law; 11) inform about the legislation on personal data protection, problems of its practical application, rights and obligations of the subjects of relations related to personal data; 12) monitor new practices, trends and technologies of personal data protection; 13) organise and ensure interaction with foreign actors of relations related to personal data, including in connection with the implementation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol, other international agreements of Ukraine in the field of personal data protection; 14) participate in the work of international organisations on personal data protection.

проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними; 12) здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних; 13) організовувати та забезпечувати взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними, у тому числі у зв'язку з виконанням Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері захисту персональних даних; 14) брати участь у роботі міжнародних організацій з питань захисту персональних даних. 2. Уповноважений Верховної Ради України з прав людини включає до своєї щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні звіт про стан додержання законодавства у сфері захисту персональних даних.	2. The Ukrainian Parliament Commissioner for Human Rights shall include in his/her annual report on the state of observance and protection of human and civil rights and freedoms in Ukraine a report on the state of observance of legislation in the field of personal data protection.
Стаття 28 Закону України "Про захист персональних даних": Порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом.	**Article 28 of the Law of Ukraine 'On personal data protection':** Violation of the legislation on personal data protection entails liability established by law.

Пункт 1.2. Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: У цьому Порядку терміни вживаються у такому значенні: безвиїзна перевірка - планова або позапланова перевірка діяльності суб'єкта перевірки Уповноваженим та/або уповноваженими ним посадовими особами, яка проводиться в приміщенні Секретаріату Уповноваженого Верховної Ради України з прав людини на підставі отриманих від суб'єкта перевірки документів та пояснень без виїзду за місцезнаходженням суб'єкта перевірки та/або за місцем обробки персональних даних; виїзна перевірка - планова або позапланова перевірка діяльності суб'єкта перевірки Уповноваженим та/або уповноваженими ним посадовими особами, яка проводиться за місцезнаходженням суб'єкта перевірки та/або безпосередньо на місці обробки персональних даних; планова перевірка - перевірка діяльності суб'єкта перевірки, яка проводиться на підставі плану проведення перевірок на відповідний квартал та рік; позапланова перевірка - перевірка діяльності суб'єкта перевірки, яка не передбачена в плані проведення перевірок. акт перевірки - службовий документ, який засвідчує факт проведення перевірки діяльності суб'єкта перевірки та стан додержання ним вимог законодавства про захист персональних даних;	**Paragraph 1.2. of the Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection:** In this Procedure, the terms are used in the following meaning: on-site inspection - scheduled or unscheduled inspection of the subject of inspection by the Ombudsman and / or his authorised officials, which is carried out in the premises of the Secretariat of the Ombudsman on the basis of documents and explanations received from the subject of verification without leaving for the location of the subject of inspection and / or at the place of personal data processing; on-site inspection - scheduled or unscheduled inspection of the activity of the subject of inspection by the Ombudsman and / or authorised officials, which is carried out at the location of the subject of inspection and / or directly at the place of personal data processing; scheduled inspection - inspection of the activity of the subject of inspection, which is carried out on the basis of the plan of inspections for the relevant quarter and year; unscheduled inspection - inspection of the subject of inspection, which is not provided for in the plan of inspections. act of inspection - an official document certifying the fact of inspection of the subject of inspection and the state of compliance with the requirements of the legislation on personal data protection; order is a mandatory written request of the Ombudsman to eliminate violations of the requirements of the legislation on personal data protection, which is sent to the subject of verification.

припис (вимога) - це обов'язкова для виконання у визначені строки письмова вимога Уповноваженого щодо усунення порушень вимог законодавства про захист персональних даних, яка вручається (надсилається) суб'єкту перевірки. Інші терміни у цьому Порядку вживаються у значенні, наведеному в Законі України "Про захист персональних даних".	Other terms in this Procedure are used in the meaning given in the Law of Ukraine 'On Personal Data Protection'.
Пункт 5.1. Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: За результатами здійснення планової або позапланової перевірки Уповноважений та/або уповноважена посадова особи складає у двох примірниках акт перевірки додержання вимог законодавства про захист персональних даних (далі - Акт) за формою згідно з додатком 1 до цього Порядку.	**Paragraph 5.1. of the Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection:** Based on the results of scheduled or unscheduled inspection, the Ombudsman and / or authorised official shall draw up in two copies of an act of verification of compliance with the requirements of personal data protection legislation (hereinafter - the Act) in the form envisaged by Annex 1 to this Procedure.
Пункт 5.2. Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: **Акт повинен містити такі відомості:** дату, час та місце складання; посади, прізвища та ініціали осіб, що проводили перевірку; посаду, прізвище та ініціали керівника (уповноваженої ним особи) або прізвище та ініціали фізичної особи суб'єкта перевірки; вид перевірки (планова, позапланова, виїзна, безвиїзна);	**Paragraph 5.2. of the Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection:** The act must contain the following information: date, time and place of compilation; positions, names and initials of the persons who conducted the inspection; position, surname and initials of the head (the person authorised by him) or surname and initials of the natural person of the subject of inspection; type of inspection (scheduled, unscheduled, on-site, off-site);

для суб'єкта перевірки - органу державної влади та місцевого самоврядування: найменування, місцезнаходження; для суб'єкта перевірки - юридичної особи: найменування, місцезнаходження; для суб'єкта перевірки - фізичної особи та/або фізичної особи - підприємця: прізвище, ім'я та по батькові, місце проживання; дані про дату, час початку та час закінчення перевірки, її загальну тривалість; факти (обставини), які встановлено за результатами перевірки; висновок про результати перевірки. При складанні Акта мають бути додержані об'єктивність і вичерпність опису виявлених фактів і даних.	if the subject of inspection is a state body or a local self-government: name, location; if the subject of inspection is a legal entity: name, location; if the subject of inspection is a natural person and / or an entrepreneur: surname, name and patronymic, place of residence; data on the date, time of the beginning and time of the end of the inspection, its total duration; facts (circumstances) established by the results of the inspection; conclusion on the results of the inspection. When drawing up the Act, the objectivity and completeness of the description of the revealed facts and data must be observed.
Пункт 5.3. Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: Акт повинен містити один із таких висновків: про відсутність у діяльності суб'єкта перевірки порушень вимог законодавства про захист персональних даних; про виявлені у діяльності суб'єкта перевірки порушення вимог законодавства про захист персональних даних, їх детальний опис із посиланням на норми чинного законодавства, які порушено. Забороняється вносити до акта перевірки відомості про порушення, які не підтверджено документально.	**Paragraph 5.3. of the Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection:** The act must contain one of the following conclusions: about the absence in the activity of the subject of verification of violations of the requirements of the legislation on personal data protection; about the violations of the requirements of the legislation on personal data protection revealed in the activity of the subject of inspection, their detailed description with reference to the norms of the current legislation, which have been violated. It is prohibited to enter information about violations that have not been documented in the act.

Пункт 5.10. Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: На підставі Акта перевірки, під час якої виявлено порушення вимог законодавства про захист персональних даних, складається припис про усунення порушень вимог законодавства у сфері захисту персональних даних, виявлених під час перевірки, за формою згідно з додатком 2 до цього Порядку (далі - припис).	**Paragraph 5.10. of the Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection:** On the basis of the Act of verification of the inspection, during which a violation of the legislation on personal data protection was revealed, an order is drawn up to eliminate violations of the legislation in the field of personal data protection revealed during the inspection, in the form of Annex 2 to this Procedure (hereinafter - the order).
Пункт 5.11. Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: У приписі зазначаються: номер, дата та місце складання припису; для суб'єкта перевірки - органу державної влади та місцевого самоврядування: найменування, місцезнаходження; для суб'єкта перевірки - юридичної особи: найменування, місцезнаходження, прізвище, ім'я та по батькові керівника юридичної особи; для суб'єкта перевірки - фізичної особи та/або фізичної особи - підприємця: прізвище, ім'я та по батькові, місце її проживання; підстава для видачі припису; заходи необхідні для усунення порушень, виявлених під час перевірки; строк виконання припису; строк інформування суб'єктом перевірки Уповноваженого про усунення виявленого порушення;	**Paragraph 5.11. of the Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection:** The following data should be mentioned in the order: number, date and place of the order; if the subject of inspection is the state body or and local self-government: name, location; is the subject of inspection is a legal entity: name, location, surname, name and patronymic of the head of the legal entity; if the subject of inspection is a natural person and / or an entrepreneur: surname, name and patronymic, place of residence; grounds for issuing an order; measures necessary to eliminate the violations revealed during the inspection; term of execution of the order; term for the subject of inspection to inform the Ombudsman about elimination of the revealed violation; signature of the authorised official (officials) who conducted the inspection.

підпис уповноваженої посадової особи (осіб), яка проводила перевірку.	
Пункт 5.15. Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: У разі невиконання припису протягом вказаного у ньому строку Уповноважений або уповноважена посадова особа складає протокол про адміністративне правопорушення, передбачене статтею 188-40 Кодексу України про адміністративні правопорушення за формою та у порядку, передбаченому законодавством та Порядком оформлення матеріалів про адміністративні правопорушення.	**Paragraph 5.15. of the Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection:** In case of non-compliance with the order within the period specified, the Ombudsman or authorised official draws up a report on an administrative offence under Article 188-40 of the Code of Administrative Offences in the form and manner prescribed by law and the Procedure for registration of materials on administrative offences.
Пункт 5.16. Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: У разі виявлення під час перевірки передбаченого статтею 188-39 чи статтею 188-40 КУпАП адміністративного правопорушення, вчиненого суб'єктом перевірки, Уповноважений або уповноважена посадова особа відповідно до пункту 1 частини першої статті 255 КУпАП складає протокол про адміністративне правопорушення за формою та у порядку, передбаченому законодавством та Порядком оформлення матеріалів про адміністративні правопорушення.	**Paragraph 5.16. of the Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection:** In case of detection during the inspection of an administrative offence envisaged by Article 188-39 or Article 188-40 of the Code of Administrative offences committed by the subject of inspection, the Ombudsman or authorised official in accordance with paragraph 1 of part 1 of Article 255 of the Code of Administrative offences draws up a report on administrative offence in the form and manner prescribed by law and the Procedure for registration of materials on administrative offences.

Пункт 5.17. Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: У разі виявлення під час перевірки суб'єкта перевірки ознак кримінального правопорушення Уповноважений направляє необхідні матеріали до правоохоронних органів.	**Paragraph 5.17. of the Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection:** In case the signs of a criminal offence are detected during the inspection, the Ombudsman shall send the necessary materials to law enforcement agencies.
Стаття 188-39 Кодексу України про адміністративні правопорушення: Неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей - тягнуть за собою накладення штрафу на громадян від ста до двохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб'єктів підприємницької діяльності - від двохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян. Невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних - тягнуть за собою накладення штрафу на громадян від двохсот до трьохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян -	**Article 188-39 of the Code of Ukraine on Administrative offences:** Failure to notify or untimely notification of the Ombudsman on the processing of personal data or the change of information subject to notification in accordance with the law, notification of incomplete or inaccurate information - entail the imposition of a fine on natural persons from one hundred to two hundred non-taxable minimum incomes; on officials and entrepreneurs - from two hundred to four hundred non-taxable minimum incomes. Failure to comply with an order (instructions) of the Ombudsman or authorised officials to prevent or eliminate violations of personal data protection legislation - entail the imposition of a fine on natural persons from two hundred to three hundred non-taxable minimum incomes; on officials and entrepreneurs - from three hundred to one thousand non-taxable minimum incomes. Repeated violation during the year a from the list provided in parts 1 or 2 of this article, for which the person has already been subjected to an administrative penalty, -

суб'єктів підприємницької діяльності - від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян. Повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню, - тягне за собою накладення штрафу на громадян від трьохсот до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб'єктів підприємницької діяльності - від п'ятисот до двох тисяч неоподатковуваних мінімумів доходів громадян. Недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних, - тягне за собою накладення штрафу на громадян від ста до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб'єктів підприємницької діяльності - від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян. Повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню, - тягне за собою накладення штрафу від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян.	entails the imposition of a fine from three hundred to five hundred non-taxable minimum incomes on natural persons; on officials and entrepreneurs - from five hundred to two thousand non-taxable minimum incomes. Failure to comply with the procedure for protection of personal data established by the legislation on personal data protection, which has led to illegal access to the data or violation of the rights of the personal data subject, - entails the imposition of a fine from one hundred to five hundred non-taxable minimum incomes on natural persons; on officials and entrepreneurs - from three hundred to one thousand non-taxable minimum incomes. Repeated violation during the year a from the list provided in part 4 of this article, for which the person has already been subjected to an administrative penalty, - entails the imposition of a fine of one thousand to two thousand non-taxable minimum incomes.

Стаття 188-40 Кодексу України про адміністративні правопорушення: Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини або представників Уповноваженого Верховної Ради України з прав людини - тягне за собою накладення штрафу на посадових осіб, громадян - суб'єктів підприємницької діяльності від ста до двохсот неоподатковуваних мінімумів доходів громадян.	**Article 188-40 of the Code of Ukraine on Administrative offences:** Failure to comply with the legal requirements of the Ukrainian Parliament Commissioner for Human Rights or the authorised official - entails the imposition of a fine on officials, sole proprietors from one hundred to two hundred non-taxable minimum incomes.
Частина 1 статті 257 Кодексу України про адміністративні правопорушення: Протокол надсилається органу (посадовій особі), уповноваженому розглядати справу про адміністративне правопорушення.	**Paragraph 1 of Article 257 of the Code of Ukraine on Administrative Offences:** The protocol is sent to the body (official) authorized to consider the case of an administrative offence.
Частина 2 статті 294 Кодексу України про адміністративні правопорушення: Постанова судді у справі про адміністративне правопорушення може бути оскаржена протягом десяти днів з дня винесення постанови особою, яку притягнуто до адміністративної відповідальності, її законним представником, захисником, потерпілим, його представником, а також прокурором у випадках, передбачених частиною п'ятою статті 7 та частиною першою статті 287 цього Кодексу. Апеляційна скарга, подана після закінчення цього строку, повертається апеляційним судом особі, яка її подала, якщо вона не заявляє клопотання про поновлення цього строку, а також якщо у поновленні строку відмовлено.	**Part 2 of Article 294 of the Code of Ukraine on Administrative offences:** The decision of a judge in a case of an administrative offence may be appealed within ten days from the date of the decision by the person brought to administrative responsibility, his/her legal representative, attorney, victim, his/her representative, and the prosecutor in cases provided for in paragraph 5 of Article 7 and part one of Article 287 of this Code. An appeal filed after the expiration of this term shall be returned by the court of appeals to the person who filed it, if he / she does not apply for renewal of this term, as well as if the renewal of the term is denied.

Стаття 182 Кримінального кодексу України: 1. Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, - караються штрафом від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, - караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п'яти років, або позбавленням волі на той самий строк.	**Article 182 of the Criminal Code of Ukraine:** 1. Illegal collection, storage, use, destruction, dissemination of confidential personal information or illegal alteration of such information, except as provided by other articles of this Code, - shall be punishable by a fine of five hundred to one thousand tax-free minimum incomes, or correctional labour for a term up to two years, or arrest for a term up to six months, or restriction of liberty for a term up to three years. 2. The same acts committed repeatedly, or if they have caused significant damage to the rights, freedoms and interests of a person protected by law, - shall be punishable by arrest for a term of three to six months or by restriction of liberty for a term of three to five years, or by imprisonment for the same term.
Стаття 60 Цивільно процесуального Кодексу України: Особи, які можуть бути представниками 1. Представником у суді може бути адвокат або законний представник. 2. Під час розгляду спорів, що виникають з трудових відносин, а також справ у малозначних спорах (малозначні справи) представником може бути особа, яка досягла вісімнадцяти років, має цивільну процесуальну дієздатність, за винятком осіб, визначених у статті 61 цього Кодексу. 3. Органи або інших осіб, яким законом надано право звертатися до суду в інтересах малолітніх чи неповнолітніх осіб або осіб, які визнані судом недієздатними чи дієздатність яких обмежена,	**Article 60 of the Civil Procedure Code of Ukraine:** Persons who can be representatives 1. A representative in court may be a lawyer or a legal representative. 2. When considering disputes arising from labor relations, as well as cases in minor disputes (minor cases), the representative may be a person who has reached eighteen years of age, has civil procedural capacity, except for persons specified in Article 61 of this Code. 3. Bodies or other persons authorized by law to apply to a court in the interests of minors or persons recognized by a court as incapable or whose legal capacity is limited shall be represented in court by their officials, except

представляють у суді їх посадові особи, крім випадків, коли такі органи та особи є стороною чи третьою особою у справі. 4. Одна й та сама особа може бути одночасно представником декількох позивачів або декількох відповідачів або декількох третіх осіб на одній стороні, за умови відсутності конфлікту інтересів між ними. **Ст. 81 Цивільний процесуальний кодекс України:** 1. Кожна сторона повинна довести ті обставини, на які вона посилається як на підставу своїх вимог або заперечень, крім випадків, встановлених цим Кодексом. 2. У справах про дискримінацію позивач зобов'язаний навести фактичні дані, які підтверджують, що дискримінація мала місце. У разі наведення таких даних доказування їх відсутності покладається на відповідача. 3. У справах щодо застосування керівником або роботодавцем чи створення ним загрози застосування негативних заходів впливу до позивача (звільнення, примушування до звільнення, притягнення до дисциплінарної відповідальності, переведення, атестація, зміна умов праці, відмова в призначенні на вищу посаду, скорочення заробітної плати тощо) у зв'язку з повідомленням ним або членом його сім'ї про порушення вимог Закону України "Про запобігання корупції" іншою особою обов'язок доказування правомірності прийнятих при цьому рішень, вчинених дій покладається на відповідача. 4. У разі посилання учасника справи на невчинення іншим учасником справи певних дій або відсутність певної події суд може зобов'язати такого іншого учасника	in cases when such bodies and persons are a party or third party in the case. 4. The same person may simultaneously represent several plaintiffs or several defendants or several third parties on the same party, provided that there is no conflict of interest between them. **St. 81 Code of Civil Procedure of Ukraine:** 1. Each party must prove the circumstances to which it refers as the basis of its claims or objections, except as provided by this Code. 2. In cases of discrimination, the plaintiff is obliged to provide factual evidence that discrimination has taken place. In the case of such data, proof of their absence is entrusted to the defendant. 3. In cases of application by the manager or employer or threat of application of negative measures of influence to the plaintiff (dismissal, coercion to dismissal, disciplinary action, transfer, certification, change of working conditions, refusal to appoint to a higher position, reduction of salary, etc.) in connection with the notification by him or a member of his family of a violation of the Law of Ukraine 'On Prevention of Corruption' by another person, the burden of proving the legality of the decisions taken, the actions taken rests with the defendant. 4. In the event that a party to a case refers to the failure of another party to take certain actions or the absence of a certain event, the court may oblige such other party to the case to provide relevant evidence of the commission of these actions or the existence of a certain event. In case of failure to provide such evidence, the court may recognize the circumstance of failure to take appropriate action or the absence of the event established. 5. Evidence shall be submitted by the parties and other participants in the case.

справи надати відповідні докази вчинення цих дій або наявності певної події. У разі ненадання таких доказів суд може визнати обставину невчинення відповідних дій або відсутності події встановленою. 5. Докази подаються сторонами та іншими учасниками справи. 6. Доказування не може ґрунтуватися на припущеннях. 7. Суд не може збирати докази, що стосуються предмета спору, з власної ініціативи, крім витребування доказів судом у випадку, коли він має сумніви у добросовісному здійсненні учасниками справи їхніх процесуальних прав або виконанні обов'язків щодо доказів, а також інших випадків, передбачених цим Кодексом.	6. Proof cannot be based on assumptions. 7. The court may not collect evidence relating to the subject matter of the dispute on its own initiative, except for the demand of evidence by the court if it has doubts about the conscientious exercise by the parties of their procedural rights or performance of duties on evidence, as well as other cases this Code.
Стаття 263 Кримінального процесуального кодексу України: 1. Зняття інформації з транспортних телекомунікаційних мереж (мереж, що забезпечують передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого виду між підключеними до неї телекомунікаційними мережами доступу) є різновидом втручання у приватне спілкування, яке проводиться без відома осіб, які використовують засоби телекомунікацій для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можна встановити обставини, які мають значення для кримінального провадження. 2. В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента	**Article 263 of the Criminal Procedure Code of Ukraine:** 1. Withdrawal of information from transport telecommunication networks (networks that provide transmission of signs, signals, written text, images and sounds or messages of any kind between connected telecommunication access networks) is a kind of interference in private communication, which is carried out without the knowledge of persons , who use telecommunications to transmit information, on the basis of the decision of the investigating judge, if during its conduct it is possible to establish circumstances that are relevant to the criminal proceedings. 2. The decision of the investigating judge on permission to interfere in private communication in this case must additionally indicate the identification features that will uniquely identify the surveillance subscriber, transport telecommunications network,

спостереження, транспортну телекомунікаційну мережу, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування. 3. Зняття інформації з транспортних телекомунікаційних мереж полягає у проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою та має значення для досудового розслідування, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку. 4. Зняття інформації з транспортних телекомунікаційних мереж покладається на уповноважені підрозділи органів Національної поліції, Національного антикорупційного бюро України, Державного бюро розслідувань та органів безпеки. Керівники та працівники операторів телекомунікаційного зв'язку зобов'язані сприяти виконанню дій із зняття інформації з транспортних телекомунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді.	terminal equipment on which interference in private communication may be carried out. 3. Withdrawal of information from transport telecommunication networks consists in carrying out with the use of appropriate technical means of observation, selection and recording of the content of information transmitted by a person and relevant for pre-trial investigation, as well as receiving, converting and recording various types of signals transmitted by communication channels. language. 4. Withdrawal of information from transport telecommunication networks shall be entrusted to authorized subdivisions of the National Police, the National Anti-Corruption Bureau of Ukraine, the State Bureau of Investigation and security bodies. Managers and employees of telecommunications operators are obliged to assist in the implementation of actions to remove information from transport telecommunications networks, to take the necessary measures not to disclose the fact of such actions and the information received, to keep it unchanged.

Стаття 264 Кримінально процесуального кодексу України: 1. Пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування. 2. Не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту. 3. В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, в якій може здійснюватися втручання у приватне спілкування.	**Article 264 of the Criminal Procedure Code of Ukraine:** 1. Search, detection and recording of information contained in the electronic information system or their parts, access to the electronic information system or its part, as well as obtaining such information without the knowledge of its owner, possessor or holder may be carried out by decision of the investigating judge, if there is information about the availability of information in the electronic information system or its part, which is important for a certain pre-trial investigation. 2. Does not require the permission of the investigating judge to obtain information from electronic information systems or part thereof, access to which is not restricted by its owner, possessor or holder or is not related to overcoming the system of logical protection. 3. The decision of the investigating judge on the permission to interfere in private communication in this case must additionally indicate the identification features of the electronic information system in which interference in private communication may be carried out.
Стаття 8 Закону України «Про оперативно-розшукову діяльність»: Негласне обстеження публічно недоступних місць, житла чи іншого володіння особи, аудіо-, відеоконтроль особи, аудіо-, відеоконтроль місця, спостереження за особою, зняття інформації з транспортних телекомунікаційних мереж, електронних інформаційних мереж, накладення арешту на кореспонденцію, здійснення її огляду та	Article 8 of the Law of Ukraine 'On operational and investigative activities': Covert inspection of publicly inaccessible places, housing or other property of a person, audio, video surveillance of a person, audio, video surveillance of a person, surveillance of a person, removal of information from transport telecommunication networks, electronic information networks, seizure of correspondence, inspection and seizure, establishment of the location of the electronic

виїмки, установлення місцезнаходження радіоелектронного засобу проводяться на підставі ухвали слідчого судді, постановленої за клопотанням керівника відповідного оперативного підрозділу або його заступника, погодженого з прокурором. Ці заходи застосовуються виключно з метою запобігання вчиненню тяжкого або особливо тяжкого злочину, запобігання і припинення терористичних актів та інших посягань спеціальних служб іноземних держав та організацій, якщо іншим способом одержати інформацію неможливо.	means is carried out on the basis of the decision of the investigating judge, made at the request of the head of the relevant operational unit or his deputy, agreed with the prosecutor. These measures are used solely to prevent the commission of a serious or particularly serious crime, to prevent and stop terrorist acts and other encroachments by special services of foreign states and organizations, if otherwise it is impossible to obtain information.
Пункт 1.11.5. Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: 1.11.5. Зняття інформації з транспортних телекомунікаційних мереж полягає в негласному проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду). **1.11.5.1. Зняття інформації з транспортних телекомунікаційних мереж поділяється на:** - контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та	**Clause 1.11.5. Instructions on the organization of covert investigative (search) actions and the use of their results in criminal proceedings:** 1.11.5. Withdrawal of information from transport telecommunications networks is the covert conduct with the use of appropriate technical means of monitoring, selection and recording of the content of information transmitted by a person, as well as receiving, converting and recording various types of signals transmitted by communication channels (signs, signals, written text, images, sounds, messages of any kind). **1.11.5.1. Withdrawal of information from transport telecommunications networks is divided into:** - control over telephone conversations, which consists in secret conduct with the use of appropriate technical means, including those installed on transport telecommunication networks, surveillance, selection and recording of telephone conversations, other information and signals (SMS, MMS, facsimile, modem communication, etc.), which are transmitted

фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний зв'язок тощо), які передаються телефонним каналом зв'язку, що контролюється; - зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні і фіксації із застосуванням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються.	by the telephone communication channel under control; - removal of information from communication channels, which consists in the secret receipt, conversion and recording using technical means, including those installed on transport telecommunications networks, in the appropriate form of various types of signals transmitted by communication channels of the Internet, other networks controlled data transmission.
Пункт 1.11.6. Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: 1.11.6. Зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача (ст. 264 КПК України) полягає в одержані інформації, у тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі.	**Clause 1.11.6. Instructions on the organization of covert investigative (search) actions and the use of their results in criminal proceedings:** 1.11.6. Withdrawal of information from electronic information systems without the knowledge of its owner, possessor or holder (Article 264 of the CPC of Ukraine) is the information obtained, including the use of technical equipment contained in computers (computer), automatic systems, computer network.

Стаття 246 Кримінально процесуального кодексу України: Стаття 246. Підстави проведення негласних слідчих (розшукових) дій 1. Негласні слідчі (розшукові) дії - це різновид слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених цим Кодексом. 2. Негласні слідчі (розшукові) дії проводяться у випадках, якщо відомості про кримінальне правопорушення та особу, яка його вчинила, неможливо отримати в інший спосіб. Негласні слідчі (розшукові) дії, передбачені статтями 260, 261, 262, 263, 264 (в частині дій, що проводяться на підставі ухвали слідчого судді), 267, 269, 269-1, 270, 271, 272, 274 цього Кодексу, проводяться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів. 3. Рішення про проведення негласних слідчих (розшукових) дій приймає слідчий, прокурор, а у випадках, передбачених цим Кодексом, - слідчий суддя за клопотанням прокурора або за клопотанням слідчого, погодженого з прокурором. Слідчий зобов'язаний повідомити прокурора про прийняття рішення щодо проведення певних негласних слідчих (розшукових) дій та отримані результати. Прокурор має право заборонити проведення або припинити подальше проведення негласних слідчих (розшукових) дій. 4. Виключно прокурор має право прийняти рішення про проведення такої негласної слідчої (розшукової) дії, як контроль за вчиненням злочину.	**Article 246 of the Criminal Procedure Code of Ukraine:** Article 246. Grounds for conducting covert investigative (search) actions 1. Undercover investigative (search) actions are a type of investigative (search) actions, information on the fact and methods of which are not subject to disclosure, except for the cases provided by this Code. 2. Covert investigative (search) actions shall be carried out in cases when information on a criminal offense and the person who committed it cannot be obtained in any other way. Covert investigative (search) actions provided for in Articles 260, 261, 262, 263, 264 (in part of actions carried out on the basis of a decision of the investigating judge), 267, 269, 269-1, 270, 271, 272, 274 of this Code, are conducted exclusively in criminal proceedings for serious or especially serious crimes. 3. The decision to conduct covert investigative (search) actions shall be made by the investigator, prosecutor, and in cases provided for by this Code - the investigating judge at the request of the prosecutor or at the request of the investigator agreed with the prosecutor. The investigator is obliged to inform the prosecutor about the decision to conduct certain covert investigative (search) actions and the results obtained. The prosecutor has the right to prohibit or suspend further covert investigative (search) actions. 4. Only the prosecutor has the right to make a decision on conducting such covert investigative (search) action as control over the commission of a crime.

Стаття 254 Кримінально процесуального кодексу України: Стаття 254**.** Заходи щодо захисту інформації, отриманої в результаті проведення негласних слідчих (розшукових) дій 1. Відомості про факт та методи проведення негласних слідчих (розшукових) дій, осіб, які їх проводять, а також інформація, отримана в результаті їх проведення, не підлягають розголошенню особами, яким це стало відомо в результаті ознайомлення з матеріалами в порядку, передбаченому статтею 290 цього Кодексу. 2. Якщо протоколи про проведення негласних слідчих (розшукових) дій містять інформацію щодо приватного (особистого чи сімейного) життя інших осіб, захисник, а також інші особи, які мають право на ознайомлення з протоколами, попереджаються про кримінальну відповідальність за розголошення отриманої інформації щодо інших осіб. 3. Виготовлення копій протоколів про проведення негласних слідчих (розшукових) дій та додатків до них до прийняття рішення про їх розсекречування у порядку, визначеному законодавством, не допускається.	**Article 254 of the Criminal Procedure Code of Ukraine:** Article 254. Measures for protection of the information received as a result of carrying out secret investigative (search) actions 1. Information on the fact and methods of conducting covert investigative (search) actions, persons conducting them, as well as information obtained as a result of their conduct, shall not be disclosed to persons who became aware of it as a result of reviewing the materials in accordance with Article 290 of this Code. 2. If the protocols on conducting covert investigative (search) actions contain information on the private (personal or family) life of other persons, the defense counsel, as well as other persons entitled to review the protocols, shall be warned of criminal liability for disclosure of information persons. 3. Making copies of protocols on conducting covert investigative (search) actions and appendices to them before making a decision on their declassification in the manner prescribed by law is not allowed.

Стаття 255 Кримінально процесуального кодексу України: Стаття 255. Заходи щодо захисту інформації, яка не використовується у кримінальному провадженні 1. Відомості, речі та документи, отримані в результаті проведення негласних слідчих (розшукових) дій, які прокурор не визнає необхідними для подальшого проведення досудового розслідування, повинні бути невідкладно знищені на підставі його рішення, крім випадків, передбачених частиною третьою цієї статті та статтею 256 цього Кодексу. 2. Забороняється використання зазначених у частині першій цієї статті матеріалів для цілей, не пов'язаних з кримінальним провадженням, або ознайомлення з ними учасників кримінального провадження чи будь-яких інших осіб. 3. У разі якщо власник речей або документів, отриманих у результаті проведення негласних слідчих (розшукових) дій, може бути зацікавлений у їх поверненні, прокурор зобов'язаний повідомити його про наявність таких речей або документів у розпорядженні прокурора та з'ясувати, чи бажає він їх повернути. Допустимість дій, передбачених цією частиною, та час їх вчинення визначаються прокурором з урахуванням необхідності забезпечення прав та законних інтересів осіб, а також запобігання завданню шкоди для кримінального провадження.	**Article 255 of the Code of Criminal Procedure of Ukraine:** Article 255. Measures on protection of the information which is not used in criminal proceedings 1. Information, things and documents obtained as a result of covert investigative (search) actions, which the prosecutor does not consider necessary for further pre-trial investigation, shall be immediately destroyed on the basis of his decision, except as provided in part three of this article and article 256 of this Code. 2. It is prohibited to use the materials specified in part one of this article for purposes not related to criminal proceedings, or to acquaint them with the participants in criminal proceedings or any other persons. 3. If the owner of things or documents obtained as a result of covert investigative (search) actions may be interested in their return, the prosecutor shall notify him of the presence of such things or documents at the disposal of the prosecutor and determine whether he wishes he will return them. The admissibility of the actions provided for in this part and the time of their commission shall be determined by the prosecutor, taking into account the need to ensure the rights and legitimate interests of persons, as well as to prevent harm to criminal proceedings.

Стаття 41 Кримінально процесуального кодексу України: 2. Під час виконання доручень слідчого, дізнавача, прокурора співробітник оперативного підрозділу користується повноваженнями слідчого. Співробітники оперативних підрозділів (крім підрозділу детективів, підрозділу внутрішнього контролю Національного антикорупційного бюро України) не мають права здійснювати процесуальні дії у кримінальному провадженні за власною ініціативою або звертатися з клопотаннями до слідчого судді чи прокурора.	**Article 41 of the Criminal Procedure Code of Ukraine:** 2. During the execution of the instructions of the investigator, coroner, prosecutor, the employee of the operational unit shall use the powers of the investigator. Employees of operational units (except for the detective unit, the internal control unit of the National Anti-Corruption Bureau of Ukraine) have no right to carry out procedural actions in criminal proceedings on their own initiative or to apply to the investigating judge or prosecutor.
Закон України «Про захист персональних даних», частина 4-5 статті 4: Володілець персональних даних може доручити обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі. Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, визначених у договорі.	**Law of Ukraine 'On the Protection of Personal Data', part 4 of the art 4:** The owner of personal data may entrust personal data processing to the manager of personal data under an agreement concluded in writing form Law of Ukraine 'On the Protection of Personal Data', part 5 of the art 4: The controller of personal data can process personal data only for the purposes and to the extent specified in the contract.
Закон України «Про захист персональних даних», частина 2 статті 15: Персональні дані підлягають видаленню або знищенню у разі: 1) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом; 2) припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом;	**Law of Ukraine 'On the Protection of Personal Data', part 2 of the art 15:** Personal data is subject to deletion or destruction in the case of: 1) expiration of the data storage period determined by the consent of the personal data subject to the processing of these data or by law; 2) termination of the legal relationship between the personal data subject and the owner or administrator, unless otherwise provided by law;

3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого; 4) набрання законної сили рішенням суду щодо видалення або знищення персональних даних.	3) issuance of the relevant instruction of the Commissioner or officials of the Secretariat of the Commissioner appointed by him; 4) entry into force of a court decision on the removal or destruction of personal data.
Закон України «Про захист персональних даних», пункт 10 частина 1 статті 23: 1. Уповноважений має такі повноваження у сфері захисту персональних даних: 10) складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом.	**Law of Ukraine 'On the Protection of Personal Data', paragraph 10 part 1 of the art 23:** 1. The Commissioner has the following powers in the field of personal data protection: 10) draw up protocols on bringing to administrative responsibility and send them to court in cases provided by law.
Закон України «Про захист персональних даних», частина 2 статті 16: 2. Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог цього Закону або неспроможна їх забезпечити.	**Law of Ukraine 'On Personal Data Protection of', part 2 of the art 16:** 2. Access to personal data shall not be granted to a third party if the said person refuses to undertake obligations to ensure compliance with the requirements of this Law or is unable to provide them.
Закон України «Про захист персональних даних», пункт 1 частина 3 статті 29: 3. Передача персональних даних іноземним суб'єктам відносин, пов'язаних із персональнимиданими, здійснюється лише за умови забезпечення відповідною державою належного захисту персональних даних у випадках, встановлених законом або міжнародним договором України.	**Law of Ukraine 'On the Protection of Personal Data', paragraph 1 part 3 of the art 29:** 3. The transfer of personal data to foreign subjects of relations related to personal data is carried out only if the relevant state provides adequate protection of personal data in cases established by law or international treaty of Ukraine.

Закон України «Про захист персональних даних», пункт 1 частина 4 статті 29: 4. Персональні дані можуть передаватися іноземним суб'єктам відносин, пов'язаних з персональними даними, також у разі: 1) надання суб'єктом персональних даних однозначної згоди на таку передачу;	**Law of Ukraine 'On the Protection of Personal Data', paragraph 1 part 4 of the art 29:** 4. Personal data may be transferred to foreign subjects of relations related to personal data, also in the case of: 1) granting by the subject of personal data unambiguous consent to such transfer;
Цивільний Кодекс України, частина 1-2 стаття 634: 1. Договором приєднання є договір, умови якого встановлені однією із сторін у формулярах або інших стандартних формах, який може бути укладений лише шляхом приєднання другої сторони до запропонованого договору в цілому. Друга сторона не може запропонувати свої умови договору. 2. Договір приєднання може бути змінений або розірваний на вимогу сторони, яка приєдналася, якщо вона позбавляється прав, які звичайно мала, а також якщо договір виключає чи обмежує відповідальність другої сторони за порушення зобов'язання або містить інші умови, явно обтяжливі для сторони, яка приєдналася. Сторона, яка приєдналася, має довести, що вона, виходячи зі своїх інтересів, не прийняла б цих умов за наявності у неї можливості брати участь у визначенні умов договору.	**Civil Code of Ukraine, part 1-2 of the art 634:** 1. A treaty of accession is a treaty, the terms of which are established by one of the parties in forms or other standard forms, which can be concluded only by the accession of the other party to the proposed treaty as a whole. The other party cannot offer its terms of the contract. 2. A treaty of accession may be amended or terminated at the request of a party which has acceded if it loses the rights which it normally had, and if the treaty excludes or limits the liability of the other party for breach of obligation or contains other conditions manifestly burdensome for the party, who joined. The acceding party must prove that, in its interests, it would not have accepted these terms if it had had the opportunity to participate in determining the terms of the contract.

Кодекс України про адміністративні правопорушення, частина 4-5, стаття 188: Недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних, - тягне за собою накладення штрафу на громадян від ста до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб'єктів підприємницької діяльності - від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян. Повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню, - тягне за собою накладення штрафу від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян.	**Code of Ukraine on Administrative Offenses, part 4-5 of the art 188:** Failure to comply with the procedure for protection of personal data established by the legislation on personal data protection, which has led to illegal access to them or violation of the rights of the personal data subject, - entails the imposition of a fine on citizens from one hundred to five hundred non-taxable minimum incomes and on officials, citizens - business entities - from three hundred to one thousand non-taxable minimum incomes. Repeated during the year the commission of the violation provided for in part four of this article, for which the person has already been subjected to an administrative penalty, - entails the imposition of a fine of one thousand to two thousand non-taxable minimum incomes.
стаття 182 Кримінального Кодексу України, : Стаття 182. Порушення недоторканності приватного життя 1. Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, - караються штрафом від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними	**art 182 of the Criminal Code of Ukraine:** Article 182. Violation of privacy 1. Illegal collection, storage, use, destruction, dissemination of confidential personal information or illegal alteration of such information, except as provided by other articles of this Code, - shall be punishable by a fine of five hundred to one thousand tax-free minimum incomes, or correctional labor for a term up to two years, or arrest for a term up to six months, or restriction of liberty for a term up to three years.

роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, - караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п'яти років, або позбавленням волі на той самий строк. Примітка. Істотною шкодою у цій статті, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян. Публічне, у тому числі через засоби масової інформації, журналістів, громадські об'єднання, професійні спілки, повідомлення особою інформації про вчинення кримінального або іншого правопорушення, здійснене з дотриманням вимог закону, не є діями, передбаченими цією статтею, і не тягне за собою кримінальну відповідальність.	2. The same acts committed repeatedly, or if they have caused significant damage to the rights, freedoms and interests of a person protected by law, - shall be punishable by arrest for a term of three to six months or by restriction of liberty for a term of three to five years, or by imprisonment for the same term. Note. Significant damage in this article, if it consists in causing material damage, is considered to be such damage, which is one hundred and more times higher than the tax-free minimum income of citizens. Public, including through the media, journalists, public associations, trade unions, personal information about a criminal or other offense committed in compliance with the law, are not actions under this article, and does not entail criminal responsibility.
Стаття 15 Конституції України: Суспільне життя в Україні ґрунтується на засадах політичної, економічної та ідеологічної багатоманітності. Жодна ідеологія не може визнаватися державою як обов'язкова. Цензура заборонена. Держава гарантує свободу політичної діяльності, не забороненої Конституцією і законами України.	**Article 15 of the Constitution of Ukraine:** Public life in Ukraine is based on the principles of political, economic and ideological diversity. No ideology can be recognized by the state as obligatory. Censorship is prohibited. The state guarantees freedom of political activity, which is not prohibited by the Constitution and laws of Ukraine.

Конституція України. Стаття 34: Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.	**Constitution of Ukraine. Article 34:** Everyone is guaranteed the right to freedom of thought and speech, to free expression of their views and beliefs. Everyone has the right to freely collect, store, use and disseminate information orally, in writing or otherwise - at their discretion. The exercise of these rights may be restricted by law in the interests of national security, territorial integrity or public order in order to prevent riots or crimes, to protect public health, to protect the reputation or rights of others, to prevent the disclosure of confidential information or to maintain authority and impartiality of justice.
Конституція України. Стаття 37: Утворення і діяльність політичних партій та громадських організацій, програмні цілі або дії яких спрямовані на ліквідацію незалежності України, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності держави, підрив її безпеки, незаконне захоплення державної влади, пропаганду війни, насильства, на розпалювання міжетнічної, расової, релігійної ворожнечі, посягання на права і свободи людини, здоров'я населення, забороняються. Політичні партії та громадські організації не можуть мати воєнізованих формувань. Не допускається створення і діяльність організаційних структур політичних партій в органах виконавчої та судової влади і виконавчих органах місцевого самоврядування, військових формуваннях, а також на державних підприємствах, у	**Constitution of Ukraine. Article 37:** Formation and activity of political parties and public organizations, whose program goals or actions are aimed at eliminating Ukraine's independence, forcibly changing the constitutional order, violating the sovereignty and territorial integrity of the state, undermining its security, illegal seizure of state power, propaganda of war, violence, to incite interethnic, racial, religious hatred, encroachment on human rights and freedoms, public health, are prohibited. Political parties and public organizations cannot have paramilitary formations. It is not allowed to create and operate organizational structures of political parties in executive and judicial bodies and executive bodies of local self-government, military formations, as well as at state enterprises, educational institutions and other state institutions and organizations. Prohibition of the activity of associations of citizens is carried out only in court.

навчальних закладах та інших державних установах і організаціях. Заборона діяльності об'єднань громадян здійснюється лише в судовому порядку.	
Закон України "Про захист персональних даних". Стаття 8: Права суб'єкта персональних даних. 1. Особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними. 2. Суб'єкт персональних даних має право: 1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом; 2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані; 3) на доступ до своїх персональних даних; 8) звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду; 9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних; 10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди; 11) відкликати згоду на обробку персональних даних; 12) знати механізм автоматичної обробки персональних даних; 13) на захист від автоматизованого рішення, яке має для нього правові наслідки.	**Law of Ukraine 'On Personal Data Protection'. Article 8:** Rights of the subject of personal data. 1. Personal inalienable rights to personal data that every individual has are inalienable and inviolable. 2. The personal data subject has the right to: 1) know about the sources of collection, location of their personal data, the purpose of their processing, location or place of residence (stay) of the owner or controller of personal data or give a corresponding order to obtain this information to authorized persons, except as provided by law; 2) receive information on the conditions for granting access to personal data, in particular information on third parties to whom his personal data is transferred; 3) access to their personal data; 8) apply to the Commissioner or to the court with complaints about the processing of their personal data; 9) apply legal remedies in case of violation of the legislation on personal data protection; 10) make reservations regarding the restriction of the right to process their personal data during the consent; 11) withdraw consent to the processing of personal data; 12) know the mechanism of automatic processing of personal data; 13) to protect against an automated decision that has legal consequences for him.

Закон України "Про санкції". Стаття 1: Суверенне право України на захист. 1. З метою захисту національних інтересів, національної безпеки, суверенітету і територіальної цілісності України, протидії терористичній діяльності, а також запобігання порушенню, відновлення порушених прав, свобод та законних інтересів громадян України, суспільства та держави можуть застосовуватися спеціальні економічні та інші обмежувальні заходи (далі - санкції).	**Law of Ukraine 'On Sanctions' Article 1:** Sovereign right of Ukraine to protection. 1. In order to protect the national interests, national security, sovereignty and territorial integrity of Ukraine, counter terrorist activities, as well as prevent violations, restore violated rights, freedoms and legitimate interests of citizens of Ukraine, society and the state, special economic and other restrictive measures may be applied. - sanctions).
Закон України "Про санкції". Стаття 4: Види санкцій. 1. Видами санкцій згідно з цим Законом є: 25) інші санкції, що відповідають принципам їх застосування, встановленому цим Законом. 2. Санкції згідно з цим Законом не є заходами захисту прав та інтересів суб'єктів зовнішньоекономічної діяльності, порядок та умови застосування яких регулюються спеціальним законом. 3. У разі якщо на дії, вчинення яких потребує одержання дозволу органів Антимонопольного комітету України на концентрацію, поширюються спеціальні економічні та інші обмежувальні заходи (санкції), передбачені частиною першою цієї статті, така концентрація забороняється, і дозвіл на її здійснення органами Антимонопольного комітету України не надається.	**Law of Ukraine 'On Sanctions'. Article 4:** Types of sanctions. 1. Types of sanctions under this Law are: 25) other sanctions that comply with the principles of their application established by this Law. 2. Sanctions in accordance with this Law are not measures to protect the rights and interests of subjects of foreign economic activity, the procedure and conditions of application of which are regulated by a special law. 3. If special economic and other restrictive measures (sanctions) provided for in part one of this Article apply to actions that require the permission of the Antimonopoly Committee of Ukraine, such concentration shall be prohibited, and permission for its implementation by the Antimonopoly Committee of Ukraine not provided.

Закон України "Про авторське право та суміжні права". Стаття 52-1: Порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет. 1. При порушенні будь-якою особою авторського права і (або) суміжних прав, вчиненому з використанням мережі Інтернет, суб'єкт авторського права і (або) суміжних прав (далі - заявник) має право звернутися до власника веб-сайту та (або) веб-сторінки, на якому (якій) розміщена або в інший спосіб використана відповідна електронна (цифрова) інформація, із заявою про припинення порушення. Заява про припинення порушення подається в порядку, передбаченому цією статтею. Порядок захисту авторського права і (або) суміжних прав, визначений цією статтею, застосовується до відносин, пов'язаних з використанням аудіовізуальних творів, музичних творів, комп'ютерних програм, відеограм, фонограм, передач (програм) організацій мовлення.	**Law of Ukraine 'On Copyright and Related Rights'. Article 52-1:** Procedure for terminating infringements of copyright and (or) related rights using the Internet. 1. In case of infringement by any person of copyright and (or) related rights committed using the Internet, the subject of copyright and (or) related rights (hereinafter - the applicant) has the right to apply to the owner of the website and (or) a web page on which (which) the relevant electronic (digital) information is posted or otherwise used, with a statement on termination of the violation. The application for termination of the violation shall be submitted in accordance with the procedure provided for in this Article. The procedure for protection of copyright and (or) related rights, defined in this article, applies to relations related to the use of audiovisual works, musical works, computer programs, videograms, phonograms, programs (programs) of broadcasting organizations.
Конституція України, ст. 31: Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.	**Constitution of Ukraine, Art. 31:** Everyone is guaranteed the secrecy of correspondence, telephone conversations, telegraph and other correspondence. Exceptions may be established only by a court in cases provided by law, in order to prevent a crime or to find out the truth during the investigation of a criminal case, if it is impossible to obtain information by other means.

Конституція України, ст. 32: Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.	**Constitution of Ukraine, Art. 32:** No one may interfere in his personal and family life, except as provided by the Constitution of Ukraine. The collection, storage, use and dissemination of confidential information about a person without his or her consent is not permitted, except in cases specified by law and only in the interests of national security, economic well-being and human rights. Every citizen has the right to get acquainted with information about himself in public authorities, local governments, institutions and organizations, which is not a state or other secret protected by law. Everyone is guaranteed judicial protection of the right to refute inaccurate information about themselves and their family members and the right to demand the removal of any information, as well as the right to compensation for material and moral damage caused by the collection, storage, use and dissemination of such inaccurate information.
Цивільний кодекс України, ст. 286: Право на таємницю про стан здоров'я. 1.Фізична особа має право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при її медичному обстеженні. 2. Забороняється вимагати та подавати за місцем роботи або навчання інформацію про діагноз та методи лікування фізичної особи. 3. Фізична особа зобов'язана утримуватися від поширення інформації, зазначеної у частині першій цієї статті, яка стала їй	**Civil Code of Ukraine, Art. 286:** The right to secrecy about health. 1.An individual has the right to secrecy about the state of his health, the fact of seeking medical care, diagnosis, as well as information obtained during his medical examination. 2. It is prohibited to request and submit at the place of work or study information about the diagnosis and treatment of an individual. 3. An individual is obliged to refrain from disseminating the information specified in part one of this article, which became known to him in connection with the performance of official duties or from other sources.

відома у зв'язку з виконанням службових обов'язків або з інших джерел. 4. Фізична особа може бути зобов'язана до проходження медичного огляду у випадках, встановлених законодавством.	4. An individual may be obliged to undergo a medical examination in cases established by law.
Цивільний кодекс України, ст. 301: Право на особисте життя та його таємницю. 1. Фізична особа має право на особисте життя. 2. Фізична особа сама визначає своє особисте життя і можливість ознайомлення з ним інших осіб. 3. Фізична особа має право на збереження у таємниці обставин свого особистого життя. 4. Обставини особистого життя фізичної особи можуть бути розголошені іншими особами лише за умови, що вони містять ознаки правопорушення, що підтверджено рішенням суду, а також за її згодою.	**Civil Code of Ukraine, Art. 301:** The right to privacy and its secrecy. 1. An individual has the right to privacy. 2. An individual determines his personal life and the possibility of acquaintance with it by other persons. 3. An individual has the right to keep the circumstances of his personal life secret. 4. Circumstances of a private person's personal life may be disclosed to other persons only if they contain signs of an offense, which is confirmed by a court decision, as well as with his consent.
Цивільний кодекс України, ст. 302: Право на інформацію. 1.Фізична особа має право вільно збирати, зберігати, використовувати і поширювати інформацію. Збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. 2.Фізична особа, яка поширює інформацію, зобов'язана переконатися в її достовірності. Фізична особа, яка поширює інформацію, отриману з офіційних джерел (інформація органів державної влади, органів місцевого самоврядування, звіти, стенограми тощо),	**Civil Code of Ukraine, Art. 302:** Right to information. 1.An individual has the right to freely collect, store, use and disseminate information. Collection, storage, use and dissemination of information about the personal life of an individual without his consent are not allowed, except as provided by law, and only in the interests of national security, economic well-being and human rights. 2. The individual who disseminates the information is obliged to verify its authenticity. An individual who disseminates information obtained from official sources (information of public authorities, local governments, reports, transcripts, etc.) is not obliged to verify its authenticity and is not responsible in case of refutation. An individual who disseminates

не зобов'язана перевіряти її достовірність та не несе відповідальності в разі її спростування. Фізична особа, яка поширює інформацію, отриману з офіційних джерел, зобов'язана робити посилання на таке джерело.	information obtained from official sources is obliged to refer to such a source.
Цивільний кодекс України, ст. 306: Право на таємницю кореспонденції. 1.Фізична особа має право на таємницю листування, телеграм, телефонних розмов, телеграфних повідомлень та інших видів кореспонденції. Листи, телеграми тощо є власністю адресата. 2.Листи, телеграми та інші види кореспонденції можуть використовуватися, зокрема шляхом опублікування, лише за згодою особи, яка направила їх, та адресата. Якщо кореспонденція стосується особистого життя іншої фізичної особи, для її використання, зокрема шляхом опублікування, потрібна згода цієї особи. 3. У разі смерті фізичної особи, яка направила кореспонденцію, і адресата використання кореспонденції, зокрема шляхом її опублікування, можливе лише за згодою фізичних осіб, визначених частиною четвертою статті 303 цього Кодексу [діти, вдови та вдівці, за їх відсутності – батьки, брати і сестри]. У разі смерті фізичної особи, яка направила кореспонденцію, і адресата, а також у разі смерті фізичних осіб, визначених частиною четвертою статті 303 цього Кодексу, кореспонденція, яка має наукову, художню, історичну цінність, може бути опублікована в порядку, встановленому законом.	**Civil Code of Ukraine, Art. 302:** The right to secrecy of correspondence. 1.An individual has the right to secrecy of correspondence, telegrams, telephone conversations, telegraph messages and other types of correspondence. Letters, telegrams, etc. are the property of the addressee. 2. Letters, telegrams and other types of correspondence may be used, in particular by publication, only with the consent of the person who sent them and the addressee. If the correspondence concerns the private life of another natural person, its use, in particular by publication, requires the consent of that person. 3. In case of death of the natural person who sent the correspondence and the addressee, the use of correspondence, in particular by its publication, is possible only with the consent of natural persons defined in part four of Article 303 of this Code [children, widows and widowers, in their absence - parents, brothers and sisters]. In the event of the death of the individual who sent the correspondence and the addressee, as well as in the event of the death of individuals specified in part four of Article 303 of this Code, correspondence of scientific, artistic, historical value may be published in accordance with law. 4.Correspondence concerning a natural person may be attached to a court case only if it contains evidence relevant to the resolution

4. Кореспонденція, яка стосується фізичної особи, може бути долучена до судової справи лише у разі, якщо в ній містяться докази, що мають значення для вирішення справи. Інформація, яка міститься в такій кореспонденції, не підлягає розголошенню. 5.Порушення таємниці кореспонденції може бути дозволено судом у випадках, встановлених законом, з метою запобігання кримінальному правопорушенню чи під час кримінального провадження, якщо іншими способами одержати інформацію неможливо.	of the case. The information contained in such correspondence shall not be disclosed. 5. Violation of the secrecy of correspondence may be permitted by a court in cases established by law, in order to prevent a criminal offense or during criminal proceedings, if it is impossible to obtain information by other means.
Закон України "Про свободу совісті та релігійні організації", ст. 3: Ніхто не має права вимагати від священнослужителів відомостей, одержаних ними при сповіді віруючих.	**The Law of Ukraine 'On freedom of conscience and religious organizations', Art. 3:** No one has the right to demand from the clergy the information obtained by them during the confession of the faithful.
Сімейний кодекс України, ст. 226: 1. Особа має право на таємницю перебування на обліку тих, хто бажає усиновити дитину, пошуку дитини для усиновлення, подання заяви про усиновлення та її розгляду, рішення суду про усиновлення. 2. Дитина, яка усиновлена, має право на таємницю, в тому числі і від неї самої, факту її усиновлення. 3. Особа, яка була усиновлена, має право після досягнення нею чотирнадцяти років на одержання інформації щодо свого усиновлення.	**Family Code of Ukraine, Art. 226:** 1. A person has the right to secrecy of registration of those who wish to adopt a child, search for a child for adoption, submission of an application for adoption and its consideration, court decision on adoption. 2. An adopted child has the right to secrecy, including from himself, of the fact of his adoption. 3. A person who has been adopted has the right to receive information on his / her adoption after reaching the age of fourteen.

Закон України «Про нотаріат», ст. 8: Нотаріальна таємниця - сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, в тому числі про особу, її майно, особисті майнові та немайнові права і обов'язки тощо. Нотаріус та особи, зазначені у статті 1 цього Закону [уповноважені особи органів місцевого самоврядування, консульські установи, дипломатичні представництва, головні лікарі, їх заступники з медичної частини, чергові лікарі, капітани суден, начальники експедицій, начальники військових частин та військових навчальних закладів, начальники установ виконання покарань, начальники слідчих ізоляторів], а також помічник нотаріуса зобов'язані зберігати нотаріальну таємницю, навіть якщо їх діяльність обмежується наданням правової допомоги чи ознайомленням з документами і нотаріальна дія або дія, яка прирівнюється до нотаріальної, не вчинялась. Обов'язок дотримання нотаріальної таємниці поширюється також на осіб, яким про вчинені нотаріальні дії стало відомо у зв'язку з виконанням ними службових обов'язків чи іншої роботи, на осіб, залучених для вчинення нотаріальних дій у якості свідків, та на інших осіб, яким стали відомі відомості, що становлять предмет нотаріальної таємниці. Особи, винні в порушенні нотаріальної таємниці, несуть відповідальність у порядку, встановленому законом.	**The Law of Ukraine 'On notary'** Notarial secrecy - a set of information obtained during the performance of a notarial act or appeal to the notary of the person concerned, including the person, his property, personal property and non-property rights and obligations, etc. Notary and persons referred to in Article 1 of this Law [authorized persons of local self-government bodies, consular posts, diplomatic missions, chief physicians, their medical deputies, doctors on duty, ship captains, chiefs of expeditions, chiefs of military units and military educational establishments, chiefs penitentiary institutions, heads of pre-trial detention centers], as well as the assistant notary are obliged to maintain notarial secrecy, even if their activities are limited to providing legal assistance or access to documents and a notarial act or an act equivalent to a notarial act has not been performed. The obligation to observe notarial secrecy also applies to persons who became aware of the notarial acts performed in connection with the performance of their official duties or other work, to persons involved in the performance of notarial acts as witnesses, and to other persons which became known information that is the subject of notarial secrecy. Persons guilty of violating a notarial secret shall be liable in accordance with the procedure established by law.

Закон України «Про банки та банківську діяльність», ст. 60: Інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку, є банківською таємницею. Банківською таємницею, зокрема, є: 1. відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України; 2. операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; 3. фінансово-економічний стан клієнтів; 4. системи охорони банку та клієнтів; 5. інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності; 6. відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація; 7. інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню; 8. коди, що використовуються банками для захисту інформації; 9. інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності. 10. Інформація про банки чи клієнтів, що збирається під час проведення	**The Law of Ukraine 'On banks and banking', Art. 60:** Information on the activity and financial condition of the client, which became known to the bank in the process of servicing the client and the relationship with him or third parties in the provision of bank services, is a bank secret. Banking secrecy, in particular, is: 1. Information on clients' bank accounts, including correspondent accounts of banks with the National Bank of Ukraine; 2. Transactions that were carried out for the benefit or on behalf of the client, transactions carried out by him; 3. Financial and economic condition of customers; 4. Bank and customer security systems; 5. Information on the organizational and legal structure of the legal entity - the client, its leaders, activities; 6. Information on commercial activities of clients or trade secrets, any project, inventions, product samples and other commercial information; 7. Information on reporting by a separate bank, except for that which is subject to publication; 8. Codes used by banks to protect information; 9. Information on an individual who intends to enter into a consumer loan agreement, obtained during the assessment of its creditworthiness. 10. Information about banks or customers collected during banking and currency supervision is a bank secret. 11. Information on banks or clients received by the National Bank of Ukraine in accordance with an international agreement or

банківського та валютного нагляду, становить банківську таємницю. Інформація про банки чи клієнтів, отримана Національним банком України відповідно до міжнародного договору або за принципом взаємності від органу банківського нагляду іншої держави для використання з метою банківського нагляду або запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, чи фінансуванню тероризму, становить банківську таємницю.	on the principle of reciprocity from a banking supervisory authority of another state for use for banking supervision or prevention of money laundering or terrorist financing is banking secret.
Кримінальний процесуальний Кодекс України, ст. 7: Загальні засади кримінального провадження. Зміст та форма кримінального провадження повинні відповідати загальним засадам кримінального провадження, до яких, зокрема, відносяться: 7. таємниця спілкування; 8. невтручання у приватне життя;	**Code of Criminal Procedure of Ukraine, Art. 7:** General principles of criminal proceedings. The content and form of criminal proceedings must comply with the general principles of criminal proceedings, which include, in particular: 7. the secret of communication; 8. non-interference in private life;
Закон України «Про інформацію», ст. 11: Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.	**The Law of Ukraine 'On Information', Art. 11:** Information about an individual (personal data) - information or a set of information about an individual that is identified or can be specifically identified.
Закон України «Про захист персональних даних», ст. 2: персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.	**The Law of Ukraine 'On Personal Data Protection', Art. 2:** personal data - information or a set of information about an individual who is identified or can be specifically identified.

Закон України «Про захист персональних даних», ст. 5: Об'єктами захисту є персональні дані.	**The Law of Ukraine 'On Personal Data Protection', Art. 5:** Subject of protection is personal data.
Закон України «Про захист персональних даних», ст. 8(2): Суб'єкт персональних даних має право: 8. звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду.	**The Law of Ukraine 'On Personal Data Protection', Art. 8(2):** The personal data subject has the right to: 8. to file complaints about the processing of their personal data to the Commissioner or to the court.
Типовий порядок обробки персональних даних, ст. 2.12: Суб'єкт персональних даних має право пред'являти вмотивовану вимогу володільцю персональних даних щодо заборони обробки своїх персональних даних (їх частини) та/або зміни їх складу/змісту. Така вимога розглядається володільцем впродовж 10 днів з моменту отримання.	**'Typical procedure for processing personal data', Art. 2.12:** The personal data subject has the right to make a reasoned request to the owner of personal data to prohibit the processing of his personal data (their part) and / or change their composition / content. Such a request is considered by the owner within 10 days of receipt.
Типовий порядок обробки персональних даних, ст. 2.13: Якщо за результатами розгляду такої вимоги виявлено, що персональні дані суб'єкта (їх частина) обробляються незаконно володілець припиняє обробку персональних даних суб'єкта (їх частини) та інформує про це суб'єкта персональних даних. Якщо за результатами розгляду такої вимоги виявлено, що персональні дані суб'єкта (їх частина) є недостовірними, володілець припиняє обробку персональних даних суб'єкта (чи їх частини) та/або змінює їх склад/зміст та інформує про це суб'єкта персональних даних.	**'Typical procedure for processing personal data', Art. 2.13:** If the results of consideration of such a request reveal that the personal data of the subject (part of them) are processed illegally, the owner terminates the processing of personal data of the subject (part of them) and informs the subject of personal data. If the review of such a requirement reveals that the personal data of the subject (part thereof) is inaccurate, the owner stops processing the personal data of the subject (or part thereof) and / or changes their composition / content and informs the subject of personal data. data.

Типовий порядок обробки персональних даних, ст. 2.15: Суб'єкт персональних даних має право відкликати згоду на обробку персональних даних без зазначення мотивів, у разі якщо єдиною підставою для обробки є згода суб'єкта персональних даних. З моменту відкликання згоди володілець зобов'язаний припинити обробку персональних даних.	**'Typical procedure for processing personal data', Art. 2.15:** The personal data subject has the right to withdraw consent to the processing of personal data without stating the reasons, if the only reason for processing is the consent of the personal data subject. From the moment of withdrawal of consent, the owner is obliged to stop processing personal data.
Рішення Конституційного Суду України від 30 жовтня 2012 року у справі № 18/203-97, параграф 1 резолютивної частини: Забороняється не лише збирання, а й зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини.	Decision of the Constitutional Court of Ukraine of 30 October 2012, case № 18/203-97, § 1 of the resolutive part: Not only the collection of confidential information about a person without his prior consent is prohibited, but also the storage, use and distribution, except in cases defined by law, and only in the interests of national security, economic well-being, human rights and freedoms.
Рішення Конституційного Суду України від 20 січня 2012 року у справі № 1-9/2012, параграф 3.1: Особистим життям фізичної особи є її поведінка у сфері особистісних, сімейних, побутових, інтимних, товариських, професійних, ділових та інших стосунків поза межами суспільної діяльності, яка здійснюється, зокрема, під час виконання особою функцій держави або органів місцевого самоврядування.	Decision of the Constitutional Court of Ukraine of 20 January 2012, case № 1-9/2012, § 3.1: The personal life of an individual is his behavior in the field of personal, family, household, sexual, friendly, professional, business and other relations outside of social activities, which is carried out, in particular, when a person performs the functions of state or local government.

Рішення Конституційного Суду України від 20 січня 2012 року у справі № 1-9/2012, параграф 1 резолютивної частини: Збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди державою, органами місцевого самоврядування, юридичними або фізичними особами є втручанням в її особисте та сімейне життя.	Decision of the Constitutional Court of Ukraine of 20 January 2012, case № 1-9/2012, § 1 of the resolutive part: Collection, storage, use and dissemination of confidential information about a person without his consent by the state, local governments, legal entities or individuals is an interference in his personal and family life.
Рішення Конституційного Суду України від 20 січня 2012 року у справі № 1-9/2012, параграф 3.: Лише фізична особа, якої стосується конфіденційна інформація, відповідно до конституційного та законодавчого регулювання права особи на збирання, зберігання, використання та поширення конфіденційної інформації має право вільно, на власний розсуд визначати порядок ознайомлення з нею інших осіб, держави та органів місцевого самоврядування, а також право на збереження її у таємниці.	**Decision of the Constitutional Court of Ukraine of 20 January 2012, case № 1-9/2012, § 3.:** Only a natural person to whom confidential information relates, in accordance with the constitutional and legislative regulation of the right of a person to collect, store, use and disseminate confidential information has the right to freely, at its discretion determine the procedure for acquaintance with others, the state and local governments. The right to keep it secret.
Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2020 рік: 1.1.1. Право на захист персональних даних. У 2020 році до Уповноваженого надійшло 2 031 повідомлення про порушення прав людини на захист персональних даних, що порівняно з 2019 роком (1061) майже удвічі більше. За результатами аналізу отриманих Уповноваженим повідомлень вбачається,	Yearly report of the Ombudsman (2020): 1.1.1. The right to protection of personal data. In 2020, the Commissioner received 2,031 reports of violations of human rights to personal data protection, which is almost twice as much as in 2019 (1,061). The analysis of the reports received by the Commissioner shows that most of them (almost 1,500) concerned the violation of the human right to non-interference in private and family life during the collection of debts on individuals' financial obligations (collection activities).

що більшість з них (майже 1 500) стосувалися порушення права людини на невтручання в особисте і сімейне життя під час здійснення діяльності зі стягнення заборгованості за грошовими зобов'язаннями фізичних осіб (колекторська діяльність).	
Закон України «Про захист персональних даних» Пункт 10 статті 6: Типовий порядок обробки персональних даних затверджується Уповноваженим.	**Law of Ukraine 'On Personal Data Protection' Article 6, paragraph 9:** The Commissioner shall approve the model rules for personal data processing.
Закон України «Про захист персональних даних» Пункт 3 статті 15: Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку.	**Law of Ukraine 'On Personal Data Protection' Article 15, paragraph 3:** The personal data collected with the violation of the requirements of this Law shall be subject to deletion or destruction as established by law.
Закон України «Про захист персональних даних» Пункт 1 статті 23: Уповноважений має такі повноваження у сфері захисту персональних даних: 1) отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду (...) 6) надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб (...)	**Law of Ukraine 'On Personal Data Protection' Article 23, § 1:** The Commissioner shall have the following authority in the sphere of personal data protection: 1) To receive proposals, claims and other requests of natural and legal persons regarding the protection of personal data and make decisions following their consideration (...) 6) To give recommendations on the practical implementation of the legislation concerning the personal data protection, to explain the rights of obligations of persons concerned following the requests of subjects of personal data, the controllers or processors of personal data, structural divisions or persons responsible for the organization of work on

12) здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних. Пункт 2 статті 24: В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.	the protection of personal data and other persons (...) 12) To monitor the new practices, tendences and technologies concerning the protection of personal data.
Закон України «Про захист персональних даних» Пункт 2 статті 24: В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.	**Law of Ukraine 'On Personal Data Protection' Article 24, paragraph 2:** Within the bodies of public administration and local self-governance as well as within the controllers and processors that perform the processing of personal data which is subject to notification under this Law, a structural division shall be created or a responsible person shall be appointed to be in charge of the organization of work on the protection of personal data with regard to its processing.
Закон України «Про захист персональних даних» Пункт 2 статті 27: Професійні, самоврядні та інші громадські об'єднання чи юридичні особи можуть розробляти кодекси поведінки з метою забезпечення ефективного захисту прав суб'єктів персональних даних, додержання законодавства про захист персональних даних з урахуванням специфіки обробки персональних даних у різних сферах. При розробленні такого кодексу поведінки або внесенні змін до нього відповідне об'єднання чи юридична особа може	**Law of Ukraine 'On Personal Data Protection' Article 27, paragraph 2:** The professional, self-governing and other public associations or legal persons may draft the codes of behavior for the purpose of securing the effective protection of the rights of subjects of personal data, nd of the compliance with personal data protection legislation, taking into account the specifics of processing of personal data in various spheres. During the drafting of such code of behavior or amending it, an association or a legal

звернутися за висновком до Уповноваженого.	person concerned may address the Commissioner for the report.
Наказ Уповноваженого Верховної Ради України з прав людини № 1/02-14: Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації: Пункт 1.2 статті 1: Для цілей цього Порядку обробка персональних даних, що становить особливий ризик для прав і свобод суб'єктів - це будь-яка дія або сукупність дій, а саме збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення, у тому числі з використанням інформаційних (автоматизованих) систем, яка здійснюється відносно персональних даних про: - расове, етнічне та національне походження; - політичні, релігійні або світоглядні переконання; - членство в політичних партіях та/або організаціях, професійних спілках,	**Decree of the Ukrainian Parliament Commissioner for Human Rights № 1/02-14:** Procedure for the Notification of the Parliamentary Commissioner of Ukraine on the Processing of Personal Data Constituting a Particular Risk for the Rights and Liberties of Subjects of Personal Data on the Structural Department or the Responsible Person in Charge of the Organization of Work on the Protection of Personal Data with Regard to Its Processing and the Disclosure of Such Information): Article 1, paragraph 1.2: For the purpose of the present Rules the processing of personal data constituting a particular risk for the rights and duties of subjects shall mean an action or a complex of actions, namely the collection, accumulation, storage, adaptation, change, renewing, usage and spread (dissemination, realization, transmission) depersonalization, destruction (including that involving the usage of informational (automatized) systems carried out with regard to the information concerning: racial, ethnic and national origin political, religious or worldview sympathies membership in political parties and/or organizations, trade unions, religious associations or public organizations of the worldview orientation health condition sexual life

релігійних організаціях чи в громадських організаціях світоглядної спрямованості; - стан здоров'я; - статеве життя; - біометричні дані; - генетичні дані; - притягнення до адміністративної чи кримінальної відповідальності; - застосування щодо особи заходів в рамках досудового розслідування; - вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»; - вчинення щодо особи тих чи інших видів насильства; - місцеперебування та/або шляхи пересування особи.	biometric data genetic data criminal or administrative liability enforcement of special measures at the stage of pre-trial investigation enforcement of measures provided by the Law 'On the Operative and Investigative Activities' commisson of the acts of violence against a person location and/or ways of movement of a person

Bibliography

English titles

Legislation

Constitution of Ukraine 1996
https://zakon.rada.gov.ua/laws/show/254к/96-вр/ed20200101

The Civil Code of Ukraine 2003 № 435-IX
<https://zakon.rada.gov.ua/laws/show/435-15#Text>

The Civil Procedure Code of Ukraine 2004 №1618-IV
<https://zakon.rada.gov.ua/laws/show/1618-15#Text>

The Criminal Code of Ukraine 2001 №2341-III
<https://zakon.rada.gov.ua/laws/show/2341-14#Text>

The Code of Criminal Procedure of Ukraine 2012 №4651-VI
<https://zakon.rada.gov.ua/laws/show/4651-17#n431>

The Code of Ukraine on Administrative Offenses №80731-X
<https://zakon.rada.gov.ua/laws/show/80732-10#Text>

The Family Code of Ukraine 2002 № 2947-III
<https://zakon.rada.gov.ua/laws/show/2947-14#n11>

The Law of Ukraine 'On Personal Data Protection' 2010 № 2297-VI
<https://zakon.rada.gov.ua/laws/show/2297-17>

The Law of Ukraine 'On Electronic Commerce' 2015 №675-VII,
<https://zakon.rada.gov.ua/laws/show/675-19>

The Law of Ukraine 'On Electronic Trust Services' 2017 2155-VIII
<https://zakon.rada.gov.ua/laws/show/2155-19?lang=uk#Text>

The Law of Ukraine 'On Electronic Documents and Electronic Document flow' 2003 №851-IV <https://zakon.rada.gov.ua/laws/show/851-15>

The Law of Ukraine 'On information protection in information and telecommunication systems' 1994 №80/94-BP
<https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>

The Law of Ukraine 'On Sanctions' 2014 №1644-VII <
https://zakon.rada.gov.ua/laws/show/1644-18#Text >

The Law of Ukraine 'On Information' 1992 № 2657-XII
<https://zakon.rada.gov.ua/laws/show/2657-12#Text>

The Law of Ukraine 'On Principles of Preventing and Combating Discrimination in Ukraine' 2012 № 5207-VI <https://zakon.rada.gov.ua/laws/show/5207-17>

The Law of Ukraine 'On the basic principles of cybersecurity in Ukraine' 2017 №2163-VIII <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

The Law of Ukraine 'On operational and investigative activities' 1992 №2135-XII <https://zakon.rada.gov.ua/laws/show/2135-12#Text>

The Law of Ukraine 'On the implementation of decisions and application of the case law of the European Court of Human Rights: Law of Ukraine' 2012 №3477-IV <https://zakon.rada.gov.ua/laws/show/3477-15#Text>

The Law of Ukraine 'On Copyright and Related Rights' 1993 № 3792-XII p. 11, art. 52-1 <https://zakon.rada.gov.ua/laws/show/3792-12#52-1>

The Law of Ukraine 'On freedom of conscience and religious organizations' 1991 № 987-XII, <https://zakon.rada.gov.ua/laws/show/987-12#Text>

The Law of Ukraine 'On notary' 1993 № 3425-XII, <https://zakon.rada.gov.ua/laws/show/3425-12#n66>

The Law of Ukraine 'On Bar' 2013 № 5076-VI, <https://zakon.rada.gov.ua/laws/show/5076-17#n173>

The Law of Ukraine 'On banks and banking' 2001 № 2121-III, <https://zakon.rada.gov.ua/laws/show/2121-14#n983>

The International Covenant on Civil and Political Rights 1966 <http://www.un.org.ua/images/International_Covenant_on_Civil_and_Political_Rights_CCPR_eng1.pdf>

Convention for the Protection of Human Rights and Fundamental Freedoms 1950 <https://zakon.rada.gov.ua/laws/show/995_004#Text>

The Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part: <https://zakon.rada.gov.ua/laws/show/984_011#Text>

Letter of explanation of the Ukrainian Parliament Commissioner for Human Rights for Human Rights as of 3 March 2014 № 2/9-227067.14-1/НД-129 <https://zakon.rada.gov.ua/laws/show/v7067715-14#Text>

Order of the Ministry Justice of Ukraine 'On approval of Methodical recommendations on identification of cases of gender discrimination and the mechanism of rendering legal aid' 2019 v0033419-19 <https://zakon.rada.gov.ua/rada/show/v0033419-19?lang=uk#Text>

Order of the Cabinet of Ministers of Ukraine 'Concept on the development of artificial intelligence in Ukraine' 2020 № 1556-p, <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>

Order of the Prosecutor General's Office of Ukraine, Ministry of Internal Affairs of Ukraine, Security Service of Ukraine, Administration of the state border service of Ukraine, Ministry of Finance of Ukraine, Ministry of Justice of Ukraine 'Instruction on Covert Investigative (Search) Actions' 2012 № 114/1042/516/1199/936/1687/5 <https://zakon.rada.gov.ua/laws/show/v0114900-12>

Decree of the President of Ukraine 'On the regulations on procedure of cryptographic information protection in Ukraine' 1998 № №505/98 <https://zakon.rada.gov.ua/laws/show/505/98#Text>

Decree of the Cabinet of Ministers of Ukraine 'On approving the concept on e-government development in Ukraine' 2017 № 649-2017-p <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text>

Decree of the Cabinet of Ministers of Ukraine 'On approving the strategy for the development of the information society in Ukraine' 2013 № 386-2013-p <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text>

Decree of the President of Ukraine 'On the decision of the National Security and Defence Council of Ukraine of 28 April 2017 'On the application of personal special economic and other restrictive measures (sanctions)' 15 May 2017 №133/2017 <https://www.president.gov.ua/documents/1332017-21850>

Decree of the President of Ukraine 'On the decision of the National Security and Defense Council of Ukraine of 2 March 2021 'On the application, abolition and amendment of personal special economic and other restrictive measures (sanctions)' 23 March 2021 №109/2021 <https://www.president.gov.ua/documents/1092021-37481>

Decree of the Ukrainian Parliament Commissioner for Human Rights 'On approval of documents in the field of personal data protection' 08.01.2014 № 1/02-14 <https://zakon.rada.gov.ua/go/v1_02715-14>

Procedure for the Ukrainian Parliament Commissioner for Human Rights to monitor compliance with the legislation on personal data protection as of 8 January 2014 № 1/02-14. <https://zakon.rada.gov.ua/laws/show/v1_02715-14#n92>

Draft Law 'On the cryptocurrency in Ukraine' 2017 № 7183 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684>

White Paper. On Artificial Intelligence - A European Approach to Excellence and Trust. COM (2020) 65 Final

<https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf>

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 <http://data.europa.eu/eli/reg/2019/881/oj>

Decision of the National Security and Defense Council of Ukraine 'On the application of personal special economic and other restrictive measures (sanctions)' as of 29 January 2021 <https://zakon.rada.gov.ua/laws/show/n0003525-21#Text>

Ministry of Justice of Ukraine in Letter №5543-0-33-13 / 6.1 dated 26.04.2013 <https://zakon.rada.gov.ua/laws/show/v5543323-13#Text>

Decision of the National Security and Defence Council of Ukraine 'About application of personal special economic and other restrictive measures (sanctions)' 28 April 2017 <https://zakon.rada.gov.ua/laws/show/n0004525-17#n2>

Reports

Romanyuk I.I., 'Protection of the right to personal data in Ukraine (civil law aspect)' (Kyiv, 2015)

Law of Ukraine 'On access to public information' Scientific and practical commentary Kyiv, 2012

Zakharov E. Yu., 'Violation of freedom of expression during the 2006 election campaign 2006'(Kharkiv Human Rights Group, 7 March 2006) <http: //www.khpg.org/index.php? Id = 1141752068>

Sayenko Kharenko, 'Analysis of Data Privacy Laws and Legislation in Ukraine' Final Report (the 'Memorandum')' (Sayenko Kharenko, 14 September 2020) p. 47 <https://ecpl.com.ua/wp-content/uploads/2020/09/ENG_09142020-_CEP_Final-Report.pdf>

Tatiana Gordienko, 'GDPR in Ukraine: who is covered by the new regulations?' (Detector Media, 4 February 2019) <https://detector.media/infospace/article/144571/2019-02-04-gdpr-v-ukraini-khto-pidpadaie-pid-diyu-norm-novogo-reglamentu/>

Lida Klymkiv, 'GDPR — how it affects Ukrainian companies' (Dead Lawyers Society, 15 March 2018) <https://medium.com/dead-lawyers-society/gdpr-how-it-affects-ukrainian-companies-ce9ed3d0dc8>

'Data Protection Day: Does Data Protection in Ukraine Meet International Standards?' (Council of Europe, 27 January 2021) <https://www.coe.int/en/web/kyiv/-/data-protection-day-does-the-personal-data-protection-in-ukraine-meet-international-standards->

Iryna Fedorovych, 'Anti-discrimination legislation in Ukraine - box ticking for the EU or real reforms to ensure equality for Ukraine's citizens?'

Freedom of the Net, 2019 Report on Ukraine, <https://freedomhouse.org/country/ukraine/freedom-net/2019>

Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2016 (Secretariat of the Commissioner, 2017) <https://ombudsman.gov.ua/files/Dopovidi/Dopovid_2016_final.pdf>

Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2017 (Secretariat of the Commissioner, 2018) <http://www.ombudsman.gov.ua/files/Dopovidi/Report-2018-1.pdf>

Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in 2019 (Secretariat of the Commissioner, 2020) <http://www.ombudsman.gov.ua/files/Dopovidi/zvit%20za%202019.pdf>

Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2020 (Secretariat of the Commissioner, 2021) <https://www.ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf>

'How Ukraine Punishes Illegal Information on the Internet' <https://www.ppl.org.ua/yak-ukra%D1%97na-karaye-za-nezakonnu-informaciyu-v-interneti.html>

Vsevolod Nekrasov, 'State registers have leaked: who is 'merging' the personal data of Ukrainians and what to do about it' (Economic truth, 13 May 2020) <https://www.epravda.com.ua/publications/2020/05/13/660405/>

Adrian Shahbaz, Allie Funk, 'Freedom House official website link: Pandemics digital shadow, article' (Freedom House) <https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow#footnote12_9h7bed5>

Freedom of speech vs. information security? Key quotes from UkraineWorld's event at Kyiv Security Forum 2019' (Ukraine world,18 April 2019) < https://ukraineworld.org/articles/infowatch/freedom-speech-vs-information-security-key-quotes-ukraineworlds-event-kyiv-security-forum-2019>

'International Report on Internet Censorship. Final Report of the International Legal Research Group on Internet Censorship (eds)' (ELSA International, 2020) <https://files.elsa.org/AA/LRG_Internet_Censorship/Final_Report.pdf>, pp. 1195-1198

Books

M. V. Bem, I. M. Gorodisky, G. Sutton, O. M. Rodionenko, 'Personal data protection: Legal regulation and practical aspects: scientific and practical manual'

D. B. Sergeeva, 'Withdrawal of information from transport telecommunications networks: problematic issues of legal regulation' (Arsis LTD, 2009)

E. F. Iskenderov, 'Withdrawal of information from transport telecommunications networks as a means of obtaining evidence by operational units' (Bulletin of Criminal Procedure, 2016) <http://vkslaw.knu.ua/images/verstka/4_2016_Iskenderov.pdf>

N. O. Goldberg, 'Withdrawal of information from transport telecommunications networks: problems of criminal procedure regulation' (Bulletin of the AMSU, 2015)

Lance J. Hoffman, Karen A. Metivier Carreiro, 'Computer Technology to Balance Accountability and Anonymity in Self-regulatory Privacy Regimes' <https://www.ntia.doc.gov/page/chapter-5-technology-and-privacy-policy>

Z. Udovenko 'Problems of security and protection of private households before the hour of knowledge of information from transport telecommunications' ('Scientific notes of NaUKMA. Legal sciences', 2019.) p. 123.

Digital resources

Complete guide to GDPR compliance <https://gdpr.eu>

Recommendation No. 32, adopted by seventh session of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) (1st edn, ECE/TRADE/277, 2001) <https://unece.org/fileadmin/DAM/cefact/recommendations/rec32/rec32_ecetrd277.pdf >

'New data protection legislation of Ukraine is being developed with the expert support of the Council of Europe' (Council of Europe, 30 January 2020)

<https://www.coe.int/en/web/national-implementation/-/new-data-protection-legislation-of-ukraine-is-being-developed-with-the-expert-support-of-the-council-of-europe>

Glossary of summaries (Eur-Lex)
<https://eur-lex.europa.eu/summary/glossary/subsidiarity.html>

Monitoring the improvement of legislation on personal data protection in order to bring it in line with Regulation (EU) 2016/679 (European integration portal)
<http://pulse.eu-ua.org/ua/streams/human-rights-justice-and-anticorupption/2020-substream5-95>

All-Ukrainian Association of Centers for Administrative Services, 'Code of Conduct for Processing and Protection of Personal Data in Centers for Administrative Services' (All-Ukrainian Association of Administrative Service Centers, 2020)
<https://drive.google.com/file/d/1J3HEaBbgwvqv9rVUtk41vI7El1wtTB-2/view?fbclid=IwAR2D-fr-kypIcdba-gOGtcJe3mt_RhXPs7TUst0ClAyZCvveLqakLCiF33M>

Kyivstar privacy policy. 'STAR GUARD family' services (Kyivstar, 29 May 2019)
<https://cdn.kyivstar.ua/sites/default/files/about/privacy_policy_star_guard_family_eng.pdf>

Diia.Business, Data protection self-assessment tool (Diia.Business)
<https://business.diia.gov.ua/en/selftesting/data-protection-tool>

Artem Kobrin, Dmytro Korchynskyi, Vladislav Nekrutenko, 'Ukrainian GDPR: The reality and future of privacy legislation in Ukraine' (IAPP, 28 September 2020)
<https://iapp.org/news/a/ukrainian-gdpr-the-reality-and-future-of-privacy-legislation-in-ukraine/>

The Ukrainian Parliament Commissioner for Human Rights, 'Control over compliance with the requirements of the legislation on personal data protection'
<https://ombudsman.gov.ua/ua/page/zpd/kontrol/>

The Ukrainian Parliament Commissioner for Human Rights, 'Information about the Department for Personal Data Protection'
<https://ombudsman.gov.ua/ua/page/zpd/info/>

O. O. Tikhomirov and others, 'Law, society, state, security: information dimension'
<http://zpd.inf.ua/page19.html#top>

Alina Pravdychenko, "Personal data online: regulation problems and protection prospects" (Center of democracy and the rule of law, 21 November 2019)
<https://cedem.org.ua/articles/personalni-dani-onlajn/>

Big Data Decisions <https://bit.ly/2ZClVCD>

Big Data for Business from Vodafone
<https://business.vodafone.ua/produkty/big-data?utm_source=Search&utm_medium=CPC&utm_campaign=Vodafone_Analytics_Search_BRD&utm_term=vodafone%20big%20data&gclid=CjwKCAjwhMmEBhBwEiwAXwFoEb9D7XwnVipjdyCOGimKeImFcmCj4a6Y8SpRkz-xab0AHuhjf1cjwhoCnUAQAvD_BwE>

'Cyberpolice exposes office for sale of personal databases'
<https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-ofis-z-prodazhu-baz-personalnyx-danyx-1858/>

Dmytro Weber, 'In the center of Sumy, a tax officer was caught selling personal data' (Segodnya, 31 September 2017)
<https://criminal.segodnya.ua/criminal/v-centre-sum-poymali-nalogovika-torgovavshego-personalnymi-dannymi--1051731.html>

How did the data of private clients of PrivatBank end up in Moscow? (Zakon i Business, 7 December 2017)
<https://zib.com.ua/ru/print/131103-kak_dannie_chastnih_klientov_privatbanka_okazalis_v_moskve.html>

In 'dark Internet' the customer base of 'Nova poshta' sells (Economic truth, 6 February 2018) <https://www.epravda.com.ua/rus/news/2018/02/6/633794/>

'It became known what messengers Ukrainians use'
<https://www.epravda.com.ua/news/2018/03/22/635239/>

Kharkiv citizen who illegally sold customs databases sentenced to fine and special confiscation (Interfaks-Ukraine, 21 March 2019)
<https://interfax.com.ua/news/general/574332.html>

Megogo User Agreement <https://megogo.net/ru/rules>

Nina Glushchenko, 'Who pays for legal video and how: statistics from Megogo' (Ain, 24 November 2016)
<https://ain.ua/2016/11/24/kto-i-kak-platit-za-legalnoe-video-megogo-oct-2016/>

Privat Bank Terms and Conditions for the provision of banking
<https://privatbank.ua/ru/terms>

Strong Talent Base
<https://2019.stateofeuropeantech.com/chapter/people/article/strong-talent-base/>

The Code of Good Practice for Personal Data Processing of 'Kyivstar'
<https://bit.ly/3kinkrG>

The National Bank and the Commissioner for Human Rights of the Verkhovna Rada of Ukraine will work together to protect the personal data of Ukrainians <https://bank.gov.ua/ua/news/all/natsionalniy-bank-ta-upovnovajeniy-verhovnoyi-radi-ukrayini-z-prav-lyudini-spilno-pratsyuvatimut-nad-zahistom-personalnih-danih-ukrayintsiv>

'The IT industry forms 4% of GDP' <https://www.epravda.com.ua/news/2019/02/13/645229/>

The Ukrainian mobile operator has launched the Internet of Things into commercial operation (Economic truth, 21 January 2020) <https://www.epravda.com.ua/news/2020/01/21/656038/>

The State Statistics Service of Ukraine, 'Express Issue' (The State Statistics Service of Ukraine, 13 November 2020) <https://ukrstat.org/uk/express/expr2020/11/136.doc>

Vodafone Terms of use <https://www.vodafone.ua/terms-of-use>

7 most prominent tech companies born in Ukraine (Silicon Canals, 18 June 2020) <https://siliconcanals.com/news/most-prominent-tech-companies-born-in-ukraine/>

'Maya Yarovaya, 'New "spill" of SoftServe data: client projects and, probably, employee data' (Ain, 16 September 2020) <https://ain.ua/2020/09/16/softserve-utechka-2/>

'Cisomag, 'NSDC Acknowledges Data Leak in Ukrainian Government Job Portal' (Cisomag, 20 January 2020) <https://cisomag.eccouncil.org/nsdc-acknowledges-data-leak-in-ukrainian-government-job-portal/>

Volodimir Kondrashov, 'Battle on two fronts. Great interview with the founders of the Ukrainian Cyber Alliance' (New Time Business, 3 March 2020) <https://biz.nv.ua/ukr/tech/zasnovniki-ukrajinskogo-kiberalyansu-mi-ne-nouneymi-yakis-neisnuyuchi-obrazi-chi-agenti-sbu-50073238.html>

National Police of Ukraine, A group of people led by a former National Police official was detained in Kyiv for unauthorized use of official information, Official Website of the National Police (Official website of the National Police, 20 February 2019) <https://www.npu.gov.ua/news/korupcziya/u-kijevi-za-nesankczionovane-vikoristannya-sluzhbovoji-informacziji-zatrimano-grupu-osib-na-choli-z-kolishnim-posadovczem-naczpolicziji/>

Alec Luhn, 'Ukraine blocks popular social networks as part of sanctions on Russia' (16 May 2017) <https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war>

Sources and data on digital participation in Ukraine (DW Akademie, 1 July 2019) <https://www.dw.com/en/sources-and-data-on-digital-participation-in-ukraine/a-49430929>

National Cyber Security Coordination Center, 'The application for bypassing Vkontakte locks stole personal data' (National Cyber Security Coordination Center of Ukraine official Facebook page, 5 February 2021) <https://www.facebook.com/ncsccUA/posts/227197159022642>

Overview of the case law of the Supreme Court of Ukraine on the inadmissibility of evidence obtained as a result of a significant violation of human rights and freedoms <https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Ogljad_KKS_VS.pdf>

Case-law

The Resolution of the Constitutional Court of Ukraine 2012 №2-рп/2012 <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>

Zaichenko v Ukraine App no 45797/09 (ECtHR, 6 July 2015) <http://hudoc.echr.coe.int/rus?i=001-152598>Surikov V. Ukraine, application no. 42788/06 <http://hudoc.echr.coe.int/eng?i=001-170462>

Surikov v Ukraine App no 42788/06 (ECtHR, 26 April 2017) <https://jurisprudencia.mpd.gov.ar/Jurisprudencia/Surikov%20vs%20Ukraine.pdf>

Case № 275/944/18 (13 February 2019) <https://reyestr.court.gov.ua/Review/80251940>

Announcement on the website of the National Commission for State Regulation of Communications and Informatization * in the register of court decisions there is no text of the decision of 23.07.2019, which was made by Judge Vovk SV in the case № 757/38387/19-k criminal proceedings № 12018060020001159 <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1749&language=uk>

Case № 127/13877/19 (24 June 2020) (Vinnytsia Court of Appeal) <https://reyestr.court.gov.ua/Review/90109587> accessed 01 June 2021

Case №806/3265/17 (26 March 2018) (Grand Chamber of the Supreme Court) <https://supreme.court.gov.ua/supreme/inshe/zrazkovi_spravu/zr_rish_806_3265_17>

Case № 757/38387/19-k (23 July 2019) <https://zakononline.com.ua/court-decisions/show/83898765>

Case № 308/1221/17 (10 February 2017) (Uzhhorod City District Court) <https://reyestr.court.gov.ua/Review/64585422>

Case № 591/442/16-к (4 March 2016) (Zarichny District Court of Sumy) <https://reyestr.court.gov.ua/Review/55398181> accessed 01 June 2021>

Case №369/1469/19 (19 September 2019) <http://www.reyestr.court.gov.ua/Review/79701294>

Case № 910/16699/19 (4 August 2020) (Economic Court of Kyiv) <https://reyestr.court.gov.ua/Review/89739526>

Case № 757/38387/ 19к (18 February 2020) (Kyiv Court of Appeal) <https://reyestr.court.gov.ua/Review/87671973> accessed 01 June 2021>

The Resolution of the Constitutional Court of Ukraine 1997 №5-зп <https://zakon.rada.gov.ua/laws/show/v005p710-97#Text>

Ukrainian titles

Legislation

Конституція України: Конституція України 1996 <https://zakon.rada.gov.ua/laws/show/254к/96-вр/ed20200101>

Кримінальний кодекс України 2001 №2341-III <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

Кримінальний процесуальний кодекс України 2012 № 4651-VI <https://zakon.rada.gov.ua/laws/show/4651-17#Text>

Кодекс України про адміністративні правопорушення 1984 №80731-X <https://zakon.rada.gov.ua/laws/show/80732-10#Text>

Цивільний Кодекс України 2003 № 435-IX <https://zakon.rada.gov.ua/laws/show/435-15#Text>

Сімейний Кодекс України 2002 № 2947-III <https://zakon.rada.gov.ua/laws/show/2947-14#n11>

Закон України «Про захист персональних даних» 2010 2297-VI <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

Закон України «Про оперативно-розшукову діяльність» від 18.02.1992. № 2135-XII із змін. <https://zakon.rada.gov.ua/laws/show/2135-12#Text>

Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затверджена Наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України,

Міністерства фінансів України, Міністерства юстиції України 2012 <https://zakon.rada.gov.ua/laws/show/v0114900-12#Text>

Закон України «Про захист персональних даних» 2010 № 2297-VI <https://zakon.rada.gov.ua/laws/show/2297-17#n12>

Закон України "Про виконання рішень та застосування практики Європейського суду з прав людини" 2012 №3477-IV <https://zakon.rada.gov.ua/laws/show/3477-15#Text>

Указ Президента України "Про рішення Ради національної безпеки і оборони України від 29 січня 2021 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)"" 2021 №36/2021 <https://zakon.rada.gov.ua/laws/show/36/2021#n2>

Закон України "Про авторське право і суміжні прав" 1994 3792-XII <https://zakon.rada.gov.ua/laws/show/3792-12>

Закон України "Про захист персональних даних" 2010 №2297-VI <https://zakon.rada.gov.ua/laws/show/2297-17>

Закон України "Про свободу совісті та релігійні організації" 1991 № 987-XII <https://zakon.rada.gov.ua/laws/show/987-12#Text>

Закон України "Про нотаріат" 1993 № 3425-XII <https://zakon.rada.gov.ua/laws/show/3425-12#n66>

Закон України "Про адвокатуру та адвокатську діяльність" 2013 № 5076-VI <https://zakon.rada.gov.ua/laws/show/5076-17#n173>

Закон України "Про банки та банківську діяльність" 2001 № 2121-III <https://zakon.rada.gov.ua/laws/show/2121-14#n983>

Закон України "Про інформацію" 1992 № 2657-XII <https://zakon.rada.gov.ua/laws/show/2657-12#n84>

Типовий порядок обробки персональних даних затверджений Наказом Уповноваженого Верховної Ради України з прав людини 2014 № 1/02-14 <https://zakon.rada.gov.ua/laws/show/v1_02715-14#n11>

Рішення Ради Національної безпеки і оборони України "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)" 2021 №n0003525-21 <https://zakon.rada.gov.ua/laws/show/n0003525-21#Text>

Наказ Уповноваженого Верховної Ради України з прав людини 2014 № 1/02-14 <https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text>

Лист Уповноваженого Верховної ради України з прав людини від 03.03.2014 № 2/9-227067.14-1/НД-129.

<https://zakon.rada.gov.ua/laws/show/v7067715-14#Text>

Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних від 8 січня 2014 № 1/02-14. <https://zakon.rada.gov.ua/laws/show/v1_02715-14#n92>

Міністерство юстиції України у листі №5543-0-33-13 (26 квітня 2013) <https://zakon.rada.gov.ua/laws/show/v5543323-13#Text>

Reports

Щорічна доповідь Уповноваженого Верховної Ради з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2016 (Секретаріат Уповноваженого, 2017) <https://ombudsman.gov.ua/files/Dopovidi/Dopovid_2017.pdf >

Щорічна доповідь Уповноваженого Верховної Ради з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2017 (Секретаріат Уповноваженого, 2018) <http://www.ombudsman.gov.ua/files/Dopovidi/Report-2018-1.pdf>

Щорічна доповідь Уповноваженого Верховної Ради з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2019 (Секретаріат Уповноваженого, 2020) <http://www.ombudsman.gov.ua/files/Dopovidi/zvit%20za%202019.pdf>

Щорічна доповідь Уповноваженого Верховної Ради з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2020 (Секретаріат Уповноваженого, 2021) <https://dpsu.gov.ua/upload/file/zvit_2020_rik.pdf>

М.Мирний "Як Україна карає за незаконну інформацію в інтернеті": аналітичний звіт "Свобода слова в інтернеті" (Платформа прав людини) <https://www.ppl.org.ua/yak-ukra%D1%97na-karaye-za-nezakonnu-informaciyu-v-internеti.html>

Некрасов В. Просочились державні реєстри: хто «зливає» персональні дані українців і що з ними робити (Українська правда, 2020) <https://www.epravda.com.ua/publications/2020/05/13/660405/>

Адріан Шахбаз, Еллі Функ. Свобода в мережі 2020: Цифрова тінь пандемії (Freedom House)

<https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow#footnote12_9h7bed5>

Свобода слова проти інформаційної безпеки? Ключові цитати з події UkraineWorld на Київському форумі безпеки 2019 '(15 квітня 2019 р.), від 24 лютого 2020 року

Books

М. В. Бем, І. М. Городиський, Г. Саттон, О. М. Родіоненко "Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник"

Д. Б. Сергєєва "Зняття інформації з транспортних телекомунікаційних мереж: проблемні питання правового регулювання" (Х.: Арсіс ЛТД, 2009)

Е. Ф. Іскендеров "Зняття інформації з транспортних телекомунікаційних мереж як засіб отримання доказів оперативними підрозділами" (Ж: Вісник кримінального судочинства №4, 2016) <http://vkslaw.knu.ua/images/verstka/4_2016_Iskenderov.pdf>

Н. О. Гольдберг Зняття інформації з транспортних телекомунікаційних мереж: проблеми кримінально-процесуальної регламентації (Вісник АМСУ. Серія: «Право», № 2 (15), 2015)

Е. Ф. Іскендеров Зняття оперативними підрозділами інформації з транспортних телекомунікаційних мереж: проблемні питання (Актуальні проблеми правоохоронної діяльності, 2016)

Ленс Дж. Гофман, Карен А. Метьє Кар'єро. Комп'ютерні технології для збалансування підзвітності та анонімності в режимах саморегулювання конфіденційності (Інститут політики кіберпростору, Школа технологій та прикладних наук, Університет Джорджа Вашингтона, Вашингтон, округ Колумбія, 20052) <https://www.ntia.doc.gov/page/chapter-5-technology-and-privacy-policy>

Digital resources

Інформація про Департамент у сфері захисту персональних даних. <https://ombudsman.gov.ua/ua/page/zpd/info/>

О. О. Тихомиров та інші, "Право, суспільство, держава, безпека: інформаційний вимір" <http://zpd.inf.ua/page19.html#top>

Аліна Правдиченко, "Персональні дані онлайн: проблеми регулювання та перспективи захисту" <https://cedem.org.ua/articles/personalni-dani-onlajn/>

Big Data Решения <https://bit.ly/2ZClVCD>

Big Data для бізнесу від Vodafone
<https://business.vodafone.ua/produkty/big-data?utm_source=Search&utm_medium=CPC&utm_campaign=Vodafone_Analytics_Search_BRD&utm_term=vodafone%20big%20data&gclid=CjwKCAjwhMmEBhBwEiwAXwFoEb9D7XwnVipjdyCOGimKeImFcmCj4a6Y8SpRkz-xab0AHuhjf1cjwhoCnUAQAvD_BwE>

Megogo Пользовательское соглашение <https://megogo.net/ru/rules>

Дмитро Вебер, «В центре Сум поймали налоговика, торговавшего персональными данными» (Сегодня, 31 серпня 2017)
<https://criminal.segodnya.ua/criminal/v-centre-sum-poymali-nalogovika-torgovavshego-personalnymi-dannymi--1051731.html>

Державна служба статистики України, «Експрес-випуск» (Державна служба статистики України, 13 листопада 2020)
<https://ukrstat.org/uk/express/expr2020/11/136.doc>

"IT-індустрія формує 4% ВВП — Кубів" (Економічна правда, 13 лютого 2019)
<https://www.epravda.com.ua/news/2019/02/13/645229/>

"Как данные частных клиентов ПриватБанка оказались в Москве?" (Закон и Бизнес, 7 грудня 2017)
<https://zib.com.ua/ru/print/131103-kak_dannie_chastnih_klientov_privatbanka_okazalis_v_moskve.html>

Кодекс поведінки при роботі з персональними даними у ПрАТ «Київстар»
<https://bit.ly/3kinkrG>

"Кіберполіція викрила офіс з продажу баз персональних даних" (Кіберполіція Національна поліція України, 5 квітня 2018)
<https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-ofis-z-prodazhu-baz-personalnyx-danyx-1858/>

Нина Глущенко, «Кто и как платит за легальное видео: статистика от Megogo» (Ain, 24 ноября 2016)
<https://ain.ua/2016/11/24/kto-i-kak-platit-za-legalnoe-video-megogo-oct-2016/>

"Національний банк та Уповноважений Верховної Ради України з прав людини спільно працюватимуть над захистом персональних даних українців
<https://bank.gov.ua/ua/news/all/natsionalniy-bank-ta-upovnovajeniy-verhovnoyi-radi-ukrayini-z-prav-lyudini-spilno-pratsyuvatimut-nad-zahistom-personalnih-danih-ukrayintsiv>

"Незаконно продававший таможенные базы данных харьковчанин приговорен к штрафу и спецконфискации" (Интерфакс-Украина, 21 березня 2019)
<https://interfax.com.ua/news/general/574332.html>

"Стало відомо, якими месенджерами користуються українці" (Економічна правда, 22 березня 2018) <https://www.epravda.com.ua/news/2018/03/22/635239/>

Умови користування Vodafone <https://www.vodafone.ua/terms-of-use>

Условия и правила предоставления банковских услуг Приват Банк <https://privatbank.ua/ru/terms>

"Український мобільний оператор запустив в комерційну експлуатацію інтернет речей" (Економічна правда, 21 січня 2020) <https://www.epravda.com.ua/news/2020/01/21/656038/>

"У «темному інтернеті» продають базу клієнтів «Нової пошти» - ЗМІ (Економічна правда, 6 лютого 2018)" <https://www.epravda.com.ua/rus/news/2018/02/6/633794/>

"У Дніпрі блокували продаж бази персональних даних виборців – СБУ (Media Sapiens, 24 жовтня 2020)" <https://ms.detector.media/kiberbezpeka/post/25811/2020-10-24-u-dnipri-blokuvaly-prodazh-bazy-personalnykh-danykh-vybortsiv-sbu/>

Case-law

Справа № 275/944/18 (13 лютого 2019) <https://reyestr.court.gov.ua/Review/80251940>

Оголошення на веб-сайті Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації *в реєстрі судових рішень відсутній текст ухвали від 23.07.2019, який був винесений суддею Вовк С.В. по справі № 757/38387/19-к кримінальне провадження № 12018060020001159 <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1749&language=uk>

Справа № 127/13877/19 (24 червня 2020), <https://reyestr.court.gov.ua/Review/90109587>

Справа №806/3265/17 (Велика палата, справа Верховного Суду, 26 березня 2018) <https://supreme.court.gov.ua/supreme/inshe/zrazkovi_spravu/zr_rish_806_3265_17>

Справа № 757/38387/19-к (дата набрання законної сили 23.07.2019) <https://zakononline.com.ua/court-decisions/show/83898765>

Справа № 308/1221/17 (10 лютого 2017 року) <https://reyestr.court.gov.ua/Review/64585422>

Рішення Конституційного Суду України від 28 січня 2012 року, справа № 1-9/2012 <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>

Рішення Конституційного Суду України від 30 жовтня 2012, справа № 18/203-97 <https://zakon.rada.gov.ua/laws/show/v005p710-97#Text>

ELSA LEGAL RESEARCH GROUPS

The European Law Students' Association