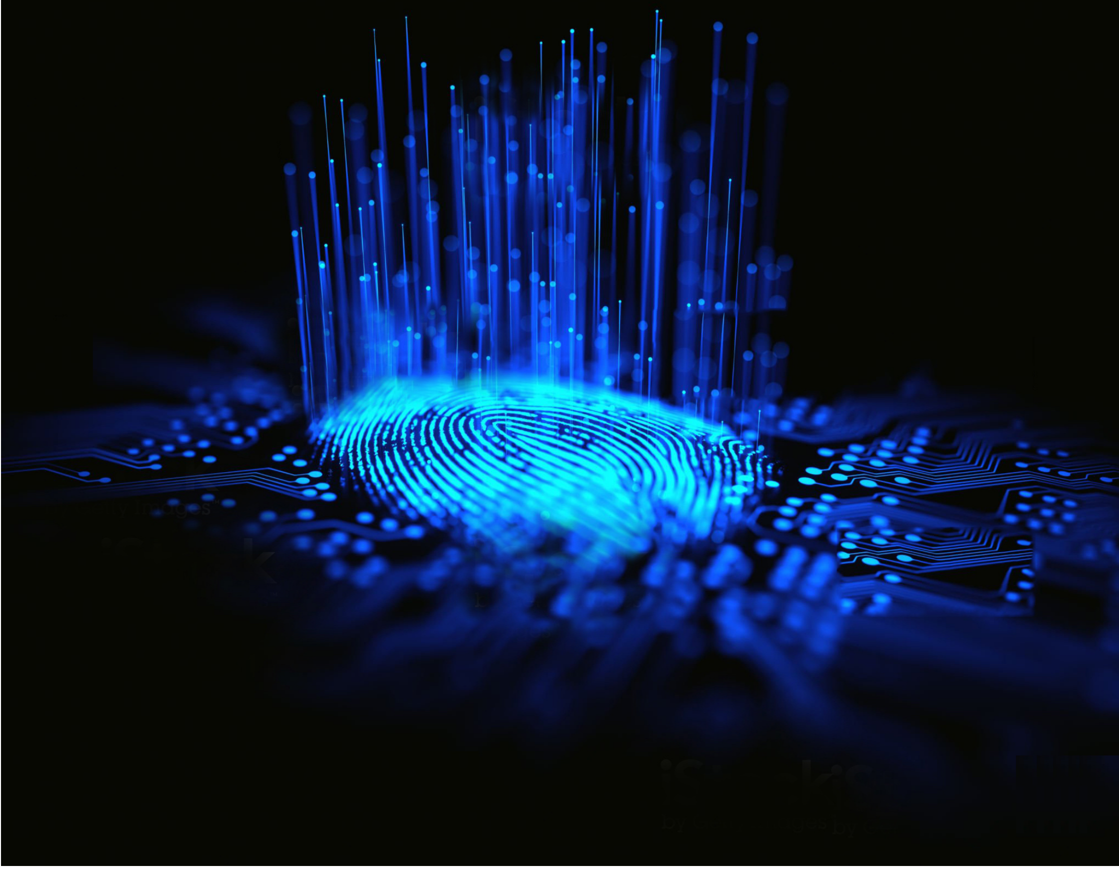
CHALLENGES AND OPPORTUNITIES AT THE INTERSECTION OF DATA PROTECTION AND ARTIFICIAL INTELLIGENCE



Organization for Security and
Co-operation in Europe
Presence in Albania

Challenges and opportunities at the intersection of DATA PROTECTION and ARTIFICIAL INTELLIGENCE

Produced by the Organization for Security and Co-operation in Europe

Organization for Security and
Co-operation in Europe
Presence in Albania

Prepared by: Nevena Ruzic

Design: Graphic Line-01

The views expressed in this publication are those of the author and do not necessarily represent the official position of the OSCE Presence in Albania.

Cite as: OSCE Presence in Albania, Challenges and opportunities at the intersection of Data Protection and Artificial Intelligence (Tirana, 2022)

CIP Katalogimi në botim BK Tiranë

Ružić, Nevena
Data protection and artificial intelligence : challenges and
opportunities at the intersection / Nevena Ruzic. - Tiranë :
Graphic Line-01, 2023
80 f. ; 21x15cm.
ISBN 978-9928-4707-2-0

1.Të drejtat e njeriut 2.Përpunimi të dhënave 3.Mbrojtja
4.Legjislacioni 5.BE 6.Shqipëri

343.43(496.5)
004.56

Summary

There is no human right that is not affected by emerging technologies. On one hand, technology has objectively improved the way we live while, on the other, the use of algorithms may also be detrimental; influencing elections to suppress voter turnout, or spreading disinformation being just a few examples of the potential misuse of technology. However, the omnipresence of technology makes it impossible to ignore. Emerging technologies such as artificial intelligence are present in everyday lives and are regularly deployed by different actors, both private and public.

The pace of technology can be difficult for non-specialists in state legislatures to follow. Nonetheless, there is a need to protect basic human rights by providing an adequate legal framework, not only to keep pace with emerging technologies but provide constant and adaptive protections while enabling the development of technology respectful of human dignity. This task, though easy in words, is difficult to achieve.

The new approach to legislation making, as well as any considerations involving emerging technology, could be best identified as a risk-based approach. The risk-based approach serves to enable assessment of the impact of emerging technologies on the society at large, most notably on the rights of individuals.

Any state assessment of its ability to anticipate human rights risks that may result from the use of new technologies must first build on the assessment of its data protection framework. The Albanian national data protection legislation adopted in 2008, amended in 2012 and 2014, does not provide for a risk-based approach. The new features of the data protection regime introduced by EU General Data Protection Regulation is still lacking in the Albanian framework, though the process to change this has already stated.

International documents, as well those considered or already adopted at national levels, pertaining to artificial intelligence rely on a set of core principles, some of them already embedded in data protection regulation, such as principles of transparency and accountability. Nonetheless, even the existence of appropriate data protection legislation does not guarantee the appropriate adherence to the rules, nor does it imply high level of awareness in society at large. Therefore, the present analysis concludes with the recommendation to better adapt national data protection legislation in order to appropriately address artificial intelligence and other emerging technologies.

Table of Contents

Human Rights and Fundamental Freedoms in the Digital Age

The relationship between democracy and digital technologies is a complex one. While interaction on the internet, as well as via other communication technologies, has encouraged greater interaction and idea exchange and ability to organize, these developments have contributed both towards efforts to defend and supress rights. There is no human right that is not affected by emerging technologies. The use of algorithms to influence elections to suppress voter turnout, tamper with election results, discriminate against groups in a targeted manner, or spread disinformation[1] are just few examples of the potential misuse of technology.

The interest in understanding this relationship between democracy and digital technology is evident worldwide. Recognising this overarching issue, many international organisations have become invested in addressing the importance of building knowledge in the field. One such an initiative was the NHRI Academy "Artificial intelligence and human rights" organised as a joint initiative of the OSCE Office for Democratic Institutions and Human Rights (ODIHR) and the European Network of National Human Rights Institutions (ENNHR) in 2022 in Albania.[2]

[1] Venice Commission, CDL(2020)037, 11 December 2020, Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes. Available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDLAD(2020)037-e.

[2] OSCE ODIHR, Artificial Intelligence and Human Rights: 2022 NHRI Academy. Video and programme available at: https://www.osce.org/odihr/2022NHRIAcademy. There are other initiatives by the OSCE institution regarding the impact of AI on specific rights, such as free speech. See: Office of the OSCE Representative on

In her 2021 report on the right to privacy in the digital age, the then United Nations High Commissioner for Human Rights Ms. Michelle Bachelet noted that artificial intelligence more than other technologies has "captured the public imagination" resulting in "negative, even catastrophic, effects if deployed without sufficient regard to their impact on human rights."[3] The use of AI, even in those cases that may not prima facie involve the processing of personal data, may nevertheless impact individuals. In this respect, even seemingly benign use of technology needs to be assessed from the human rights perspective.

The concise but elaborative report of Ms. Bachelet assessed the decision-making processes of many AI systems as opaque.[4] Of particular concern was the use of AI in law enforcement, national security, criminal justice and border management. She urged a human rights-based approach to new technologies in general, and artificial intelligence in particular,[5] and concluded with the list of recommendations directed to government but also business sector.

In November 2022, the EU Agency for Cybersecurity listed top 10 emerging cybersecurity threats. These are:

1) Supply chain compromise of software dependencies
2) Advanced disinformation campaigns

Freedom of the Media, The Rise of Artificial Intelligence & How it will Reshape the Future of Free Speech, organised in July 2020.

[3] UN Human Rights Council, 48th Session, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, The right to privacy in the digital age, A/HRC/48/31. Para. 2.

[4] UN Human Rights Council, 48th Session, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, The right to privacy in the digital age, A/HRC/48/31. Para. 20.

[5] UN Human Rights Council, 48th Session, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, The right to privacy in the digital age, A/HRC/48/31. Para. 37.

3) Rise of digital surveillance authoritarianism/loss of privacy

4) Human error and exploited legacy systems within cyber-physical ecosystems

5) Targeted attacks enhanced by smart device data

6) Lack of analysis and control of space-based infrastructure and objects

7) Rise of advanced hybrid threats

8) Skills shortage

9) Cross-border ICT service providers as a single point of failure

10) Artificial intelligence abuse[6]

Almost all of them are related to personal data directly, such as the case of disinformation, or digital surveillance, or indirectly. Therefore, addressing the correlation between the use of emerging technologies and personal data entail addressing the issues of comprehensive data protection environment (legislation, enforcement and culture), as well as cybersecurity, and overall strategy, policies and practice regarding emerging technologies.

[6] ENISA, 11 November 2022, Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! Available at : https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030.

Challenges and Opportunities for Data Protection

The importance of and focus on data protection has grown over the past decades. Though the right to privacy, both personal and territorial privacy as well as the privacy of communications, has been part of many constitutional provisions worldwide for centuries, as well as the first human rights international instruments, the right to personal data protection has had a somewhat different path. Nonetheless, as of 1970s many laws explicitly pertaining to data protection has been adopted. The first "Hessische Datenschutzgesetz" adopted by the State of Hesse in Germany, was a reaction to concerns about computing advancements and privacy in the processing of personal data.[7] The number of comprehensive data protection laws today is astonishing. According to the most recent list, close to 130 UN member states have respective data protection laws in place, while nearly all of them have independent data protection or information commissions with mandates to oversee their implementation.[8] Notwithstanding this, it is still early to claim that a) data protection is a recognized human right worldwide, b) that these laws offer uniform understanding of crucial obligations for data controllers and c) that the implementation of the law is an overall success.

At the international level, existing human rights instruments, such as the Universal Declaration, the International Covenant, or the

[7] Following this, Sweden adopted its first national privacy law called the Data Act in 1973, the which criminalised data theft and gave data subjects freedom to access their records. Later at the federal level, Germany adopted the Federal Data Protection Act in 1978 establishing basic data protection standards - the requirement of consent for the processing of personal data.

[8] David Banisar, October 2022, National Comprehensive Data Protection/Privacy Laws and Bills 2022. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416.

European Convention on Human Rights contain articles referring to the right to privacy that through later interpretations by relevant institutions, such as the European Court of Human Rights, or academia, became applicable to the right to data protection.[9] However, a true transformation regarding the way the society, at least in Europe, observes personal data started with the adoption of the first data protection only international binding instrument – the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) adopted in January 1981. Adopted way before ubiquitous email addresses and participatory platforms, Convention 108 proved for long time to be a technologically neutral instrument. However, this document alone, apart from supporting efforts of governments to adopt legislation could not address the rapid growth of information and communication technologies. It was the importance of the European market that put focus on the need for a stringent data protection regime, as was the case with the adoption of GDPR and radiating effect it has had since 2018.

[9] For instance, Article 12 of the Universal Declaration on Human Rights reads: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

GDPR and Convention 108+

Following the Lisbon Treaty, personal data protection has been placed within the competence of the EU rather than of its Member States. In addition, the EU Charter of Fundamental Rights stipulates both the right to private and family life (Art. 7) and the right to protection of personal data (Art. 8).[10] The adoption of General Data Protection Regulation (GDPR) was a revolution in terms of data protection but also how the society perceived technology.

A bit of history in a nutshell – the drafting of the document took several years. It commenced in 2012, when the European Commission proposed a comprehensive reform of Data Protection Directive 95/46/EC to strengthen online privacy rights. The work on the draft was finalised in 2014 and the Draft Regulation was adopted by the European Parliament. Following this, more than 4,000 amendments were submitted by MEPs, the then highest number of amendments in the history of the EU Parliament. The overall process will be remembered by the great number of lobbying groups and stakeholders, from business sectors as well as human rights activists.[11]

As a result, the EU Data Protection Directive was substituted by the General Data Protection Regulation (GDPR)[12] in 2016, effective from May 2018. The aim of GDPR was, summarily, ensuring a comprehensive and directly applicable set of rules for

[10] Charter of Fundamental Rights of the European Union, 2012/C 326/02.

[11] The awarded documentary “Democracy: Im Rausch der Daten“ by David Bernet in 2015 presents the lobbying for the new legal instrument.

[12] 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), L 119/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

regular personal data processing in both public and private sectors, empowering individuals who those personal data refer to (i.e., data subjects) in the exercise of the control over and of their rights pertinent to the processing of data. Furthermore, GDPR has also entrusted specially designated authorities independent from the executive with vast powers to supervise the overall implementation of the provisions, and even impose astronomic fines in cases of incompliance. GDPR, however, is not applicable to data processing resulting from the fight against crime or public safety, nor the matter of national security. The former is regulated under so-called Law Enforcement Directive (LED)[13] adopted together with GDPR. The latter remains within the realm of national legislatures. LED provides minimum standards in the field. The following paragraphs will refer, in general, to GDPR. However, when necessary for the emphasis, the reference to LED will be provided (see in particular DPIA).

Simultaneously, at the level of the Council of Europe, in 2018, a new amending Protocol (Convention 108+) was adopted levelling up European standards in data protection, as well as of those non-CoE member states that have signed, and ratified, the Convention 108+.[14] Convention 108+ incorporated numerous novel provisions referring to, amongst others, definitions of processing of personal data, categories personal data, consent, data subjects' rights, trans-border data transfer, and competences of independent authorities.

[13] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, L 119/89. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN.

[14] The list of countries that have signed (and ratified) Convention is available at:https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

In other words, the revision was significant enough so as to represent a new set of rules. Convention 108+, like the first one, is not limited in terms of its scope, though Member States are given a margin of appreciation when restricting application in the field of national security, however, such exceptions or restrictions cannot refer to standards set by Convention regarding the legitimacy of data processing, data security, transparency of processing or the rights of data subjects. State Parties need to apply specific measures if they intend to use exceptions to some well-defined provisions of the Convention in relation to public interest related tasks and duties.

In the words of the Council of Europe, "if GDPR has been described as the new golden standard for data protection, Convention 108 may represent the potential global standard in this field."[15] This is true if one considers existing different concepts of privacy, as it is not in every country that the right to personal data protection is seen through human rights perception but, as in the USA, as a consumer right.

These developments have resulted in numerous new data protection legislation both Europe-wide and worldwide.[16] However, as noted above, the adoption of new legislation per se, particularly if replicating the provisions of foreign legal instruments, does not secure the level of required data protection.

[15] CoE Conference Convention 108 + And the future data protection global standard, 2019. Available at: https://www.coe.int/en/web/data-protection/convention-108-and-the-future-data-protection-global-standard.

[16] See David Banisar, October 2022, National Comprehensive Data Protection/Privacy Laws and Bills 2022. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416.

General Features of GDPR (and Convention 108+)

Some provisions are essential features of all data protection laws. Firstly, there is a prerequisite that any processing of personal data must be based on at least one of several grounds specified in the law. For the processing of special categories of personal data, such as information about health or political opinions, the legal rules define additional conditions. Secondly, there is a set of rules, i.e., the data protection principles, with which those who are responsible for processing personal data must ensure compliance. Laws are specific in setting requirements for controllers, as well as data processors, to ensure appropriate level of security of the personal data being processed. There is a requirement for controllers to provide information about the processing that they do to the persons to whom personal data refer to i.e., data subjects. Laws are providing a plethora of rights for data subjects in respect of their data which are being processed, such as access to data, rectification or deletion thereof, as well as those important when technology is being used such as right to object to processing or right not be subject to an automated processing of data.[17] In the past year, the rules on the transfer of personal data to third countries have become increasingly strict.[18] The laws allow for

[17] Article 9(1(a)) of Convention 108+ reads: not be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration.

[18] This mainly refer to the transfer to the USA following the revelation of Eduard Snowden as well cases initiated by Maximilian Schremms at the European Court of Justice.

exceptions, however, only in cases these are necessary to protect the data subject, other individuals or specified important national interests. At the end of the list, however, a significant feature of data protection laws, in particular those adopted in the European continent, is the established independent authority responsible for supervising compliance with the law.

All these features are found both in Convention 108+ and the GDPR, though these can be tracked in corresponding provisions in the earlier instruments. The re-examined stance towards significance of personal data, not only for individuals but as being instrumental for a variety of services, public or private, other features have been introduced as compulsory for an appropriate regulatory framework. These refer to requirements for controllers to inform the independent supervisory authorities, as well as data subjects in specific cases, where there has been a data breach. Also, these new features encompass requirements for adopting the concepts of privacy by design and by default. In the case of the GDPR, certain controllers must appoint a data protection officer to assist in better compliance and provide independent advice on data protection matters.

Rights of Data Subjects

Both GDRP and Convention 108+ provide for a plethora of rights for data subjects. According to Art 9 of Convention 108+, every person has a right:

a) not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;

b) to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1;

c) to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;

d) to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;

e) to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention;

f) to have an appropriate judicial and non-judicial remedy when this Convention has been violated;

g) to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority in exercising his or her rights under this Convention.

Under GDPR, the rights of data subjects are defined in Chapter 3. These are:

- Right to be informed (Transparency)
- Information and access to personal data
- Right of access by the data subject
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restriction of processing
- Right to data portability
- Right to object
- Right related to automated individual decision-making, including profiling

The right to remedy, as listed under Convention 108+, is assumed, and is the subject matter of another Chapter. In addition, the right to address the relevant data protection authority must be indicated in the privacy notice, and information provided to the data subject at the moment of the first processing activity – data collection.

Without elaborating on each of them, here it is important to emphasise that these rights are not absolute and may be denied if other rights and interests prevail. As in the case of other human rights, under European Convention of Human Rights applicable to all CoE Member States, any restriction must be in accordance with the known tripartite test – being provided by law in order to protect legitimate interest, while the limitation must be necessary in a democratic society.

The right to be informed corresponds to the obligation of a data controller to provide information about the relevant aspect of the processing, such as the identity of a controller, purpose of processing and legal basis thereof, as well as the rights of data subjects including those of addressing the data protection authority. The information i.e., the notification of processing should also include information about other recipients as well as data transfer outside the jurisdiction. This requirement is not an easy task if the use of AI is involved in the processing of data.

In addition, the rights listed are not applicable to every processing of personal data as they correspond to the legal basis for the processing. For example, the right to data portability (GDPR, Art. 20), is applicable only in cases the processing is based on a data subject's consent or on a contract. In practice, one may think of this right as easily explainable in cases of social networks. Another example is the right to object (GDPR, Art. 21) which is applicable in cases the processing of data is based on a legitimate interest of a data controller or a third party, or in cases the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

In the age of heavy reliance on technologies, the right not to subject to a decision significantly affecting data subject based solely on an automated processing of data is presumably demanding to implement. There has to be a human interaction involved in the decision making, and this interaction needs to be meaningful. This is an onerous task, as the fulfilment of the requirement for a meaningful human review may assume that the action is carried out by someone who possesses authority and competence to change the decision, and in so doing, able to take all relevant data into consideration.[19]

In their toolkit prepared to provide practical support to organisations to reduce the risks caused by their AI systems to individuals' rights and freedoms, the UK's Information Commissioner noted three key considerations of what meaningful human review should be. Primarily, human reviewers must be involved in checking the system's recommendation and should not just apply the automated recommendation to an individual in a routine fashion. Secondly, their involvement must be active and not just a token gesture, thus they may even go against the recommendation. Finally, they must 'weigh-up' and 'interpret' the recommendation, consider all available input data, and take into account other additional factors.[20]

[19] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), adopted on 22 August 2018, approved by EDPB on 25 May 2018, p. 21. Available at: https://ec.europa.eu/newsroom/article29/items/612053/en.

[20] ICO, AI and data protection risk toolkit, last updated in May 2022. Available for download at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/.

Privacy by Design/Default

The concept of privacy by design (PbD) has been designed by Ann Cavoukian,[21] the former Information and Privacy Commissioner of Ontario and developed since 1990s. The seven principles[22] of information management, and the philosophy and methodology they express, can apply to specific technologies, business operations, physical architectures, and networked infrastructure, in other words to entire information ecosystems. PbD requires the incorporation of data privacy protections into the very design of an information system, thus securing personal data from breaches and protecting individuals in the exercise of their rights.[23] The concept of privacy as the default is one of the seven foundational principles of PbD. Together they are abbreviated as PbDD.

The obligations provided under GDPR, as well as Convention 108+, refers most solely to data controllers, those that define purpose and means of the processing of personal data. Data processors, that process personal data on behalf of the controller also have duties, however, save for few these are mainly supporting duties of data controllers. This leave many vendors out of the reach of data protection regimes. In practice, technology is developed by companies that may later never come in touch with personal data including as a part of the maintenance of the equipment. However, the concept of PbDD puts those entities under the rule of data protection, as even vendors are required to have their products in

[21] Privacy by Design – The 7 Foundational Principles, available at: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

[22] These are: Preventatives not counteractive and Preemptive not reactive; Privacy as default setting; Embedded privacy in design; Full functionality: positive-sum instead of zero-sum; Transparency and visibility: keep it exposed; Endwise security and full lifespan protection, and Respect for the privacy of user and keep it user-centric.

[23] Privacysense.net, Privacy by Design, (November 28, 2017, last updated on May 12, 2022), available at: https://www.privacysense.net/terms/privacy-by-design/.

compliance with this concept to be an eligible contracting party to a data controller or even processor.

This is clear from the Preamble of GDPR. “When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.”[24]

The “state of the art” refers to the considerations vis-à-vis emerging technologies, and imposes an obligation on controllers, to “have knowledge of, and stay up to date on technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that secure effective implementation of the principles and rights of data subjects taking into account the evolving technological landscape”.[25] That means that whenever technology is used, data controllers may not free themselves due to the lack of knowledge.

[24] GDPR, Recital 78.

[25] EDPB, Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

Data Protection Impact Assessment

GDPR has introduced various new methods and measures at the EU level to create legal tools to ensure better compliance as well as secure that the rights of data subjects are adhered to. A way for data controllers to ensure that their data processing processes comply rules is through the data protection impact assessment (DPIA). As a result of a properly conducted assessment, a controller can ensure that the principles are optimised, privacy, information security and reputation risks are minimised. In this context, the DPIA is seen as one of the main achievements of the recent reform.

In comparison to PbDD, DPIA has to be performed and documented, and eventually examined by the data protection authority. In particular, the innovative and ambitious nature of this solution is highlighted, as it represents a novelty not previously regulated under previous EU law. Convention 108+ also refers to impact assessment, as a duty of the state to prescribe this obligation for data controllers. According to Art 10, each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

Naturally, even though any processing of personal data may result in risks for the rights and freedoms of natural persons, not every processing should be assessed through DPIAs, but only those that are likely to result in high risks. Art. 35 GDPR stipulates three such cases: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences referred; or (c) a systematic monitoring of a publicly accessible area on a large scale. However, DPIA is also mandatory in cases of processing identified as resulting in high risks by competent data protection authority.[26] In addition, even in cases that are not on the list, the controller is obliged to perform a DPIA.

There is no given methodology for performing DPIA and it is left to the controller to choose one. Although the obligation is on the controller, they are assumedly not competent to perform DPIA for processing activities not performed by themselves. In this respect, the role of processor is to assist the controller. The duty to perform DPIAs is also envisaged by LED (Art 27).

Its minimal content is specified by GDPR Article 35(7) and LED Article 27 as follows:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects; and

d) the measures envisaged to address the risks, including

[26] Every national data protection authority has provided the list of processing operations for which DPIA is mandatory.

safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the legislation taking into account the rights and legitimate interests of data subjects and other persons concerned.

GDPR, as well as LED, also imply that DPIA is performed in the process of the making of legislation that, due to, for example, its scope, may result in high risk. Taking into consideration the reliance on technology and deployment thereof on personal data, the legislative DPIA should result in understanding all the risks some general provision may have on rights and freedoms and shaping that provision in a way to mitigate those risks. For example, the introduction of biometric measures by means of a legislation should be analysed by a legislative DPIA, together or later accompanied by a specific DPIA that could be understood as a project. It is very important to distinguish between these different yet connected processes. The purpose of a legislative DPIA is fostering public and professional discussions about the need and, if applicable, acceptance of a certain measure in society. The focus of a legislative DPIA is to objectively assess the proportionality, the necessity, the risks involved and possible risk mitigation measures in order to allow public discussion whether the proposal is adequate or not. Risk mitigation measures should therefore mostly be of law provision level (e.g. a specific conditions or banning of application of AI) and not those of the implementation level (e.g. specific security measures).

In November 2022, Privacy Company in the Netherlands, commissioned by the Dutch Ministry of the Interior and Kingdom Relations, published their findings on DPIAs on government use of Facebook Pages acknowledging seven high data protection risks. Data protection risks can be grouped in the following categories:

Inability to exercise rights (including but not limited to privacy rights); inability to access services or opportunities; loss of control over the use of personal data; discrimination; identity theft or fraud; financial loss; reputational damage; physical harm; loss of confidentiality; re-identification of pseudonymised data; or any other significant economic or social disadvantage.[27] Following this report, the Secretary of State for Digitisation, explained that she was in dialogue with Facebook to mitigate all risks, however, she warned that if those risks would not be removed the government would stop using Facebook pages.[28]

[27] Privacy Company, Data protection impact assessment on the processing of personal data on government Facebook Pages, Version 1.0, 16 November 2022, p. 138. Available at: https://www.privacycompany.eu/blogpost-en/dpia-on-government-use-of-facebook-pages-seven-high-data-protection-risks.

[28] NL Times, 17 November 2022, Dutch government will stop using Facebook if it doesn't improve private data handling. Available at: https://nltimes.nl/2022/11/19/dutch-government-will-stop-using-facebook-doesnt-improve-private-data-handling.

Data Protection Officer

The mandatory appointment of data protection officers (DPO) is one of the new features of modern data protection legislation. They best described as "'a cornerstone of accountability' since they facilitate compliance, while also acting as intermediaries between the supervisory authorities, data subjects and the organisation by which they have been appointed."[29] Under GDPR the appointment of DPOs is mandatory for certain data controllers and processors that are either considered public authorities, hence greater duty of care, or which main activities entail processing which require the regular and systematic monitoring of data subjects on a large scale, or of data that are of special category at large-scale (Art. 37). Convention 108+ does not refer to DPOs, however, they are mentioned in the Explanatory Report accompanying the Convention.[30]

Their main tasks are to monitor compliance with GDPR, provide opinion on DPIA, and cooperate with the supervisory authority and act as a contact point (GDPR Art. 39). The task to monitor compliance with GDPR they may perform through collecting information to identify processing activities, checking the compliance of processing activities, as well as informing and counselling the controller or the processors.[31] As a contact point for a data protection authority a DPO has an active role in cases of a data breach. To perform these tasks, DPOs should be provided

[29] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, Handbook on European data protection law : 2018 edition, Publications Office of the European Union, 2019, p. 175. Available at: https://data.europa.eu/doi/10.2811/343461.

[30] Explanatory Report of Convention 108+, para. 87.

[31] Article 29 Working Party (2017), Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, last revised and adopted 5 April 2017, paras. 4.1.-4.3. Available at: https://ec.europa.eu/newsroom/article29/items/612048/en.

with appropriate resources.

DPOs are expected to possess knowledge, expertise, and abilities for performing their tasks. In the lack of further elaboration on the nature of the required expert knowledge and abilities a conclusion is that these would depend on the activities of the controller.[32] DPOs may be appointed as an in-house or external expert, however, DPOs cannot be a legal entity but a natural person, and are usually a single person.. In practice however, especially in cases of data controllers that are processing data on large scale, such as authorities competent for public security, or the processing activities may result in high risk to data subjects, such as the case with financial institutions, there may be a team or unit dealing with data protection compliance.

Despite this, they are not responsible for the compliance with a data protection regime and cannot be held accountable for a failure to comply. It is important to emphasise that the overall accountability is on the actual data controllers and data processors.

[32] Douwe Korff and Marie Georges, The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, As approved by the Commission, July 2019.

Data Breach

By definition, a data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (GDPR Art. 4(12)). In such a case there is a duty to report to the data protection authority, as well as data subject in certain cases. This duty is envisaged by Convention 108+, according to which Parties must, as a minimum, require controllers to notify the competent supervisory authority of data breaches that may seriously interfere with the rights of the data subjects. Such notification should be completed 'without delay'.[33] GDPR sets deadline for the reporting to 72 hours of the moment controllers become aware of the breach (Art. 33-34).

In practice, if processing activities are outsourced and performed by data processors it would be them, and not the controller, that first become aware of a data breach. Under the GDPR they are bound to report to the controller and assist them in reporting to the data protection authority, as well as taking measures to minimise any consequences. Not reporting the breach is a breach of law per se. In the past, it was realised that many data breaches were not reported due to the impact on reputation. However, it is fair to acknowledge that data breaches are neither rare nor exclusive for a particular sector and, with such reliance, and dependence on technology, data breaches are both inevitable and quite frequent.

In 2022, still as an EU Member State, the UK Information Commissioner Office issued a 18.4 GBP Million fine following a cyber-attack on several hotels that later were acquired by Marriott. Attack resulted in hackers having access to more than 339 million

[33] Convention 108+ Art. 7 (2) and Explanatory Report, paras. 64-66.

guest records, including seven million records related to people in the U.K. The breach, which occurred in 2014, was undetected until September 2018. Personal data accessed in the breach included names guests, their email addresses, phone numbers, unencrypted passport numbers, as well as arrival/departure information, as well as VIP status or loyalty programme membership number.[34]

[34] Forbes, Carly Page, 30 October 2020, Marriott Hit With £18.4 Million GDPR Fine Over Massive 2018 Data Breach. Available at: https://www.forbes.com/sites/carlypage/2020/10/30/marriott-hit-with-184-million-gdpr-fine-over-massive-2018-data-breach/?sh=72f03b09e4b0.

Data Transfers

Trans-border data flow has always been a part of data protection regimes. The objective of GDPR is to lay down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data (Art. 1). Convention 108+, but also Convention 108 adopted in 1981, provide rules for trans-border data flow. The Council of Europe Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows deals in particular with the issue of data transfers.[35] However, that does not mean that any transfer is allowed or that there are no strict rules. Quite contrary – the rules for data transfers have become in time even more stringent, in particular transfers outside the European Union, or the European Economic Area.[36]

Under Art. 14 of Convention 108+, as a rule, the Party should not for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the

[35] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181), adopted in 2001, in force since July 2004.

[36] Decision of the Council and the Commission of 13 December 1993 on the conclusion of the Agreement on the European Economic Area between the European Communities, their Member States and the Republic of Austria, the Republic of Finland, the Republic of Iceland, the Principality of Liechtenstein, the Kingdom of Norway, the Kingdom of Sweden and the Swiss Confederation, OJ 1994 L 1.

Convention. However, the Party may prevent a transfer if there is a real and serious risk that the transfer would lead to circumventing the provisions of the Convention. If the transfer of personal data is to be carried out to a country that is not a party to this instrument, the transfer is allowed if there are appropriate levels of protection either set out in the law of that State, or international organisation, as if there are ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing. There are other extraordinary exceptions to this rule, though the interpretation thereof should be limited.

GDPR stipulates stringent rules to data transfers. Transfer is acceptable in cases where there is an adequacy decision by the European Commission (Art. 45), or, in the absence thereof, if the controller or processor provides appropriate safeguards (Art. 46). The former refers to the procedure of estimating whether a jurisdiction provides for appropriate safeguards, including the state of rule of law. The list of adequacy decisions is available to the public.[37] The latter may depend either on the existence of specific instruments, such as Standard Contractual Clauses, or approved binding corporate rule, or on the decision of a designated data protection authority.

Transfer from the EU to the USA is under a specific regime and the issue whether it is safe to transfer data is still pending. Initially, transfers to the USA were waived from additional conditions based on a so-called Safe Harbour. In 2015, the agreement was quashed by the European Court of Justice as the set principles only bound US companies but not their public authorities, while derogations from principles for national security were estimated as being without

[37] Adequacy Decisions are available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

any safeguards.[38] Following this, a new framework was adopted in 2016, the EU–US Privacy Shield, however, this, too was annulled in 2020.[39] The Court ruled that, prior to the transfer of data outside the allowed transfer bubble, an adequate level of data protection must be evaluated on a case-by-case basis, creating thus a new assessment –the Transfer Impact Assessment. This assessment is not needed only for transfers to the USA but also other countries that are not referred to in adequacy decisions, such as Albania.[40] A new framework pertaining to transfer of personal data between EU and USA is still pending.[41]

In December 2022, Data Protection Authority of Portugal fined the National Statistics Authority with €4.3 million EUR for five breaches of the GDPR made while carrying out the 2021 census, including unlawful international transfers. The other breaches referred to unlawful processing of special categories of data (related to health and religion), failure to notify data subjects, failure to conduct DPIA and failure to adequately perform due diligence in selecting a subcontractor.[42]

[38] C-362/14 Maximillian Schrems v Data Protection Commissioner, Joined Party Digital Rights Ireland Ltd, ECLI:EU:C:2015:650

[39] Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (called "Schrems II case"), ECLI:EU:C:2020:559

[40] Transfers to other Western Balkan countries (Montenegro, North Macedonia or Serbia) are also subject to this assessment.

[41] Draft decision Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (dated 13 December 2022) is available: https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf.

[42] Portugal News, 12 December 2022, €4.3 million fine for breaching data protection rules in the Census. Available at: https://www.theportugalnews.com/news/2022-12-12/43-million-fine-for-breaching-data-protection-rules-in-the-census/72883.

Data Protection Law of Albania

On Data Protection in Albania

As an EU candidate country, Albania is obliged to harmonise its legislation concerning personal data protection with Community law and other European and international legislation on privacy, including the establishment of independent supervisory bodies with sufficient financial and human resources to efficiently monitor and guarantee the enforcement of national legislation on personal data protection.[43]

With regard to international commitments, Albania has ratified all relevant conventions of the Council of Europe, including Convention 108+ in 2022.[44] The Commissioner for the Right to Information and Protection of Personal Data (the Commissioner) is a member of the Global Privacy Assembly, the international standard setting body comprising of authorities in the field of data protection. The Commissioner was the host of the Conference of European Data Protection Authorities, in 2018, the 41st International Conference, in 2019. The latter was the first event of its type hosted in a Western Balkan country.

[43] Article 79 of Stabilisation and Association Agreement between the European Communities and their Member States of the one part, and the Republic of Albania, of the other part, 2009, O.J. (L107). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22009A0428(02).

[44] Convention was signed on 28 January 2022, symbolically on the Data Protection Day, and ratified on 22 July. The list of other signatures and ratification available of the CoE webpage: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

The Law on the Protection of Personal Data was adopted in 2008,[45] and amended in 2012 and 2014. The amendments in 2012 were substantial in terms of definitions,[46] while those of 2014 referred to only few articles vis-à-vis the position of the Commissioner, as the independent data protection authority. The Law, therefore, has not been compliant with GDPR and LED as noted in the EU annual state report in 2018, the year of the implementation of the said acts.[47] In the 2022 Report, the EU noted not only the need to adopt appropriate legislation but also the references were made to data breaches that occurred in the country.[48]

Noteworthy is that in late 2020, the Commissioner commenced the drafting of the new law supported by the EU funded project and was expected to be finalised by the end of 2021.[49] However, the process is still pending.

[45] Official Journal No. 9887 of 10.3.2008., amended in 2012 (OJ No. 48/2012) and in 2014 (OJ No. 120/2014).

[46] Law No. 9887 dated 10.03.2008, as amended by the Law No. 48/2012, dated 26.04.2012. Official translation of the text published in the Official Journal No.53, date 16.05. 2012 on Protection of Personal Data. The translation was commissioned by the EU funded Project "Strengthening of the Data Protection Commissioner office in Albania, for alignment with EU standards".

[47] European Commission, 2018, Albania 2018 Report, 17.4.2018., SWD(2018) 151 final, p. 26, available at: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-albania-report.pdf.

[48] European Commission, 2020, Albania 2020 Report, 6.10.2020, SWD(2020) 354 final, p. 30, available at: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/albania_report_2020.pdf.

[49] Nevena Ruzic, Nationalising the General Data Protection Regulation in Western Balkan, in Regional Law Review 2021, p. 317. Available at: https://rlr.iup.rs/archives/year-2021.

Features of the Law

Many features elaborated above are not included in the national law. For example, there is no obligation to perform DPIA, crucial to comprehend the impact an activity may have on rights and freedoms. Secondly, there is no explicit duty to report a data breach, though the provisions on security measures should be interpreted as requiring that actions need to be taken once a breach is acknowledged. Likewise, there is no duty to notify individuals affected by the breach. Thirdly, neither data controllers nor data processors are obliged to appoint a DPO, which would assist in improving compliance with data protection requirements. Furthermore, provisions on data transfers, although in place and quite elaborative (Art. 8, 9), do not reflect the current rules on trans-border data flow, nor provide a basis for the adoption of template agreements that incorporate all data protection principles, prima facie, the principle of accountability. Finally, the current definition of sensitive data does not address genetic data or biometric data.[50] The latter will be of essential importance for the use of facial recognition technologies that nowadays assume the use of AI.

Like other laws adopted at the time, the Data Protection Law prescribes the duty to notify the Commissioner about the processing of personal data for which a controller is responsible in due time, i.e., the Law imposes a prior notification on processing (Art. 21). Although this was envisaged in the EU Data Protection Directive, the effect thereof is that the respective authorities were overburdened with tasks to register numerous applications instead of being engaged with other issues. For example, every

[50] According to Art 3(4), “Sensitive data” shall mean any piece of information related to the natural person in referring to his racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal prosecution, as well as with data concerning his health and sexual life.

data controller, as a legal person, public authority, agency or any other body [Art. 3(1(5))], is an employer. The employer by default processes data for different purposes, such as to comply with various legal obligations, or to perform contract or to pursue legitimate interests like using video surveillance to protect premises, or publishing CVs of the top management. If every employer in the country notified the Commissioner about every processing of personal data, those notifications alone would block the work of the institution.

Data Breach Case/s

There have been several reported data breaches that have caught the attention of media as well as international organisations due to their impact on the right to privacy and freedom of expression, as well as their cascading impact on other rights and freedoms. Due to the fact that media coverage about the outcome of the breaches is light on technical details or otherwise reveals little on the issue, there is a need to refrain in this part from the assessment of reactions of competent authorities, notably of the Commissioner. In addition, it should be emphasised that data breaches happen in many countries, as presented in numerous examples above. However, the cases here presented are of great significance for the understanding of the necessity for making data protection rules more stringent as well as their enforcement. Finally, the cases presented are not only relevant for the application of data protection laws but other laws such as criminal codes which will presumably be enforced.

In April 2021, Transparency International reported on the online exposure of close to million people database whose personal data were held by the country's ruling Socialist Party.[51] The revelation also indicated "that 'patrons' were assigned to voters who tracked their political preferences. Additional comments, recorded by the patrons, reportedly detail their interactions with citizens, with some instances amounting to possible voter intimidation."[52] According to the Balkan Investigative Reporting Network, many of those patrons were "employed in the public sector, including central and local government entities and state utility companies dealing, for

[51] Transparency International, Albania: Alarm over Indications of Personal Data Breach, Election Campaign Violations, 22 April 2021. Available at: https://www.transparency.org/en/press/albania-alarm-over-indications-of-personal-data-breach-election-campaign-violations.

[52] Ibid.

example, with water and electricity supplies”.[53]

In December 2021, the database of the taxation authority as distributed on social media containing names, data pertaining to their place of work, as well as their respective salaries for the month of January 2021 of more than six hundreds of thousands of people, both employed in public and private sector personnel.[54] According to the news from January 2022, a year after, four people were arrested for the leak, including two IT technicians working at the taxation office.[55]

In May 2022, several media freedom organisations gathered under the name of Media Freedom Rapid Response sent an open letter to the Albanian Commissioner urging his office to “to conduct a swift and thorough investigation into the breach of personal data – which was then used to frighten and pressure one of the journalists”.[56] According to the allegations, the journalists that were reporting on a sensitive issue were being intimidated via proxies using information collected through unauthorised access to personal data, such as “the certificate for his family from the Civil Registry – a document only available to registered notaries in Albania.”[57]

[53] BIRN, Gjergj Erebara, 21 April 2021, Police, Soldiers among Albanian Ruling Party’s Voter Tracking ‘Army’. Available at: https://balkaninsight.com/2021/04/21/police-soldiers-among-albanian-ruling-partys-voter-tracking-army/.

[54] A2 (CNN), 22 December 2021, Private information about salary of 630,000 Albanians leaked online. Available at: https://english.a2news.com/2021/12/22/private-information-about-salary-of-630000-albanians-leaked-online/.

[55] DataBreaches.net, 7 January 2022, Albania arrests four over massive personal data leak. Available at: https://www.databreaches.net/albania-arrests-four-over-massive-personal-data-leak/.

[56] Article 19, an open letter to Mr. Besnik Dervishi, Commissioner for the Right to Access to Information and Personal Data Protection, on 09 May 2022, sent electronically. Available at: https://www.article19.org/resources/albania-data-breaches-and-intimidation-of-journalists-must-be-investigated/.

[57] Ibid.

Need for New Legislation

Considering the time of the adoption of Law on the Protection of Personal Data, it is only logical to strongly recommend new legislation. The arguments for such a need are many.

Apart from political commitments as an EU candidate country, there are also international commitments taken with the ratification of Convention 108+ that sets higher bar for national data protection legislation. Consequently, the individuals will be given greater protection of their rights.

Furthermore, cooperation or any exchange with counterparts from the European Union will be much easier for national companies if the regulatory framework provides appropriate safeguards. Through these, the country may be considered eligible to pass the demanding screening procedure and be granted the adequacy decision that would open new business opportunities for companies, including those active in technology sector.

Finally, the appropriate data protection legislation, and appropriate enforcement thereof, is a solid basis to address the emerging technologies. This is due to the fact that even golden data protection standards, as GDPR is believed to be, is not enough to be adequately applied to artificial intelligence and other emerging technologies.

Individual Behaviour

The individual perception of privacy is a key element for the overall improvement of the respect of right to privacy and data protection. The fact that there is data protection legislation in place would mean little to the society if the right were not perceived as important. How people interact with others, how they use technologies and what they share should be a part of broader debate, involving not only lawyers or IT specialist but others as well.

In an attractive short video clip dated 10 years ago, a performer dressed as a guru lured people in his tent to read their mind, but in fact revealed astonishing information, mostly financially related, collected solely through publicly available data that they themselves revealed.[58] One of the best illustrations of how platforms operate was presented in research conducted by the University of Cambridge and Stanford back in 2015, i.e. seven years ago – too long ago when thinking of emerging technologies. According to their findings, only 10 likes on Facebook were enough for the platform to "more accurately predict a subject's personality than a work colleague. With 70 likes, it could know more about someone than their friends, and with 150 it would be more knowledgeable than a family member. With 300 likes it could determine [one's] personality better than a spouse."[59]

The impact of technology to children is multifaceted. The oversharing of their children's photos, as well as videos, called sharenting has become an issue of not only ethics but also lawsuits.

[58] Duval Guillaume YouTube channel, Amazing mind reader reveals his 'gift', uploaded on 24 September 2012. Available at: https://www.youtube.com/@duvalguillaume/about.

[59] CNBC, Arjun Kharpal, 13 January 2015, Facebook knows you better than your family. Available at: https://www.cnbc.com/2015/01/13/facebook-knows-you-better-than-your-family.html.

For the rock music lovers, this phenomenon is best known through the lawsuit filed by person against the band Nirvana, that in the ‘90s used the photo of him as a cover for their hit album “Nevermind”.[60] However, the challenge of sharenting does not only effect the right to privacy of minors, but may jeopardise their safety as well. The danger of overexposure led the French authorities to initiate a public campaign targeting perilous behaviour of parents.[61] Online behaviour is part of the culture that does not reflect the culture of offline interactions. The use of different gadgets at early age does have effect not only on data protection but may result in cyberbullying.[62]

Therefore, education is an inevitable piece of a puzzle of an appropriate data protection framework and it should not be the task reserved by one or even a few stakeholders.

[60] Rolling Stone, Nancy Dillon, 13 January 2022, ‘Nevermind’ Baby Is Still Suing Nirvana, available at: https://www.rollingstone.com/music/music-news/nevermind-baby-is-still-suing-nirvana-1284031/. The case is pending.

[61] The Verge, taken from Le Figaro, Amar Toor, 2 March 2016, French police tell parents to stop posting Facebook photos of their kids. Available at: https://www.theverge.com/2016/3/2/11145184/france-facebook-kids-photos-privacy.

[62] The Economic Times, Stephanie Bodoni, 31 December 2020, 12-yr-old London girl can sue TikTok for privacy breach, court grants anonymity. Available at: https://economictimes.indiatimes.com/magazines/panache/12-yr-old-london-girl-can-sue-tiktok-for-privacy-breach-court-grants-anonymity/articleshow/80046082.cms.

Opportunities and Challenges of Artificial Intelligence

Artificial Intelligence (AI) may be subject to different perceptions that may, and often do, alter the way we approach and understand it. However, it is worth noting that AI systems should not be perceived as just a sum of software components. The socio-technical system around it must be considered as equally important. When we are talking about governance, the focus should not be just on technology, since social structure should be included: organisations, people, and institutions. They are all affected by AI. Citizens in relation to governments or employees in relation with employers are just few examples of the radiating effect a computer code may have.

There are different forms of AI. PricewaterhouseCoopers (PwC) distinguishes between Automated Intelligence (automation of manual/cognitive and routine/non-routine tasks), Assisted Intelligence (helping people to perform tasks faster and better), Augmented Intelligence (helping people to make better decisions) and Autonomous Intelligence (Automating decision-making processes without human intervention).[63] This broad understanding of AI leads to the acknowledgement of the use of AI for more than many decades. For example, according to the UNESCO's paper on AI and Education, the use of AI may be said to have started in 1970s, when "researchers were interested in seeing how computers might substitute for one-to-one human tutoring"[64].

Back in 2017, in an own-initiative opinion prepared by the EU

[63] PwC, 2017, Sizing the prize – What's the real value of AI for your business and how can you capitalise?, available at: https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf.

[64] UNESCO, 2021, AI and Education: Guidance for policy-makers, available at: https://unesdoc.unesco.org/ark:/48223/pf0000376709.

Back in 2017, in an own-initiative opinion prepared by the EU European Economic and Social Committee, 11 areas of societal challenges caused by AI were identified: "ethics; safety; privacy; transparency and accountability; work; education and skills; (in) equality and inclusiveness; law and regulations; governance and democracy; warfare; superintelligence."[65] Investigating the impact of automatable occupations in the article addressing the future of work almost 10 years ago, the researchers estimated that "almost 47 percent of total US employment is in the high risk category, meaning that associated occupations are potentially automatable over some unspecified number of years."[66] Expectedly, not all occupations are equally affected by the advancement of technology. According to other estimates, it is a matter of time when AI will begin outperforming humans in specific tasks such as translating from foreign languages (by 2024), writing essays at the level of high-school students (by 2026), driving vehicles (by 2027), or writing bestsellers (by 2049), or even performing surgery (by 2053).[67]

A common argument is that one should start from the premise that technology is neutral. Nevertheless, the way we deploy may not be, or rather seldom is. AI per se may be judged through positive

[65] EESC, 2017, "Artificial Intelligence – The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society (own-initiative opinion)", para 1.5. Adopted on 31/05/2017, Reference: INT/806-EESC-2016-05369-00-00-AC-TRA, Official Journal: OJ C 288, 31.8.2017, p. 1, available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/artificial-intelligence-consequences-artificial-intelligence-digital-single-market-production-consumption-employment-and.

[66] Carl Benedikt Frey and Michael A. Osborne, "The Future of Employment: How Susceptible are Jobs to Computerisation?", September 2013, Oxford Martin Programme on Technology and Employment. Available at: https://www.oxfordmartin.ox.ac.uk/downloads/academic/future-of-employment.pdf.

[67] Katja Grace, John Salvatier, Allan Dafoe, Baobao Zhang, Owain Evans, "When Will AI Exceed Human Performance? Evidence from AI Experts", 3 May 2018, Journal of Artificial Intelligence Research, available at: https://arxiv.org/pdf/1705.08807.pdf.

or rather optimistic attitude, or, quite contrary through sceptical or negative ones. Nonetheless, the ‘either/or’ approach is not helpful and the reasons are many. Firstly, as a society we are already witnessing the deployment of artificial intelligence in many areas. Secondly, again as a society, we have already testified how AI creates amazing benefits for many areas of our lives. Thirdly, we have been made aware that the technology may be used to single out individuals or groups. Lastly, though each reason pertains to a number of cases different in scope and effect, it does create both opportunities and challenges sometimes of equivalent significance.

For those using mobile phones with Android as an operating system, having a Google email account is inevitable. As simple as it may seem, it is thanks to AI algorithms that some emails sent to one’s Gmail may never reach inbox as they are marked as spam. If the user realises that the sorting was wrong, once that email, or the sender, is removed from the spam folder as placed in the inbox, similar emails, e.g., from that sender, are never sent there again. Like in other cases, “the algorithms do not work perfectly, but they are continuously improved”[68].

[68] Geneva Internet Platform, DigWatch, “Artificial Intelligence”, available at: https://dig.watch/technologies/artificial-intelligence/.

Opportunities of AI

There are many areas of life the AI systems have been deployed or considered to be deployed – medicine, education, finance, transport, media, including internet industry, safety. The list of areas is not exclusive and set not in order of importance. For many challenging the AI may appear as the best solution.[69]

One the greatest achievements of the use of technology advancement is certainly in medicine. Relying on data processed using artificial intelligence may help doctors identify diseases long before they evolved to irreversible degree. Overall, the computer-based systems that can structure and use data sets as the basis of medical knowledge may serve to guide diagnosis (i.e., to expedite diagnosis, correct misdiagnosis, or diagnose previously undiagnosed patients) and select treatment. The latter is said to still be lagging,[70] however, it may be just a matter of time.

In 2021, at the MIT, dermatologists that have been working with the researchers visually classified the lesions in the images for comparison, founding that the system being "more than 90.3 percent sensitivity in distinguishing SPLs [suspicious pigmented lesions] from nonsuspicious lesions".[71] The investment in AI systems to be used in medicine is significant. For example, the IBM's Watson (recently changed into Merative) provides a luring

[69] Moderately comprehensive overview of problem solving examples of AI is available at: https://indatalabs.com/ai-business-use-cases.

[70] Brasil S, Pascoal C, Francisco R, dos Reis Ferreira V, A. Videira P, Valadão G. Artificial Intelligence (AI) in Rare Diseases: Is the Future Brighter? Genes. 2019, p. 16, 10(12):978, available at: https://doi.org/10.3390/genes10120978.

[71] Megan Lewis, "An artificial intelligence tool that can help detect melanoma", Institute for Medical Engineering and Science, April 2, 2021, available at: https://news.mit.edu/2021/artificial-intelligence-tool-can-help-detect-melanoma-0402.

overview of how AI may help health care providers and patients.[72]

Financial Institutions, prima facie banks, are not immune to the use of technology. The way clients, particularly digital natives, are expecting their banks to address their needs has significantly changed over the past years. “The rise of omni-channel experiences and digital platforms has led to customers not only wanting, but expecting, a white glove user experience from all the products they interact with – one that is consistent, intuitive, and generates trust and excitement.”[73] Banks are using AI to predict, based on customer data, how prone their clients are to redeem their credit card points, thus to provide them with offers for certain categories, e.g. travel, or just gift cards. The result was that the number or those AI-recommended email offers turned high.[74]

Addressing the importance of AI for bank sector, Deloitte has concluded that it would be “possible that banks’ competitive features could very well depend on building the technological foundations and processes to fully realize the benefits that AI promises to deliver.”[75] However, though this part is dedicated to the benefits of the use of AI in different fields of life, it needs to be emphasised that financial institutions have to apply appropriate legal bases for processing of personal data. In February 2022, the National Authority for Data Protection and Freedom of Information fined the Budapest Bank HUF 250 million (approx. €653,000) due to the use of artificial intelligence to analyse audio recordings

[72] https://www.ibm.com/watson-health.

[73] AIThority, Omar Arab, 10 September 2020, Reimagining Banking’s Customer Experience for the Digital Era. Available at: https://aithority.com/technology/financial-services/reimagining-bankings-customer-experience-for-the-digital-era/.

[74] Tearsheet, Tanaya Macheel, 20 March 2018, HSBC is using AI to personalize its rewards program. Available at: https://tearsheet.co/artificial-intelligence/hsbc-is-using-ai-to-personalize-its-rewards-program/.

[75] Deloitte, 2021, Artificial intelligence: Transforming the future of banking. Available at: https://www2.deloitte.com/us/en/pages/consulting/articles/ai-in-banking.html.

of customer service calls failing to comply with several GDPR provisions, including those pertaining to the legal basis for data processing as well as the rights of data subjects.[76]

The wide range of Internet Service Providers as well as social media are increasingly well developed due to AI integration for many years. The searches via most popular search engines, such as Google, is defined by one's geolocation as well as previous searches or other data. It will appear that, as with zebras and stripes, no two people will get the same results with crawling, indexing or ranking, as the key AI actions underlying each will differ.

The way users are being offered the content they will most probably find appealing has been elaborated on in many articles, as well as popular documentaries[77]. The awarded documentary Social Dilemma is an excellent stop to expose oneself to the particles of how AI reaches individual in daily lives.

Education is an area in which the use of computer systems has been used of very long time. Overall, reading and language learning tools rely on AI to augment the outcomes of better pronunciation while comparing the voice to those of native speakers.[78] And these tools are not used only in educational institutions but are well spread worldwide and used individually.[79] Some of those promising

[76] OneTrust Data Guidance, 12 May 2022, Hungary: NAIH fines Budapest Bank record HUF 250M fine for unlawful AI analysis of customer calls. Available at: https://www.dataguidance.com/news/hungary-naih-fines-budapest-bank-record-huf-250m-fine.

[77] Apart from the movie available on different movie platforms, the website https://www.thesocialdilemma.com/ provide plethora of additional materials and interviews on the topic.

[78] UNESCO, 2021, AI and Education: Guidance for policy-makers, p. 20. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000376709.

[79] Duolingo has reported 23% increase of monthly users in 2022 (more than 42 million users) in comparison to 2021 (ca. 39 million). Available at : https://investors.duolingo.com/news-releases/news-release-details/duolingo-announces-record-bookings-first-quarter-2022-and-raises.

examples used at universities refer to the use of algorithms to identify students that are likely to fail exams by analysing big data from the university's education management information system and to later share data with the university staff to offer assistance.[80]

Some other ongoing uses of AI in education may not go farther than scheduling courses or managing the scheduling for individual students.[81] At the same time, AI is beneficial to teachers, liberating them from mundane albeit time consuming tasks such as keeping attendance records or providing repetitive answers to ordinary questions.[82]

Opportunities of AI may also be observed in public sector. As noted in the OECD Working Papers on Public Governance, in 2019, "one of the most important and most immediately achievable benefits of AI is to change the way that public servants themselves do their jobs", resulting from the focusing on high-value instead of low-value work, thus "reducing or eliminating repetitive tasks, revealing new insights from data… and enhancing agencies' ability to achieve their missions."[83]

The example of the US Bureau of Labor Statistics is one example of successful use of AI to enable staff focusing on less tedious tasks.[84]

[80] OU Analyse is a system developed at the Knowledge Media Institute of the Open University, UK, for early identification of students at risk of failing powered by machine learning methods. The project is presented at: https://analyse.kmi.open.ac.uk/project_info.

[81] UniTime is a scheduling system that supports developing course and exam timetables, managing changes to these timetables, sharing rooms with other events, and scheduling students to individual classes. The project, as well as licenses, are available at: https://www.unitime.org/.

[82] UNESCO, 2021, AI and Education: Guidance for policy-makers, p. 18. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000376709.

[83] OECD, 2019, Artificial intelligence and its use in the public sector, P.77.Available at:https://www.oecd-ilibrary.org/docserver/726fd39d-en.pdf?expires=1670969672&id=id&accname=guest&checksum=3E 6FA9EC383457223434E80471D353DA.

[84] The case was used as an example in OECD, 2019, Artificial intelligence and its use in

The statistical analysis of reported injuries and illnesses was needed to help companies as well as authorities to prevent them. The data collection assumed reading hundreds of thousands reports and assigning predefined codes to pieces of information, such as the position of an employee or a place of injury. In 2014, they started using AI to code responses referring to the occupation of those reporting illness or injury and few years later they included other code. The end result was that “the computer coded more accurately, on average, than a trained human coder”, while the Bureau’s staff could be focused on “more complicated cases that require human judgment, shifting from mind-numbing to more interesting tasks”[85].

Autonomous vehicles are far from fiction and are in fact an example of how AI may be deployed, albeit not free from numerous risks and ethical issues. As already mentioned, jobs in transportation are susceptible to being replaced by technology.[86] However, a driver free vehicle is not the only example, even though the most spoken about, of the use of AI in transportations. It is used to better manage traffic systems, with a capability to predict heavy traffic, thus avoiding those routes, taking into account delays in international transport, or even saving fuel, and assuring timely maintenance.[87]

the public sector, and in full presented in Partnership for Public Service/IBM Center for the Business of Government, 2018, The Future Has Begun, p. 10. Available at : https://www.businessofgovernment.org/sites/default/files/Using%20Artificial%20Intelligence%20to%20Transform%20Government.pdf.

[85] Partnership for Public Service/IBM Center for the Business of Government, 2018, The Future Has Begun, p. 10. Available at : https://www.businessofgovernment.org/sites/default/files/Using%20Artificial%20Intelligence%20to%20Transform%20Government.pdf.

[86] See above. Katja Grace, John Salvatier, Allan Dafoe, Baobao Zhang, Owain Evans, “When Will AI Exceed Human Performance? Evidence from AI Experts”, 3 May 2018, Journal of Artificial Intelligence Research, available at: https://arxiv.org/pdf/1705.08807.pdf.

[87] Available at: https://indatalabs.com/blog/ai-in-logistics-and-transportation.

Challenges of AI

Looking at the use of emerging technologies, in particular AI, from the perspective of human rights, the focus is more on the side of challenges it represents to the right to privacy, and there are many. Although the positive effects of AI in medicine and the above examples may not be denied, that positive attitude is not always the best one. One of the recent examples that the whole world experienced was the potential of AI tools during the Covid-19 pandemic. According to some post analysis of those predictive tools that AI community and individual researchers developed so to help struggling medical staff, "none of them made a real difference, and some were potentially harmful".[88] The explanation was the quality of data, which was poor due to the haste in which data was collected. However, it is worth noting that the quality of data is, following the articulation of the need of technology, one of the first steps in building the system.

[88] MIT Technology Review, Will Douglas Heaven, 30 July 2021, Hundreds of AI tools have been built to catch covid. None of them helped. Available at: https://www.technologyreview.com/2021/07/30/1030329/machine-learning-ai-failed-covid-hospital-diagnosis-pandemic/.

Facial recognition technology

Over the past years, the use of video surveillance with embedded facial recognition technology has rapidly grown. It is used in both private and public sector. However, this widespread use does not imply that it is appropriate. These tools are used also by law enforcement authorities and there are many examples of these technologies being tested in certain situations often limited in space or time.[89]

Observing the practice in EU Member States, but also outside, notably the USA, in their 2019 report the EU Fundamental Rights Agency concluded that there were many issues that raised concerns. Biometric data, such as the facial images, is regarded as special category of data, hence the circumstance of the processing is also subject to additional requirements. Primarily, such data may be processed only if the processing is strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject.[90] The strictly necessary requirement is not easily demonstrable. The way the technology is used is also essential as facial recognition may be used to compare images either against each other or against the whole system of recorded images of unknown number of individuals. Consequently, live facial recognition raises even more concerns. Apart from the crucial questions regarding the necessity of such intrusive technology, there are other matters to be taken into account. These refer to procedures of when the use of such technologies are allowed, the level of security and other security measures in place, including organisational ones. The latter would refer to strict control of access. Also, as in the case of

[89] FRA, 2019, Facial recognition technology: fundamental rights considerations in the context of law enforcement. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

[90] Law Enforcement Directive, Art. 10.

any processing of personal data, if such processing is permitted, data subjects must be informed, and enabled to exercise their rights, such as right to access. The supervision must be performed by an independent authority.

In August 2021, Serbian Ministry of the Interior proposed the Draft Law on Internal Affairs containing provisions that would allow for mass biometric surveillance, thus becoming "the first European country conducting permanent indiscriminate surveillance of citizens in public spaces."[91] In the open letter to the Prime Minister, as well as other officials, on behalf of several civil society organisations, the European Digital Rights noted that "such practices are highly likely to unduly restrict the rights and freedoms of large parts of the Serbian population and to constitute unjustified biometric mass surveillance practices. They treat each person as a potential suspect, and they obscure the possibility of targeted use, as passers-by are an inherent feature of public spaces."[92] The Ministry later withdrew the Draft, however, in December 2022, again proposed similar provisions in the new draft that is currently being debated.[93]

[91] EDRi, by ShareFoundation, 22 September 2021, Total surveillance law proposed in Serbia. Available at: https://edri.org/our-work/total-surveillance-law-proposed-in-serbia/.

[92] EDRi, open letter, 17 September 2022. Available at: https://www.sharefoundation.info/wp-content/uploads/EDRi-Civil-Society-consultation-on-the-proposal-for-the-Zakon-o-unutrasnjim-poslovima.pdf.

[93] BiometricUpdate.com, Alessandro Mascellino, 16 December 2022, Serbian rights group warns of implications in biometric surveillance act. Available at: https://www.biometricupdate.com/202212/serbian-rights-group-warns-of-implications-in-biometric-surveillance-act.

Cybersecurity

As noted above, cybersecurity threats are affecting the functioning of different systems regardless of whether these are controlled by private or public sectors. The need for appropriate cybersecurity strategies accompanied by action plans delegating the tasks to different stakeholders has never been more relevant. The list of emerging risks presented by The European Union Agency for Cybersecurity [94] is rather concerning as the effects thereof are significant to the rights of individuals.

The examples of recent cyberattacks are many[95] and Albania is not excluded from being exposed. Cyberattacks that occurred in the summer of 2022 resulted in all online government services being brought to a halt, thus causing significant problems for authorities, businesses, as well as individuals, with long-term solutions still pending.[96] Following the revelation that the attack was allegedly directed from the Islamic Republic Iran, Albania has since frozen all diplomatic relationship with the country. [97]

Apart from stringent rules that assume their full enforcement, it is of outmost importance to educate and equip individuals, companies, and society at large. A culture of cybersecurity, as in

[94] See above. ENISA, 11 November 2022, Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! Available at: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030.

[95] The list of references is long. Number of technology oriented media, or websites in general are providing different ratings, analyses or presentations of cyberattacks worldwide.

[96] Euractiv, Alice Taylor, 13 December 2022, Hackers continue to leak data from Albanian intelligence services. Available at: https://www.euractiv.com/section/politics/news/hackers-continue-to-leak-data-from-albanian-intelligence-services/.

[97] Euractiv, Alice Taylor, 7 September 2022, Albania has frozen all diplomatic ties with Iran and asked diplomats to leave the country. Available at: https://www.euractiv.com/section/politics/news/albania-cuts-diplomatic-ties-with-iran-over-cyberattacks/.

the case of personal data, is a prerequisite. In Autumn 2022, as a joint initiative of the OSCE Presence in Albania and the National Authority on Online Certification and Cyber Security several awareness raising activities were organised aiming at children and those responsible for their growing up and education regarding the existing threats stemming from the use of technology as well the need for data confidentiality.[98]

[98] OSCE Presence in Albania, Press Release, 2 November 2022, Cyber threats in focus of OSCE Presence information sessions with schools across Albania. Available at: https://www.osce.org/presence-in-albania/530332.

Regulating AI

Placing AI under legislative acts in not an easy task. Firstly, the use of AI is vast and legislatures aim into providing regulatory framework that could be applied to not only specific cases, but as a general rule. Secondly, legislative acts requires time for elaboration and deliberation and, since the issue is about emerging technologies there is a concrete risk that the result will not be technology neutral. Finally, many issues evolving around AI are not solely a matter of legal norms but also ethics.

In the mentioned report of the UN Human Rights Commissioner, she recommended to States to "expressly ban AI applications that cannot be operated in compliance with international human rights law and impose moratoriums on the sale and use of AI systems that carry a high risk for the enjoyment of human rights, unless and until adequate safeguards to protect human rights are in place." Similar initiatives, though pertaining to facial recognition technology, was initiated by different bodies of the European Union.[99]

[99] Joint initiative of the European Data Protection Board and the European Data Protection Supervisor, 21 June 2021, EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination. Available at: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en.

National AI Strategies

The OECD's AI Policy Observatory offers an overview of different national AI strategies, as well as incentives to businesses. Their interactive map, although not presenting all countries, is an informative way to acquaint oneself with how governments are trying to cope with this ever-emerging field.[100] Many national examples may use as succinct models to be implemented in other countries. Such is the case with the above mentioned AI and data protection toolkit prepared by the UK ICO. [101] In Canada, the government is working on Algorithmic Impact Assessments, as a tool that policymakers and other officials may use to assess and mitigate the risks associated with deploying an automated decision-making system.[102] The Austrian Council on Robotics and Artificial Intelligence, an advisory body whose mandate ended in 2021, issued a whitepaper in 2018 proposing three key elements when addressing AI – Smart Governance, Smart Innovation, and Smart Regulation.[103]

[100] OECD AI Observatory Policy. Available at: https://oecd.ai/en/. At the time of the preparation of this analysis, Albania was not presented in their Country dashboards and data.

[101] ICO, AI and data protection risk toolkit, last updated in May 2022. Available for download at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/.

[102] OECD AI Observatory Policy, data on Canada. Available at: https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-24387.

[103] Österreichischer Rat für Robotik und Künstliche Intelligenz, November 2018, White Paper des Österreichischen Rats für Robotik und Künstliche Intelligenz. Available at: https://www.acrai.at/wp-content/uploads/2020/04/ACRAI_White_Paper_DE_.pdf.

EU Framework for Trustworthy AI

The idea of addressing AI in a unique way for the European Union had a rather remarkable start. In their 2017 Resolution the European Parliament called on the Commission, when carrying out an impact assessment of its future legislative instrument, to explore, analyse and consider the implications of all possible legal solutions, including those regarding a "specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently." [Emphasis added][104]

Departing from that initial notion, the EU continued its work on AI and in April 2019, the High-Level Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence. The work is said to illustrate that Europe is "determined to revive in the AI domain the same approach followed for the GDPR, which places the fundamental right to data protection at the forefront, with no concession to data-hungry AI techniques."[105] The evident emphasis on ethics in the Framework should be seen as the overall aim thereof – to prevent negative effects of digital technology on citizens and civil society and setting a high bar for those wishing

[104] European Parliament (EP) (2017), Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), Art 59(f). Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html.

[105] Andrea Renda, "Europe: Toward a Policy Framework for Trustworthy AI", in Markus D. Dubber, Frank Pasquale and Sunit Das (eds.), *The Oxford Handbook of Ethics of IA*, OUP 2020, Oxford, p. 653.

to access EU Single Market.[106]

According to the Ethics Guidelines for Trustworthy AI, trustworthy AI has three components, present throughout to entire life cycle of the system:

1. Lawfulness, i.e., compliant with all applicable laws and regulations;

2. Ethics, i.e., adherence to ethical principles and values; and

3. Robustness, both from a technical and social perspective, since "even with good intentions, AI systems can cause unintentional harm."[107]

According to the Ethics Guidelines for Trustworthy AI, there are seven key requirements that AI systems should meet in order to be trustworthy:

1) Human agency and oversight
2) Technical robustness and safety
3) Privacy and Data governance
4) Transparency
5) Diversity, non-discrimination and fairness
6) Societal and environmental well-being
7) Accountability

The principle of human agency and oversight starts from the

[106] Andrea Renda, "Europe: Toward a Policy Framework for Trustworthy AI", in Markus D. Dubber, Frank Pasquale and Sunit Das (eds.), *The Oxford Handbook of Ethics of IA*, OUP 2020, Oxford, p. 653.

[107] High-Level Expert Group on Artificial Intelligence, 2019, Ethics Guidelines for Trustworthy AI, p. 5. Available at: file:///C:/Users/nruzic/Downloadsai_hleg_ethics_guidelines_for_trustworthy_ai-en_87F84A41-A6E8-F38C-BFF661481B40077B_60419%20(1).pdf.

premise that an assessment of the impact on fundamental rights has been carried out. This is the core of a risk-based approach. In their interaction with the AI system, persons need to know the system at the other end. Furthermore, the system must be secured from overreliance, as expectedly people may start relying on to the extent that they do not have confidence in their own knowledge or expertise.[108] Finally, human oversight must be present to the point of shutting the system down if needed.[109]

The principle of technical robustness and safety addresses the resilience of the system. Here, too, the risk-based approach in inevitable. The question is whether and how vulnerable the system is against potential cyberattacks, and if it occurs whether the system may insure reproducibility.[110]

The third principle of privacy and data governance pertains to the whole set of questions vis-à-vis the processing of personal data, even though many of the issues are also addressed through other principles. Such as the case with the principle of human agency and oversight also addressed the right to privacy and personal data protection. However, this principle also addresses for example organisational security measures regarding the authorised access to data and log files to track access and reconstruct the incident if occurred.[111]

The principle of transparency consists of three prongs – traceability, explainability, and communication. Traceability may also be

[108] This unquestionable reliance on technology is well illustrated through examples of drivers using interactive maps even for the routes well-known to them.

[109] High-Level Expert Group on Artificial Intelligence, 2019, Ethics Guidelines for Trustworthy AI, p. 26. Available at: file:///C:/Users/nruzic/Downloads/ai_hleg_ethics_guidelines_for_trustworthy_ai-en_87F84A41-A6E8-F38C-BFF661481B40077B_60419%20(1).pdf.

[110] Ibid, p. 27.

[111] Ibid, p. 28.

understood as the ability to explain how the system is developed and what methods have been used to train it. Explainability should enable an understandable explanation as to why the system took a certain choice resulting in a certain outcome that all users[112] can comprehend. Communication means ability to communicate to (end) users that they are interacting with an AI system[113] and that system is labelled as an AI system.[114]

The fifth principle of diversity, non-discrimination, and fairness should ensure the avoidance of (unfair) biases in the AI system, both regarding the use of input data as well as for the algorithm design. If should also ensure the broad participation of different stakeholders. The appropriate implementation of the AI system should consider vulnerable or other underrepresented groups.[115]The principle of societal and environmental well-being refers to impacts the AI system radiates towards society at large as well as environment. The system needs to be sustainable and environmentally friendly and should present a significant value to the society.[116]

The last, and certainly not least important, is the principle of accountability. Adherence to this principle again entails risk assessment approach. The question is how to ensure a meaningful audit of the system. It also concerns the way organisational measures are applied to secure that those that are involved in the deployment, or design of the AI system are aware of legislation as well as ethical issues. This does not refer to staff members but

[112] Here the word ‘users’ refers to all individuals involved.

[113] Note that this is also a part of the first principle.

[114] High-Level Expert Group on Artificial Intelligence, 2019, Ethics Guidelines for Trustworthy AI, p. 29. Available at: file:///C:/Users/nruzic/Downloads/ai_hleg_ethics_guidelines_for_trustworthy_ai-en_87F84A41-A6E8-F38C-BFF661481B40077B_60419%20(1).pdf.

[115] Ibid, p. 30.

[116] Ibid, p. 31.

parties such as vendors or data processors.[117]

Without trying to establish the ranking of the principles, it should be, however, noted that the principle of accountability should be always in the minds of those thinking of developing, or deploying an AI system. Should the adherence to this principle be insignificant, the other principles may as well be ignored. Therefore, insisting on accountability, or even broader on responsibility, is the key.

[117] Ibid, p. 32.

Multistakeholder Approach and Role of Data Protection Authority in AI

The EU High-Level Expert Group on Artificial Intelligence was divided into two working groups, first with the task to draft AI ethics guidelines, and second to focus on the policy and investment strategy. The Group was support by independent experts selected through an open call procedure through which more than 500 applicants expressed their desire to be involved.[118] The external expert group comprised of 52 individuals representing companies (23 members), academia (19) and civil society (10).[119]

The OECD's insights form national AI strategies provides different example of how respective countries decided to address the emerging technologies. For example, some have decided to establish an ad hoc body (similar to the EU High-Level Expert Group), others used the existing bodies, commonly within ministries competent of innovation.[120] However, whatever the formal decision has been, civil society organisations were involved, at least on a paper. In addition to this, according to their national AI policy database, the

[118] European Commission Press Release, 14 June 2018, Commission appoints expert group on AI and launches the European AI Alliance. Available at: Commission appoints expert group on AI and launches the European AI Alliance | Shaping Europe's digital future (europa.eu).

[119] European Commission, 2019, Concept Note – The High-Level Expert Group on Artificial Intelligence.

[120] OECD, June 2021, State of Implementation of the OECD AI Principles - Insights from National AI Policies, OECD Digital Economy Papers No. 311. Pp. 76-77. Available at: https://www.oecd-ilibrary.org/docserver/1cd40c44-en.pdf?expires=1672000860&id=id&accname=guest&checksum=DBA47656299F355BBD52DC97E5215DAC.

OECD emphasised the value of consultations, regardless of their formats (e.g. surveys, conferences and public hearings, workshops, focus groups, or the establishment permanent bodies to coordinate the implementation of the AI strategy).[121]

The multistakeholder approach was also emphasised in the UN High Commissioner on Human Rights report. According to her, for consultations on emerging technologies to be meaningful, they need to be "carried out with potentially affected rights holders and civil society, while experts with interdisciplinary skills should be involved in impact assessments, including in the development and evaluation of mitigations."[122] The elaboration on why other interested parties are needed in addressing artificial intelligence is well presented in UNESCO Series on Internet Freedom from 2019. According to UNESCO, this approach is needed not only at national level, but international as well due to borderless significance of technology.[123] The most important aspects of the multi-stakeholder approach are transparency, inclusion, engagement, multi-stakeholderism, bridging the divides, understanding all the participants.

Therefore, the role of data protection authorities is also inevitable. However, whether they possess capacity to take an active part is yet another issue. The then International Conference of Data Protection and Privacy Commissioners, now the Global Privacy Assembly (GPA), adopted in 2018 the Declaration on Ethics and

[121] Ibid. p. 18.

[122] UN Human Rights Council, 48th Session, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, The right to privacy in the digital age, A/HRC/48/31. Para. 50.

[123] UNESCO, 2019, Steering AI and Advanced ICTs for Knowledge Societies A Rights, Openness, Access, and Multi-stakeholder Perspective. Available at: https://www.developmentaid.org/api/frontend/cms/file/2019/11/372132eng.pdf.

Data Protection in Artificial Intelligence.[124] The data protection authorities reaffirmed "the commitment of data protection authorities and the Conference of Data Protection and Privacy Commissioners to uphold data protection and privacy principles in adapting to this evolving environment, notably by engaging resources and developing new skills in order to be prepared for future changes."[125]

Following this, the AI Working Group was established and presented its work with regard to risks for rights and freedoms at the 2020 annual conference of the GPA.[126] The report emphasised the risk-based approach as essential to taking emerging technologies and their impact on the society at large into consideration. The understanding of the notion of risk management is taken from ISO 31000 standards – "The purpose of risk management is the creation and protection of value – It improves performance, encourages innovation and supports the achievement of objectives".[127]

The report also provides the list of actors and stakeholders that should be involved in the policy making process and should also "exercise their power and influence to promote accountability for fair and responsible development and use of AI systems". These are:

[124] ICDPCC, 2018, Declaration on Ethics and Data Protection in Artificial Intelligence, adopted at 40th International Conference of Data Protection and Privacy Commissioners, on 23rd October 2018, Brussels. Available at: https://privacyconference2018.org/system/files/2018-10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.

[125] Ibid.

[126] GPA, 2022, AIWG Action Point n.6, Risks for Rights and Freedoms of Individuals Posed by Artificial Intelligence Systems - Proposal for a General Risk Management Framework.Available at: https://globalprivacyassembly.org/wp-content/uploads/2022/11/2.2.f-Report-RISKS-FOR-RIGHTS-AND-FREEDOMS-OF-INDIVIDUALS-POSED-BY-ARTIFICIAL-INTELLIGENCE-SYSTEMS-PROPOSAL-FOR-A-GENERAL-RISK-MANAGEMENT-FRAMEWORK.pdf.

[127] Ibid. p. 4.

- Regulators (Legislators, Public Authority with governance/ enforcement powers)
- Researchers (Academia, Public and private research entities)
- Standards Organizations (developing standards and best practices)
- Producers and Providers (Designers and developers of algorithms, software and related data structure for machine learning human interfaces and actuators, system integrator, producers of system and providers of services, data providers - (Combine Designers, Producers, Operators,
- End users (as users of AI systems)[128]

The AI Working Group was also tasked to assess the capacity and expertise of data protection authorities that was done through a survey presented to the GPA in 2022.[129] According to the analysis,[130] the vast majority considered knowledge sharing and capacity building between authorities at regional or international level relevant, while the main challenges, alongside those regarding regulatory framework, were "the lack of sufficient human, material and financial resources.[131]

[128] Ibid. p. 8.

[129] GPA, 2022, AIWG, Report – July 2022. Available at: https://globalprivacyassembly.org/wp-content/uploads/2022/11/2.2.f.-Ethics-and-Data-Protection-in-AI-Working-Group-English.pdf.

[130] In total the AIWG received 38 responses, majority coming from European authorities. In this respect, the finding should be taken with reservations.

[131] GPA, 2022, AIWG, Report – July 2022, pp. 7-8. Available at: https://globalprivacyassembly.org/wp-content/uploads/2022/11/2.2.f.-Ethics-and-Data-Protection-in-AI-Working-Group-English.pdf.

Concluding Observations/ Recommendations

It is obvious that the author has been more focused on the challenges of artificial intelligence in the present analysis. One reason of such an approach is that there is a track record of cases not necessarily involving emerging technologies in which there has been an obvious lack of risk assessment, but also need assessment. Another reason is that being a human right lawyer, the question asked is who may be held accountable, or at least responsible, in cases where technology was designed or deployed in means largely detrimental to the public good. The question remains both for cases of intentional and unintentional misuse. As in the case of data protection principles, the basic principle of the ethical use of AI is accountability.

However, claiming that AI does not contribute to societal, as well as individual, development would be patently untrue. After all, the very preparation of this analysis has been supported by AI embedded in the code of the tools used for it.

Assessing the preparedness of state institutions and citizens of a country to anticipate any human rights risks that may result from the use of emerging technologies must start with data protection frameworks. Firstly, the data, of some sort, is essential for the use of any technology. As noted, the poor quality of data usually results in poor analytics and unreliable decisions. Secondly, what is more important than the quality of data is how data is collected. For that, in cases where data refers to personal data, data protection legislation is the foundation on which all other activities will depend. Finally, the risk-based approach contained in all existing international and national instruments addressing artificial intelligence may be seen as an advanced data protection impact assessment.

It is the opinion of the author that at the current stage, considering that the data protection regulation in the country is not in compliance with GDPR and the numerous recent cases of data breaches, that the reform of the data protection framework should be regarded as the basis towards examining the readiness to implement advanced technologies in any systemic way. In addition, relying on the findings of the General Privacy Assembly, the need for knowledge sharing as well as providing sufficient human, material and financial resources to the data protection authority should be addressed.

However, a data protection authority is just one of the stakeholders that should be engaged in the assessment of the country's preparedness to deploy emerging technologies. The group of stakeholders, according to the UNESCO's concept of multistakeholderism for AI, should be inclusive, diverse, collaborative, transparent, equal, flexible and relevant, safe and private, accountable and legitimate, as well as responsive.

Taking into account the different groups of stakeholders listed in the GPA's document, a data protection authority is just one of the authorities identified as regulators. Regulators are also the Government, respective ministries (e.g. competent for science, innovation, technology, or education), Parliament (i.e. respective committees or an ad hoc bodies) as well as other authorities (e.g. Ombudsperson or Equity Commissioners, as well as other agencies). As noted above, apart from the regulators, academia and researchers in a broad sense should also be involved in shaping the policy pertaining to the use of artificial intelligence. Due to the impact on human rights, civil society organisations should be given the opportunity to provide their inputs most notably those dealing with human rights, and in particular digital rights, as well as with vulnerable groups (e.g. youth, elderly, or migrants).

The initiatives to address AI so far also involved representatives of the business sector, for at least two reasons. First, as these emerging technologies are generally developed by this sector, hence the insight is best presented by them. Secondly, the idea of policy making is not to prohibit the use of technology but to understand its reach as well as to direct it to better serve the society.

Another issue to consider is which entity should take the lead in gathering such a group of different actors. There are many examples of how countries have chosen their own modus operandi, either through parallel initiatives, centralised or even through the establishment of a tasked body to prepare the starting points. What is common to all, albeit with no equal outcomes, is the engagement of other stakeholders, as well as the public consultations.

List of Resources

All internet pages listed are last visited on 17 December 2022.

Bibliography

- Katja Grace, John Salvatier, Allan Dafoe, Baobao Zhang, Owain Evans, “When Will AI Exceed Human Performance? Evidence from AI Experts”, 3 May 2018, Journal of Artificial Intelligence Research, available at: https://arxiv.org/pdf/1705.08807.pdf.

- Carl Benedikt Frey and Michael A. Osborne, “The Future of Employment: How Susceptible are Jobs to Computerisation?”, September 2013, Oxford Martin Programme on Technology and Employment. Available at: https://www.oxfordmartin.ox.ac.uk/downloads/academic/future-of-employment.pdf.

- Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, Handbook on European data protection law: 2018 edition, Publications Office of the European Union, 2019. Available at: https://data.europa.eu/doi/10.2811/343461.

- Documentary “Democracy: Im Rausch der Daten“ by David Bernet, 2015.

- Douwe Korff and Marie Georges, The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, As approved by the Commission, July 2019.

- Megan Lewis, “An artificial intelligence tool that can help detect melanoma”, Institute for Medical Engineering and Science, April 2, 2021, available at: https://news.mit.edu/2021/artificial-intelligence-tool-can-help-detect-melanoma-0402.

- Brasil S, Pascoal C, Francisco R, dos Reis Ferreira V, A. Videira P, Valadão G. Artificial Intelligence (AI) in Rare Diseases: Is the Future Brighter? Genes. 2019, 10(12):978, available at: https://doi.org/10.3390/genes10120978.
- Andrea Renda, "Europe: Toward a Policy Framework for Trustworthy AI", in Markus D. Dubber, Frank Pasquale and Sunit Das (eds.), *The Oxford Handbook of Ethics of IA*, OUP 2020, Oxford.
- Nevena Ruzic, Nationalising the General Data Protection Regulation in Western Balkan, in Regional Law Review 2021. Available at: https://rlr.iup.rs/archives/year-2021.

International Documents

- Council of Europe – Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181), adopted in 2001, in force since July 2004.
- Council of Europe – Conference Convention 108 + And the future data protection global standard, 2019. Available at: https://www.coe.int/en/web/data-protection/convention-108-and-the-future-data-protection-global-standard.
- Council of Europe – Venice Commission, CDL(2020)037, 11 December 2020, Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes. Available at:https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2020)037-e.
- EU – Article 29 Working Party (2017), Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, last revised and adopted 5 April 2017. Available at: https://ec.europa.eu/newsroom/article29/items/612048/en.

- EU – Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), adopted on 22 August 2018, approved by EDPB on 25 May 2018. Available at: https://ec.europa.eu/newsroom/article29/items/612053/en.
- EU–Adequacy Decisions: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
- EU – Charter of Fundamental Rights of the European Union, 2012/C 326/02.
- EU – C-362/14 Maximillian Schrems v Data Protection Commissioner, Joined Party Digital Rights Ireland Ltd, ECLI:EU:C:2015:650
- EU – C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (called "Schrems II case"), ECLI:EU:C:2020:559
- EU – Draft decision Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (dated 13 December 2022) is available: https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf.
- EU – EDPB, Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
- EU – EESC, 2017, "Artificial Intelligence – The consequences of artificial intelligence on the (digital) single market, production,

consumption, employment and society (own-initiative opinion)", adopted on 31/05/2017, Reference: INT/806-EESC-2016-05369-00-00-AC-TRA, Official Journal: OJ C 288, 31.8.2017. Available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/artificial-intelligence-consequences-artificial-intelligence-digital-single-market-production-consumption-employment-and.

- EU – ENISA, 11 November 2022, Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! Available at: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030.
- EU – European Commission, 2018, Albania 2018 Report, 17.4.2018., SWD(2018) 151 final, available at: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-albania-report.pdf,
- EU – European Commission, 2020, Albania 2020 Report, 6.10.2020, SWD(2020) 354 final, available at: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/albania_report_2020.pdf.
- EU – European Parliament (EP) (2017), Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html.
- EU – Decision of the Council and the Commission of 13 December 1993 on the conclusion of the Agreement on the European Economic Area between the European Communities, their Member States and the Republic of Austria, the Republic of Finland, the Republic of Iceland, the Principality of Liechtenstein, the Kingdom of Norway, the Kingdom of Sweden and the Swiss Confederation, OJ 1994 L 1.
- EU – Directive (EU) 2016/680 of the European Parliament and of

the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, L 119/89. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN.

- EU – FRA, 2019, Facial recognition technology: fundamental rights considerations in the context of law enforcement. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.
- EU – High-Level Expert Group on Artificial Intelligence, 2019, Ethics Guidelines for Trustworthy AI. Available at: file:///C:/Users/nruzic/Downloads/ai_hleg_ethics_guidelines_for_trustworthy_ai-en_87F84A41-A6E8-F38C-BFF661481B40077B_60419%20(1).pdf.
- EU – Joint initiative of the European Data Protection Board and the European Data Protection Supervisor, 21 June 2021, EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination. Available at: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en.
- EU – 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), L 119/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

- EU – Stabilisation and Association Agreement between the European Communities and their Member States of the one part, and the Republic of Albania, of the other part, 2009, O.J. (L107). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22009A0428(02).
- GPA, 2022, AIWG Action Point n.6, Risks for Rights and Freedoms of Individuals Posed by Artificial Intelligence Systems - Proposal for a General Risk Management Framework. Available at: https://globalprivacyassembly.org/wp-content/uploads/2022/11/2.2.f-Report-RISKS-FOR-RIGHTS-AND-FREEDOMS-OF-INDIVIDUALS-POSED-BY-ARTIFICIAL-INTELLIGENCE-SYSTEMS-PROPOSAL-FOR-A-GENERAL-RISK-MANAGEMENT-FRAMEWORK.pdf.
- GPA, 2022, AIWG Report – July 2022. Available at: https://globalprivacyassembly.org/wp-content/uploads/2022/11/2.2.f.-Ethics-and-Data-Protection-in-AI-Working-Group-English.pdf.
- ICDPCC, 2018, Declaration on Ethics and Data Protection in Artificial Intelligence, adopted at 40th International Conference of Data Protection and Privacy Commissioners, on 23rd October 2018, Brussels. Available at: https://privacyconference2018.org/system/files/2018-10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.
- OECD, 2019, Artificial intelligence and its use in the public sector. Available at: https://www.oecd-ilibrary.org/docserver/726fd39d-en.?expires=1670969672&id=id&accname=guest&checksum=3E6FA9E C383457223434E80471D353DA.
- OECD AI Observatory Policy. Available at: https://oecd.ai/en/.
- OECD, June 2021, State of Implementation of the OECD AI Principles - Insights from National AI Policies, OECD Digital Economy Papers No. 311. Available at: https://www.oecd-ilibrary.org/

docserver/1cd40c44-en. pdf?expires=1672000860&id=id&accname=guest&checksum=DBA47656299F355BBD52DC97E5215DAC

- OSCE ODIHR, Artificial Intelligence and Human Rights: 2022 NHRI Academy. Video and programme available at: https://www.osce.org/odihr/2022NHRIAcademy.

- OSCE Presence in Albania, Press Release, 2 November 2022, Cyber threats in focus of OSCE Presence information sessions with schools across Albania. Available at: https://www.osce.org/presence-in-albania/530332.

- UN Human Rights Council, 48th Session, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, The right to privacy in the digital age, A/HRC/48/31.

- UNESCO, 2019, Steering AI and Advanced ICTs for Knowledge Societies A Rights, Openness, Access, and Multi-stakeholder Perspective. Available at: https://www.developmentaid.org/api/frontend/cms/file/2019/11/372132eng.pdf.

- UNESCO, 2021, AI and Education: Guidance for policy-makers, available at: https://unesdoc.unesco.org/ark:/48223/pf0000376709.

- UK – ICO, AI and data protection risk toolkit, last updated in May 2022. Available for download at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/.

- Austria – Österreichischer Rat für Robotik und Künstliche Intelligenz, November 2018, White Paper des Österreichischen Rats für Robotik und Künstliche Intelligenz. Available at: https://www.acrai.at/wp-content/uploads/2020/04/ACRAI_White_Paper_DE_.pdf.

Online Media and other Online References:

- A2 (CNN), 22 December 2021, Private information about salary of 630,000 Albanians leaked online. Available at: https://english.a2news.com/2021/12/22/private-information-about-salary-of-630000-albanians-leaked-online/.

- AIThority, Omar Arab, 10 September 2020, Reimagining Banking's Customer Experience for the Digital Era. Available at: https://aithority.com/technology/financial-services/reimagining-bankings-customer-experience-for-the-digital-era/.
- Article 19, an Open Letter to Mr. Besnik Dervishi, Commissioner for the Right to Access to Information and Personal Data Protection, on 09 May 2022, sent electronically. Available at: https://www.article19.org/resources/albania-data-breaches-and-intimidation-of-journalists-must-be-investigated/.
- Banisar, D., October 2022, National Comprehensive Data Protection/Privacy Laws and Bills 2022. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416.
- BiometricUpdate.com, Alessandro Mascellino, 16 December 2022, Serbian rights group warns of implications in biometric surveillance act. Available at: https://www.biometricupdate.com/202212/serbian-rights-group-warns-of-implications-in-biometric-surveillance-act.
- BIRN, Gjergj Erebara, 21 April 2021, Police, Soldiers among Albanian Ruling Party's Voter Tracking 'Army'. Available at: https://balkaninsight.com/2021/04/21/police-soldiers-among-albanian-ruling-partys-voter-tracking-army/.
- CNBC, Arjun Kharpal, 13 January 2015, Facebook knows you better than your family. Available at: https://www.cnbc.com/2015/01/13/facebook-knows-you-better-than-your-family.html.
- Computer Weekly, Alex Scroxton, 7 October 2020, ICO wraps up Cambridge Analytica investigation. Available at: https://www.computerweekly.com/news/252490206/ICO-wraps-up-Cambridge-

Analytica-investigation.

- DataBreaches.net, 7 January 2022, Albania arrests four over massive personal data leak. Available at: https://www.databreaches.net/albania-arrests-four-over-massive-personal-data-leak/.
- Duval Guillaume YouTube channel, Amazing mind reader reveals his 'gift', uploaded on 24 September 2012. Available at: https://www.youtube.com/@duvalguillaume/about.
- Deloitte, 2021, Artificial intelligence: Transforming the future of banking. Available at: https://www2.deloitte.com/us/en/pages/consulting/articles/ai-in-banking.html.
- EDRi, by ShareFoundation, 22 September 2021, Total surveillance law proposed in Serbia. Available at: https://edri.org/our-work/total-surveillance-law-proposed-in-serbia/.
- EDRi, open letter, 17 September 2022. Available at: https://www.sharefoundation.info/wp-content/uploads/EDRi-Civil-Society-consultation-on-the-proposal-for-the-Zakon-o-unutrasnjim-poslovima.pdf.
- Euractiv, Alice Taylor, 13 December 2022, Hackers continue to leak data from Albanian intelligence services. Available at: https://www.euractiv.com/section/politics/news/hackers-continue-to-leak-data-from-albanian-intelligence-services/.
- Euractiv, Alice Taylor, 7 September 2022, Albania has frozen all diplomatic ties with Iran and asked diplomats to leave the country. Available at: https://www.euractiv.com/section/politics/news/albania-cuts-diplomatic-ties-with-iran-over-cyberattacks/.
- Forbes, Carly Page, 30 October 2020, Marriott Hit With £18.4 Million GDPR Fine Over Massive 2018 Data Breach. Available at: https://www.forbes.com/sites/carlypage/2020/10/30/marriott-hit-with-184-million-gdpr-fine-over-massive-2018-data-

breach/?sh=72f03b09e4b0.

- Geneva Internet Platform, DigWatch, “Artificial Intelligence”, available at: https://dig.watch/technologies/artificial-intelligence/.
- MIT Technology Review, Will Douglas Heaven, 30 July 2021, Hundreds of AI tools have been built to catch covid. None of them helped. Available at: https://www.technologyreview.com/2021/07/30/1030329/machine-learning-ai-failed-covid-hospital-diagnosis-pandemic/.
- NL Times, 17 November 2022, Dutch government will stop using Facebook if it doesn’t improve private data handling. Available at: https://nltimes.nl/2022/11/19/dutch-government-will-stop-using-facebook-doesnt-improve-private-data-handling.
- OneTrust Data Guidance, 12 May 2022, Hungary: NAIH fines Budapest Bank record HUF 250M fine for unlawful AI analysis of customer calls. Available at: https://www.dataguidance.com/news/hungary-naih-fines-budapest-bank-record-huf-250m-fine.
- Partnership for Public Service/IBM Center for the Business of Government, 2018, The Future Has Begun. Available at : https://www.businessofgovernment.org/sites/default/files/Using%20Artificial%20Intelligence%20to%20Transform%20Government.pdf.
- Portugal News, 12 December 2022, €4.3 million fine for breaching data protection rules in the Census. Available at: https://www.theportugalnews.com/news/2022-12-12/43-million-fine-for-breaching-data-protection-rules-in-the-census/72883.
- Privacy by Design – The 7 Foundational Principles, available at: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.
- Privacy Company, Data protection impact assessment on the processing of personal data on government Facebook Pages, Version

1.0, 16 November 2022. Available at: https://www.privacycompany.eu/blogpost-en/dpia-on-government-use-of-facebook-pages-seven-high-data-protection-risks.

- Privacysense.net, Privacy by Design, (November 28, 2017, last updated on May 12, 2022), available at: https://www.privacysense.net/terms/privacy-by-design/.
- PwC, 2017, Sizing the prize – What's the real value of AI for your business and how can you capitalise?, available at: https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf.
- Rolling Stone, Nancy Dillon, 13 January 2022, 'Nevermind' Baby Is Still Suing Nirvana, available at: https://www.rollingstone.com/music/music-news/nevermind-baby-is-still-suing-nirvana-1284031/.
- Tearsheet, Tanaya Macheel, 20 March 2018, HSBC is using AI to personalize its rewards program. Available at: https://tearsheet.co/artificial-intelligence/hsbc-is-using-ai-to-personalize-its-rewards-program/.
- The Economic Times, Stephanie Bodoni, 31 December 2020, 12-yr-old London girl can sue TikTok for privacy breach, court grants anonymity. Available at: https://economictimes.indiatimes.com/magazines/panache/12-yr-old-london-girl-can-sue-tiktok-for-privacy-breach-court-grants-anonymity/articleshow/80046082.cms.
- The Verge, taken from Le Figaro, Amar Toor, 2 March 2016, French police tell parents to stop posting Facebook photos of their kids. Available at: https://www.theverge.com/2016/3/2/11145184/france-facebook-kids-photos-privacy.
- Transparency International, Albania: Alarm over Indications of Personal Data Breach, Election Campaign Violations, 22 April 2021. Available at: https://www.transparency.org/en/press/albania-alarm-over-indications-of-personal-data-breach-election-campaign-violations.