https://doi.org/10.12697/JI.2021.30.12

Paloma Krõõt Tupay

Lecturer
of Constitutional Law
University of Tartu

Martin Ebers

Associate Professor
of IT Law
University of Tartu

Jakob Juksaar

Consultant
Northern District
Prosecutor's Office

Kea Kohv

Cybersecurity Legal Advisor
Estonian Ministry of
Economic Affairs
and Communications

Is European Data Protection Toxic for Innovative AI?

An Estonian Perspective[*1]

1. Introduction

Data constitute the lifeblood of Artificial Intelligence (AI).[*2] To fulfil their function, AI systems need data as a source for their learning. Big Data, which refers to the exponential growth in the volume of digital data, has been a key element in enabling the rapid development of successful AI applications. In turn, the development of AI systems based on machine learning[*3] fosters the creation of vast datasets. As machine learning sees more and more extensive deployment, it magnifies the ability to use personal information in ways that may impinge on the rights of the individual.[*4] For example, while an AI tool used by law-enforcement

1 This work has been supported by the research project 'Machine learning and AI powered public service delivery', RITA 1/02-96-04, funded by the Estonian government.

2 No legal definition of AI has yet been set forth in EU hard law. The Artificial Intelligence Act proposal of the European Commission published in April 2021 offers the following definition for AI: 'Software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.' See Commission, 'Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM (2021) 206 final, art 3(1). For different definitions, cf Sofia Samoili and others, 'AI Watch: Defining Artificial Intelligence –. Towards an operational definition and taxonomy of artificial intelligence' (Publications Office of the European Union 2020) EUR 30117 EN <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC118163/jrc118163_ai_watch._defining_artificial_intelligence_1.pdf> accessed 1 July 2021. According to the definition proposed by Estonia's AI Taskforce, AI 'includes systems that exhibit intelligent behaviour by analysing their environment and making decisions that are somewhat independent to meet certain objectives'. 'Report of Estonia's AI Taskforce' (May 2019) 7 <https://f98cc689-5814-47ec-86b3-db505a7c3978.filesusr.com/ugd/7df26f_486454c9f32340b28206e140350159cf.pdf> accessed 1 July 2021.

3 Machine learning (ML) consists of a set of mathematical techniques at the intersection of algorithmic, statistical learning and optimisation theory that are aimed at extracting information from a set of examples (images, sensor records, text, etc.) for purposes of solving a problem related to said data (classification, recognition, generation, etc.). High-Level Expert Group on Artificial Intelligence, 'A Definition of AI: Main Capabilities and Scientific Disciplines' (2019) 3 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341> accessed 1 July 2021; Ronan Hamon, Henrik Junklewitz, and Ignacio Sanchez, 'Robustness and Explainability of Artificial Intelligence – from Technical to Policy Solutions' (Publications Office of the European Union 2020) 10 <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC119336/dpad_report.pdf> accessed 1 July 2021.

4 Martin Ebers, 'Regulating AI and Robotics: Ethical and Legal Challenges' in Martin Ebers and Susana Navas (eds), *Algorithms and Law* (CUP 2020) 63: '[P]ersonal data is increasingly both the source and the target of AI applications.' – DOI: https://doi.org/10.1017/9781108347846.003. See also European Parliamentary Research Service, 'The Impact of the

officers to analyse biometric data[*5] for facial recognition and emotion detection may serve as an efficient mechanism for identifying offenders, such use of AI may, at the same time, lead to discrimination and false accusations.

Unlike those for data protection, the international, national, and regional regulatory frameworks for AI are still at an early stage of development, and no consensus exists yet on how AI should be regulated. However, change is afoot: at EU level, the European Commission published the first-ever proposal for a legal framework on AI, the Artificial Intelligence Act, on 21 April 2021.[*6]

This paper examines, from the perspective of Estonia as an EU member state in the broader sense and from the Estonian national perspective in the narrower sense, the extent to which the application of AI systems is possible while respect is maintained for privacy and the personal-data protection rights[*7] guaranteed by EU and Estonian law.

2. Regulating personal data's protection in the EU: How much space for AI?

The rapid expansion of the Internet in the mid-1990s called for a legal response to regulate associated risks, particularly those to the right to privacy. In 1995, the EU adopted its first general data-protection act, the European Union Data Protection Directive, covering both private actors and the public sector.[*8] The EU data-protection reform of 2016 and the adoption of the General Data Protection Regulation (GDPR) involved more than a revision of the 1995 Data Protection Directive: the GDPR has been designed to keep up with technological and socioeconomic changes while guaranteeing fundamental rights and providing people with means to exercise control over their personal data.[*9]

2.1. The GDPR

As an EU regulation, the GDPR applies directly in all member states, as well as outside the EU to all companies that offer goods or services to customers or businesses in the EU.[*10] Public institutions too are subject to the rules of the GDPR, when processing personal data, except when said data are being processed for the purposes of prevention, investigation, or detection of criminal offences; prosecution for them; or the execution of criminal-law penalties, which falls within the scope of the Data Protection Law Enforcement Directive (or Law Enforcement Directive).[*11] Although the GDPR applies to all processors of personal data, public-sector entities may take advantage of many exceptions that are not available for activities in the private sector. Most notably, nearly half of the articles of the GDPR comprise so-called opening clauses that allow member states to substantiate, supplement, or modify the regulatory content of the respective

General Data Protection Regulation (GDPR) on Artificial Intelligence' (2020) 1 <www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> accessed 1 July 2021.

5 'Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data' per 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, GDPR) [2016] OJ L119, art 4(14).

6 See n 2 and the paper's sub-s 2.2, on a proposal for the regulation of artificial intelligence.

7 Art 4(1) GDPR defines personal data as any information related to an identified or identifiable natural person, one who can be identified, directly or indirectly – in particular, by reference to an identifier.

8 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive).

9 Lilian Mitrou, 'Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?' (2019) 26. – DOI: https://doi.org/10.2139/ssrn.3386914.

10 Art 3 GDPR.

11 Art 2(d) GDPR; 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 (Data Protection Law Enforcement Directive) [2016] OJ L119.

provision.[*12] Some of the opening clauses extend across multiple articles or even allow the restriction of numerous principles for the sake of public interest, national security, *et cetera*.[*13] For this reason, the GDPR has been deemed an 'atypical hybrid of a regulation and a directive'.[*14]

2.1.1. Automated decision-making

The GDPR specifically addresses automated individual-specific decision-making – including decisions generated by means of AI – and articulates the right of the data subject not to be subject to decisions that are based solely on automated processing without human intervention.[*15] Appealing to the GDPR, people may object to automated decisions made about them.

However, the GDPR does specify as an exception that fully automated decision-making may, *inter alia*, be allowed by EU or member state's law on condition that the law lays down 'suitable measures to safeguard the data subject's rights and freedoms and legitimate interests'.[*16] An exception of this nature can be found in § 15[1] of the Estonian Social Welfare Act[*17], which allows automated processing of data of persons aged 16 to 26 for purposes of identifying young people who are not in an employment, education, or training relationship (the so-called NEET youth). According to the law's explanatory memorandum, the amendment permits the use of information-technology solutions (incl. algorithms) in aims of analysing young citizens' eligibility for social benefits and their possible need for help.[*18] The system foresees no specific measures to safeguard the data subject's rights. In the opinion of the legislator, the right of the data subject to object to further data-processing when contacted by the municipality provides sufficient protection.[*19] Still, under this law, the name and identity code of those young persons who decline further data-processing shall be recorded in the database until the relevant person's 27th birthday. The Estonian Data Protection Inspectorate's director general and also Estonia's Chancellor of Justice have criticised the amendment, stating that interference in the private life of a norm's addressees requires there to exist a concrete danger to a legally protected right.[*20] However, the legality of the law has not been contested in court.

2.1.2. General data-protection principles

The use of AI and Big Data systems pose unique challenges connected with the GDPR. Some scholars have stated that, while Big Data technologies are evolving and innovation is encouraged on global scale, the GDPR has created a legal framework within the EU that establishes unnecessary boundaries, ultimately inhibiting innovation.[*21]

The terms of the GDPR regarding data-processing are based on seven principles[*22], five of which are particularly relevant for discussion of AI systems.[*23] These are described below.

12 Jürgen Kühling and Mario Martini, 'Die Datenschutz-Grundverordnung – Revolution oder Evolution im Datenschutzrecht im europäischen und nationalen Datenschutzrecht?' (2016) EuZW 448, 450.

13 Ibid; see, for example, art 23 GDPR.

14 Kühling and Martini (n 12) 449.

15 Art 22 GDPR.

16 Art 22(2)(b) GDPR.

17 English translations of Estonian legal acts are available from the Estonian Ministry of Justice's official journal: 'Riigi Teataja' (2021) <www.riigiteataja.ee/en/> accessed 1 July 2021.

18 Ministry of Social Affairs, 'Seletuskiri sotsiaalhoolekande seaduse ja maksukorralduse seaduse muutmise seaduse eelnõu juurde' ['Explanatory Memorandum to the Draft Law Amending the Social Welfare Act and Taxation Act'] 17 <https://m.riigikogu.ee/download/dfe1c650-c7ac-4af8-a0c4-023a721c7945> accessed 1 July 2021.

19 Ibid.

20 Paloma Krõõt Tupay, 'Estonia, the Digital Nation – Reflections of a Digital Citizen's Rights in the European Union' (2020) VI European Data Protection Law Review 14. – DOI: https://doi.org/10.21552/edpl/2020/2/16.

21 Tal Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 996. Abstract at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646> accessed 1 July 2021.

22 Art 5 GDPR.

23 Accuracy, storage limitations, confidentiality, and the accountability principle are not addressed in this article.

2.1.2.1. Limitation of purpose

The purpose-limitation principle requires data to be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[*24] The purpose must be stated at the time of the collection of data. Importantly, the principle of purpose limitation conflicts with the way Big Data material is collected and used, which is characterised by collecting vast quantities of data whilst the methods of analysis and the specific purpose of the data-handling are determined only during or after collection.[*25] Furthermore, the purpose-limitation principle requires the purpose to be indicated unambiguously. A purpose statement such as 'to improve the service' is not deemed specific enough.[*26] In practice, however, often neither the data controller nor the data subject knows at the time of data collection what exact purposes the processing might serve in future.

The GDPR establishes an exception to the purpose-limitation principle by allowing further processing for 'statistical purposes', an aim not considered incompatible with the initial purposes, whatever those may be.[*27] This offers some leeway for the use of Big Data and machine learning, as the latter is often statistical in nature and employed for statistical purposes with existing datasets (one example is the use of logistic regression for the classification of data). On the other hand, the GDPR states that results of data-processing performed for statistical purposes must not be 'used in support of measures or decisions regarding any particular natural person'.[*28] The specific safeguards applied to processing for statistical purposes are to be regulated by the EU's member states.[*29] According to the GDPR, pseudonymisation may ensure the protection of data subjects' rights and freedoms in this regard.[*30] Some argue that this inhibits the use of Big Data, in that pseudonymisation reduces the usefulness of the result of the data processing,[*31] while others see this approach as the legislators' way of enabling the use of Big Data analysis.[*32]

The most important exceptions to the purpose-limitation principle can be derived from Art. 6(2) and (3) GDPR, whereby member states are allowed to maintain or introduce specific provisions for application of the GDPR within the framework of public administration[*33], while derogation based on Art. 6(3) GDPR may be laid down also by EU law.

Implementation of the Estonian Once-Only Principle (OOP) constitutes one such derogation. According to this principle, which is laid down by law,[*34] the state should request any given piece of information from a private person only once. Information obtained from private parties must, therefore, be managed by the state in such a way that it can be accessed by other public agencies when needed. In essence, the principle represents the reusability of citizens' data in state databases. Following on from the success of the

24 Art 5(1)(b) GDPR.

25 Zarsky (n 21) 1006–1007.

26 Recital (39) GDPR; Michèle Finch and Asia Biega, 'Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems' (2021) Max Planck Institute for Innovation and Competition (research paper series) 1. – DOI: https://doi.org/10.2139/ssrn.3749078. See also Article 29 Data Protection Working Party (Art 29 WP), 'Opinion 03/2013 on Purpose Limitation (WP 203)' (2013) 00569/13/EN 16.

27 Art 5(1)(b) GDPR.

28 Recital (162) GDPR.

29 Recital (162) GDPR: 'Union or Member State law should [...] determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality.'

30 Art 89(1) GDPR: 'Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.' According to art 4(5) GDPR '[p]seudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information'.

31 Zarsky (n 21) 1008. Identifiable data are data that can be attributed to an identified or identifiable natural person. When pseudonymisation is employed, personal data cease to be identifiable data without the use of additional information, provided that said additional information is maintained separately and is subject to appropriate technical and organisational measures. See art 4(5) GDPR.

32 Viktor Mayer-Schönberger and Yann Padova, 'Regime Change? Enabling Big Data through Europe's New Data Protection Regulation' (2016) XVII Columbia Science & Technology Law Review 329 <www.researchgate.net/publication/303665079_Regime_Change_Enabling_Big_Data_Through_Europe's_New_Data_Protection_Regulation> accessed 1 July 2021.

33 See Boris P Paal, Daniel A Pauly, and Eike Michael Frenzel's annotations to art 6 GDPR in *Beck'scher Online-Kommentar*, marginal notes 32–33, 42–44; Jürgen Kühling and Benedikt Buchner's annotations to art 6 GDPR in *Beck'scher Online-Kommentar*, marginal notes 194–98.

34 Public Information Act (Avaliku teabe seadus) RT I, 15.03.2019, para 43^1 s 3.

Once-Only Principle, the European Commission has devised a proposal to implement the OOP for public services by 2023.[*35]

It follows from the above that, on foundations of Art. 6(2)-(3) GDPR, an exemption for the application of AI systems based on the processing of personal data in public administration may be created by national or EU law.[*36] However, the regulation of derogations in light of the given opening clauses raises various legal questions that have not yet been answered. On the one hand, with regard to derogation by the member states, it is unclear whether each of the opening clauses, which are similar in their respective content, constitutes an independent legal basis or, rather, they must be applied cumulatively.[*37] On the other hand, the scope of possible exceptions based on Art. 6(2)-(3) GDPR[*38] is unclear.[*39] For example, is it possible to derogate freely from the data-processing principles regulated in Art. 5 GDPR such that these principles do not apply in the context of the public administration? Or must such exceptions remain faithful to the principles of the GDPR to a certain extent?[*40] There is still much need for discussion to answer these questions within the EU.[*41]

According to Art. 6(4) GDPR, processing for another purpose is lawful on the condition that the new purpose is compatible with the original one. The GDPR requires, alongside other evaluations, considering the reasonable expectations of the data subjects with regard to the usage of their data, as well as the consequences of the new processing, when one is assessing the compatibility of the previous and the latter purpose.[*42]

Finally, GDPR Art. 6(4) allows further processing of collected data if said processing is based on member state or EU law that represents 'a necessary and proportionate measure in a democratic society' to safeguard the important interests of the state as listed in Art. 23(1) GDPR.[*43] In this respect, the question of the relationship between Art. 6(4) and possible exceptions based on Art. 6(2) and (3) arises.

Furthermore, the European Data Protection Supervisor (EDPS) has noted that Art. 6(4) GDPR does not grant 'open-ended permission to enact any sweeping and generic legislative text to allow for unlimited reuse of personal data across government departments' and that the reuse of data under the OOP needs to be fully aligned with the principles of data protection.[*44] According to the EDPS, easing the administrative burden on individuals or organisations, increasing the efficiency of administrative procedures, and saving time and resources do not constitute separate grounds under Art. 23(1) GDPR for restricting the principle of purpose limitation.[*45]

As can be seen, there are several legal ways to enable the use of AI systems (especially in the public domain) by making use of an exemption from the purpose-limitation principle. However, the unclear wording of the exception clauses renders it difficult to assess the extent to which public administrations may rely on them when using AI systems.[*46]

35 Commission and Connecting Europe Facility Digital, 'Once-Only Principle (OOP)' <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle> accessed 1 July 2021. The once-only principle is designed to allow public administrations in Europe to reuse, or share, data and documents that people have already supplied, in a transparent and secure manner, by 2023. Some public administrations have already implemented this principle, among them Estonia's.

36 In essence, art 22(2)(b) GDPR also allows member-state law to circumvent the restriction on automated individual-specific decision-making. See section 2.1.1 of this paper, on automated decision-making.

37 Kühling and Büchner (n 33) marginal note 195ff; Marion Albers and Raoul-Darius Veit's annotations to art 6 GDPR in *Beck'scher Online-Kommentar,* Datenschutzrecht, marginal notes 59–62.

38 Art 6(4) GDPR.

39 Paal and others (n 33) marginal notes 32, 43.

40 See also Marion Albers and Raoul-Darius Veit's annotations to art 6 GDPR in *Beck'scher Online-Kommentar*, Datenschutzrecht, marginal note 56.

41 Mario Martini and Michael Wenzel, 'Once Only Versus Only Once: Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit' [2017] DVBI 2017, 749, 758. – DOI: https://doi.org/10.1515/dvbl-2017-1206.

42 Mitrou (n 9) 48; recital (50) GDPR.

43 Art 6(2) and (3) GDPR.

44 European Data Protection Supervisor, 'Opinion 8/2017: EDPS Opinion on the Proposal for a Regulation Establishing a Single Digital Gateway and the "Once-Only" Principle' (2017) 7, 10 <https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en_0.pdf> accessed 1 July 2021.

45 European Data Protection Supervisor, 'A Digital Europe Needs Data Protection' (2017) 6, 10 <https://edps.europa.eu/press-publications/press-news/press-releases/2017/digital-europe-needs-data-protection-0_en> accessed 1 July 2021.

46 Paal and others (n 33) marginal notes 32, 43; Martini and Wenzel (n 41).

2.1.2.2. Data minimisation

The principle of data minimisation requires the processing of personal data to be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.[*47] In contrast, companies active in the field of Big Data analytics often gather and store as many data as possible.[*48] Data minimisation obligates the developers of AI systems to know which pieces of information the system requires for achieving the system's purpose.[*49] Having this awareness prior to the system's use may prove difficult. This is especially true in the case of Big Data: the functioning of many AI systems is made possible purely by dint of the vast volumes of data gathered.[*50]

Additionally, just as with the principle of purpose limitation, exceptions may apply. Hence, as noted above, the use of Big Data analysis is expressly permissible when the data are processed for statistical purposes that do not involve decisions related to any particular natural person.[*51]

Moreover, the GDPR's principle of data protection, by design and by default, obligates the controller to implement appropriate technical and organisational measures to comply with the regulation's data-protection requirements.[*52] Many of these principles were considered in the course of developing digital contact-tracing apps to fight the spread of the COVID-19 pandemic in the summer of 2020. Whereas using location data to trace contacts would have allowed performing further data-processing and, thereby, learning more about the data subjects' movements, the designers of many apps, among them the Estonian app HOIA, opted for Bluetooth Low Energy signals. In essence, instead of storing the location data of each user, the app gathers only anonymous Bluetooth codes from nearby mobile phones, thus minimising data collection.[*53]

2.1.2.3. Lawfulness

Among the prerequisites specified by the GDPR is a requirement for every instance of personal-data processing to have a legal basis; data-processing shall not be performed if it lacks legitimate grounds. Art. 6 GDPR provides for six separate legal bases for processing of personal data – namely, consent, performance of a contract, legitimate interest, vital interest, a legal requirement, and public interest:[*54]

As mentioned above, the GDPR places great emphasis on how consent is obtained and for what it can be used.[*55] Most importantly, data subjects may withdraw their consent at any time.[*56] Where consent has been withdrawn, the processing already undertaken is still lawful but further processing must cease.[*57] Both the need for consent and the withdrawal right may pose an obstacle for AI systems. As many AI systems continuously learn from past data, it is difficult to stop the process of such learning. Therefore, the GDPR's consent provisions present a permanent liability risk with regard to AI systems that continuously learn from information whose subsequent processing would be unlawful.[*58]

The invocation of a legitimate interest as the legal basis for data-processing by the data controller requires careful assessment. A balancing test must be carried out to evaluate whether the data subject's

47 Art 5(1)(c) GDPR.

48 Zarsky (n 21) 1010–11.

49 Biega and Finck (n 26) 30–31.

50 Ibid 31–32.

51 See this paper's section 2.1.2.1, addressing purpose limitation.

52 See art 25 GDPR.

53 Dan Bogdanov and Triin Siil, 'Infotehnoloogilised võimalused põhiõiguste kaitsel' [2020] (6) Juridica 474, 478 accessible via <www.juridica.ee/article.php?uri=2020_6_infotehnoloogilised_v_imalused_p_hi_iguste_kaitsel> accessed 1 July 2021; see also European Parliament, 'National COVID-19 Contact Tracing Apps' (briefing, 2020) PE 652.711 <www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf> accessed 1 July 2021.

54 Agencia Española de Protección de Datos, 'RGPD Compliance of Processings That Embed Artificial Intelligence: An Introduction' (2020) 19 <www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia-en_0.pdf> accessed 1 July 2021.

55 See section 2.1.2.1, above.

56 Art 7(3) GDPR.

57 Ibid.

58 Matthew Humerick, 'Taking AI Personally: How the EU Must Learn To Balance the Interests of Personal Data Privacy & Artificial Intelligence' (2018) 406–407 <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1633&context=chtlj> accessed 1 July 2021.

fundamental rights or freedoms override the legitimate interests of the data controller.[*59] An organisation's legitimate interest might include profiling customers for targeted marketing, preventing fraud, or pursuing physical and information security.[*60] Remarkably, legitimate interests may not be taken as a legal basis for data-processing by public authorities. Under Art. 6(1)(e) GDPR, public agencies may instead appeal to public interests as the basis for data-processing.

In one exception, the GDPR foresees that processing may be carried out without the consent of the data subject when this is for the performance of a task in the public interest or in the exercise of official authority vested in the controller.[*61] One can cite the above-mentioned regulation pertaining to NEET youth as an example in this regard.[*62]

2.1.2.4. Transparency

Data subjects can consent to data-processing and exercise their rights only if they understand what is being done with their data.[*63] Accordingly, the GDPR establishes that controllers are obliged to provide 'concise, transparent, intelligible and easily accessible' information to data subjects to ensure transparency of their data-processing operations.[*64] The Article 29 Working Party has noted that phrasings such as 'We may use your personal data to develop new services' and 'We may use your personal data for research purposes' do not convey the purpose of the data-processing in a clear enough manner.[*65]

As machine-learning systems are growing more sophisticated by the day, providing meaningful and at the same time easily understandable information about the logic involved can prove to be a difficult task. The deduction mechanisms and learning processes of machine-learning models are often hard to explain, especially since users usually have no prior knowledge of how automatic systems work. This may prove a particular challenge for organisations utilising unsupervised machine-learning models, whereby an AI system can evolve on its own.[*66]

2.1.2.5. Accuracy and integrity

Under the principle of accuracy, personal data must be processed accurately and, where necessary, kept up to date.[*67] According to the GDPR, every reasonable measure must be taken to ensure that a personal datum that is inaccurate, with respect to the purposes for which it is processed, is erased or rectified without delay.[*68] Personal data intended for processing and their sources must be validated, as data of unknown credibility can lead to a breach of data integrity.[*69] This issue is particularly important with regard to Big Data and AI systems, wherein poor-quality or biased/unrepresentative data in particular may lead to a discriminatory outcome. Therefore, controllers are obliged also to ensure the representativeness of the data[*70] in the future environment of the system.[*71]

59 Information Commissioner's Office, 'Big Data, Artificial Intelligence, Machine Learning and Data Protection' (2017) 34 <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 1 July 2021.

60 Ibid 33.

61 Art 1(e) GDPR.

62 See the discussion in section 2.1.1, above.

63 Mitrou (n 9) 55.

64 Art 12(1) GDPR.

65 Art 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (2017) 9 <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850> accessed 1 July 2021.

66 Humerick (n 58) 411–12. As to the question of whether the GDPR provides individuals with a right to explanation of AI models and decisions, cf Martin Ebers, 'Regulating Explainable AI in the European Union: An Overview of the Current Legal Framework(s)' in Liane Colonna and Stanley Greenstein (eds), *Nordic Yearbook of Legal Informatics 2020–2021* (forthcoming).

67 Art 5(1)(d) GDPR.

68 Ibid.

69 ENISA, 'Big Data Security: Good Practices and Recommendations on the Security of Big Data Services' (2015) 13–15 <www.enisa.europa.eu/publications/big-data-security/at_download/fullReport> accessed 6 July 2021.

70 Data representativeness is the concept of how well a dataset represents the entire population with regard to the characteristic under study. In essence, the dataset should project actual conditions as precisely as possible.

71 Mitrou (n 9) 51–52.

The GDPR confers on data subjects the right to demand rectification of inaccurate personal data without undue delay.[*72] If use of incorrect personal data has resulted in an incorrect outcome, one often can correct the mistake by simply running the process again but with the data rectified. Handling mistakes in data used as input to AI systems may, however, prove to be much more complex. For AI-based systems, the only solution is to re-teach the system, from rectified data, and doing so presents serious financial repercussions for the data controller. That said, the obligations specified apply only where the pattern learnt allows the identification of the data subject. In the context of AI systems, this is typically not the case.[*73]

2.2. The proposal for a regulation laying down harmonised rules on artificial intelligence

Unlike the realm of data protection, regulatory frameworks for that of AI are still in only their early stages.[*74] At EU level, the High-Level Expert Group on AI established by the European Commission has developed guidelines and other soft-law documents aimed at ensuring the ethical use of AI.[*75] In 2020, the European Commission published its White Paper on AI.[*76] The following consultations resulted in a proposal for a regulation laying down harmonised rules on artificial intelligence (the so-called Artificial Intelligence Act)[*77]. This proposal was released in 2021. The regulation would apply to both public and private actors, within and external to the EU, wherever an AI system is placed on the European Union market or its use affects people located in the EU.[*78] According to Art. 2(4) of the proposal, the regulation would not apply, however, to public authorities in a third country or to international organisations using AI systems in the framework of international agreements for law enforcement and judicial co-operation with the EU or with one or more member states.

In its draft, the European Commission proposes prohibiting the use of four kinds of AI system: firstly, 'AI systems that deploy subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour' in a manner that may cause physical or psychological harm; secondly, 'AI systems that exploit any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group' in a manner that may cause physical or psychological harm; thirdly, AI systems used by public authorities for the 'evaluation or classification of the trustworthiness of natural persons' on the basis of their social behaviour or personal/personality characteristics, where the 'social score' leads to unfavourable consequences disproportionate to the social behaviour; and, fourthly, with certain exceptions, 'real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement'.[*79]

Some types of AI system are deemed 'high-risk' for purposes of the proposal.[*80] Although the articulation of this concept is not clearly developed, the European Commission provides a list of areas wherein the use of an AI system is deemed high-risk.[*81] Per the proposal, high-risk AI systems shall be subject to increased regulation, laid out in the draft act's second chapter. Among other requirements, the providers of high-risk AI systems are subject to an obligation to establish risk-management systems, follow concrete

72 Art 16 GDPR.

73 Tina Krügel, '§ 11 Datenschutzrechtliche Herausforderungen künstlicher Intelligenz und Robotik' in Martin Ebers and others (eds), *Künstliche Intelligenz und Robotik* (2020) marginal note 34. – DOI: https://doi.org/10.17104/9783406769818.

74 Ebers (n 4) 83ff.

75 High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (2019) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419> accessed 1 July 2021.

76 Commission, 'White Paper on Artificial Intelligence' COM(2020) 65 final 2, 16.

77 Commission, 'Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM(2021) 206 final.

78 Ibid art 2(1).

79 Ibid art 5. The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) concluded in their joint opinion that a stricter approach is necessary; EDPB–EDPS, 'Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)' (2021) 12, no 30 <https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf> accessed 1 July 2021.

80 Ibid art 6, annexes II and III.

81 Ibid annex III.

data-governance practices, compile technical documentation, retain system logs, ensure transparency for the users, and implement measures for human oversight while the system is in use.[*82]

Importantly, the proposed regulation's explanatory memorandum states that 'the proposal is without prejudice and complements the General Data Protection Regulation'.[*83] The proposed regulation, therefore, would not make substantial changes to the general applicability of the data-protection rules of the GDPR to AI systems. Only two exceptions are foreseen so far. The first of them, regulated in Art. 10(5) of the proposal, pertains to the processing of special categories of data by high-risk AI systems; this processing would be allowed only to the extent 'that is strictly necessary for the purposes of ensuring bias monitoring'. Hence, the proposed amendment specifies the regulatory content of Art. 9 GDPR, comprising the processing of special categories of personal data.[*84] With the second exception, the proposal provides a legal basis for the use of regulatory sandboxes for the development of AI in the public interest[*85], a matter not explicitly regulated in the GDPR. However, as the European Data Protection Board and the European Data Protection Supervisor stressed in their joint opinion on the European Commission's proposal, the GDPR already has a provision for further data-processing in the public interest, and the use of regulatory sandboxes would still have to comply with the requirements of the GDPR.[*86]

The proposal is still to be negotiated between the European Parliament and the Council, and it will be subject to changes accordingly. Only time will tell whether those lead toward more privacy-preserving AI rules or a more flexible approach.

3. Estonian law regarding AI and data protection

3.1. Data-protection regulation in Estonia

According to the Estonian Constitution, all persons are entitled to access information about them held by public authorities.[*87] Also enshrined in the Constitution is the right to privacy, which, according to the Estonian courts' practice, includes protection against the processing of their personal data.[*88] Furthermore, the Supreme Court of Estonia has acknowledged the right to informational self-determination,[*89] which can be defined as the right of a person to decide for him- or herself how much – if at all – his or her personal data are to be collected by the state.[*90]

In response to the EU's data-protection reform, Estonian law needed to be revised. To this end, Estonia adopted a new version of the Personal Data Protection Act and amended other laws so as to be consistent with EU law.[*91]

Estonian law presents some deviations from the GDPR. To ensure the exercise of state supervision, the Estonian Law Enforcement Act foresees derogation from certain rules of the GDPR for law-enforcement agencies.[*92] Most importantly, the law allows deviation from the rights of the data subject laid down in

82 Ibid art 9–15.

83 Ibid 4; cf Recital 41 of the proposal: 'The fact that an AI system is classified as high risk under this Regulation should not be interpreted as indicating that the use of the system is necessarily lawful under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data.'

84 Critically, the EDPB–EDPS (n 79) 20ff, no 73: the proposal does not seem 'sufficiently clear to create a legal basis for the processing of special categories of data, and need[s] to be complemented with additional protective measures'.

85 Ibid art 53-54, recital (72); cf again EDPB–EDPS (n 79) 18ff.

86 EDPB–EDPS (n 79) 18ff.

87 Constitution of the Republic of Estonia para 44 (3), per the Riigi Teataja archive (n 17).

88 Art 26 of the Constitution of Estonia; see also Supreme Court of Estonia Administrative Law Chamber 23.10.2003, decision 3-3-1-57-03 <www.riigikohus.ee/et/lahendid/?asjaNr=3-3-1-57-03> accessed 1 July 2021.

89 Supreme Court of Estonia Constitutional Review Chamber 12.1.1994, decision III-4/A-1/94 <https://rikos.rik.ee/?asjaNr=III-4/1-1/94> accessed 1 July 2021.

90 Commentaries to the Estonian Constitution sub-s 26(24) <https://pohiseadus.ee/sisu/3497> accessed 1 July 2021; Supreme Court Administrative Law Chamber 12.7.2012, Judgment 3-3-1-3-12 19 <www.riigikohus.ee/et/lahendid?asjaNr=3-3-1-3-12> accessed 1 July 2021.

91 Law on the Implementation of the Personal Data Protection Act (Isikuandmete kaitse seaduse rakendamise seadus) RT I, 13.03.2019 2, per the Riigi Teataja archive (n 17).

92 Law Enforcement Act (Korrakaitseseadus) RT I, 03.03.2021 5, para 13, per the Riigi Teataja archive (n 17).

Chapter 3 of the GDPR.[*93] Yet Estonian law does not provide for any safeguards or restrictions in this regard, even though these are required by Art. 23(2) GDPR. Interestingly, when transposing the Law Enforcement Directive into national law, the Estonian legislator decided that the prevention of threats to public security would fall not under the directive but under the GDPR; thereby, stricter rules were applied to the maintenance of law and order than to offence-related proceedings. In Estonia, the scope of said directive is reduced to covering only the latter.[*94]

Further exceptions to the rights laid down in the GDPR apply when personal data are processed for scientific and historical research, as well as official statistics. In these instances, personal data may be processed in certain cases without the data subject's consent.[*95] Furthermore, in Estonia, information-society services may be provided directly to a child on the basis of his or her consent if the child is at least 13 years old.[*96]

The Personal Data Protection Act also covers some issues that are not regulated in the GDPR: matters such as the right to process personal data of deceased persons[*97], processing of data in connection with the violation of contractual obligations[*98], and data related to public places.[*99]

In addition to the Personal Data Protection Act, many other legal acts are relevant to processing personal data and using automated decision-making. These include, above all:

- the Public Information Act, which foresees that all non-restricted data contained in public databases shall be published online[*100];
- the Cybersecurity Act[*101], setting forth the requirements connected with the maintenance of fundamentally important networks and information systems (for example, the Estonian Electronic Health Record System)[*102];
- the Code of Civil Procedure,[*103] which provides that payment orders may be made in an automated manner by the court if the prerequisites specified for making the order (i.a., the sum must not be greater than the prescribed amount) are met[*104];
- the Law Enforcement Act, according to which the police may process personal data by using monitoring equipment and may obtain data from electronic-communications undertakings[*105];
- the State Liability Act, which provides for compensation for damages in the event that an administrative act extraordinarily restricts a person's fundamental rights.[*106]

93 Ibid.

94 The Personal Data Protection Act (Isikuandmete kaitse seadus), RT I, 04.01.2019 11, para 12 s 2 states that the chapter transposing the Law Enforcement Directive does not apply to processing of personal data in the exercise of activities of law-enforcement agencies with the aim of 'preventing a threat, ascertaining and countering a threat or eliminating a disturbance'. The explanatory memorandum to the Personal Data Protection Act (2018) 19 further clarifies that the above-mentioned chapter covers only offence-related proceedings. On the other hand, the Law Enforcement Directive is not limited to offence proceedings and applies also to the safeguarding against and the prevention of threats to public security. Recital 12 of that directive states, further, that the scope includes 'maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence'. The Estonian restrictive approach to the scope of the Law Enforcement Directive was, *inter alia*, criticised by the director general of the Estonian Data Protection Authority. See Estonian Data Protection Authority, 'Andmekaitse Inspektsiooni peadirektori seisukohad uue andmekaitseõiguse kontseptsiooni asjus (koostatud Justiitsministeeriumis 27.04.2017)' (2017) 2 <www.aki.ee/sites/default/files/dokumendid/reform/jum_oigusraamistiku_kontseptsiooni_markused_27.04.2017.pdf> accessed 1 July 2021.

95 The right to derogate is set out in art 89 GDPR. See the Personal Data Protection Act (n 94) para 6.

96 Cf the Personal Data Protection Act (n 94) para 8(1); art 6(1)(a) GDPR.

97 Personal Data Protection Act (n 94) para 9.

98 Personal Data Protection Act (n 94) para 10.

99 Personal Data Protection Act (n 94) para 11.

100 Public Information Act (n 34) paras 28, 30, and 32.

101 Cybersecurity Act (Küberturvalisuse seadus) RT I, 22.05.2018 1 para 1 s 1, per the Riigi Teataja archive (n 17).

102 For further information, see 'Health Information System Statute'; Health and Welfare Information Systems Centre, 'Patient Portal' <www.digilugu.ee/login?locale=en> accessed 1 July 2021.

103 Code of Civil Procedure (Tsiviilkohtumenetluse seadustik) RT I, 09.04.2021 17 para 489^2, per the Riigi Teataja archive (n 17).

104 Addressed in detail by Piia Kalamees, 'Tarbija õiguste kaitse maksekäsu kiirmenetluses Euroopa Kohtu praktika valguses' [2019] (8) 613 <www.juridica.ee/article.php?uri=2019_8_tarbija_> accessed 1 July 2021.

105 Law Enforcement Act (n 92) paras 34 and 35.

106 State Liability Act (Riigivastutuse seadus) RT I, 17.12.2015 76 para 16, per the *Riigi Teataja* archive (n 17).

3.2. The regulation of AI systems in Estonia

In Estonia, there are (as yet) no laws dealing specifically with AI systems. Instead, general laws apply. The processing of personal data within the realm of AI systems – especially by means of profiling and automated decision-making – requires compliance with general regulations on the protection of equal treatment and non-discrimination, therefore. Among the relevant equal-treatment acts are the Equal Treatment Act[*107], the Gender Equality Act[*108], and the Employment Contracts Act (which obliges employers to protect their employees against discrimination, to follow the principle of equal treatment, and to promote equality[*109]). So far, there is also no Estonian case law regarding the use of AI or AI-based decision-making.

Yet a working group managed by the Ministry of Economic Affairs and Communications and the Government Office did publish a report on the possibilities for applying AI in Estonia on wider scale.[*110] The report, released in May 2019, presents the conclusion that neither significant changes to the legal system nor a separate 'AI law' is necessary for successfully regulating AI systems[*111] and that personal-data processing in the context of AI is sufficiently protected by the GDPR and the respective national law.[*112] However, the report explicitly excludes ethics issues from consideration, and the authors note that human interaction with AI may give rise to further questions related to fundamental rights, which the report does not address in detail.[*113]

Then, in 2020, the Estonian Ministry of Justice prepared a project for the legislative regulation of algorithmic systems.[*114] The project argument states that a separate legislative act must be enacted to regulate algorithmic systems, as current legislation does not provide for sufficient protection of fundamental rights in the use of AI.[*115] With regard to data protection, the expert opinion identified a particular danger to fundamental rights in the lack of human control and the opacity of algorithms.[*116] The Ministry of Economic Affairs and Communications, in response to the legislative intent, asked whether a separate AI law is needed at all. The ministry recommended instead amending multiple regulations that hinder the adoption of self-learning algorithmic systems. Regarding fundamental-rights protection, it proposed avoiding over-regulation and making the necessary individual amendments to the existing law instead of adopting a new, separate legal act.[*117] Most comments on the Ministry of Justice's project recommended co-ordinating Estonian legislation on AI with the (legislative) plans of the EU.[*118] In this spirit, the Ministry of Justice decided to put new legislation on hold[*119] until the European Commission could present its proposals on the regulation of AI in 2021.[*120]

107 Equal Treatment Act (Võrdse kohtlemise seadus) RT I, 26.04.2017 9, per the Riigi Teataja archive (n 17).

108 Gender Equality Act (Soolise võrdõiguslikkuse seadus) RT I, 10.01.2019 19, per the Riigi Teataja archive (n 17).

109 Employment Contracts Act (Töölepingu seadus) RT I, 28.05.2021 19 para 3, per the Riigi Teataja archive (n 17).

110 Report of Estonia's AI Taskforce (n 2).

111 Ibid 38.

112 Ibid 40.

113 Ibid 42.

114 Ministry of Justice, 'Algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsus ("krati VTK")' (2020) <https://adr.rik.ee/jm/fail/7458503/subfile/1> accessed 1 July 2021.

115 Ibid 30.

116 Ibid 11.

117 Ministry of Economic Affairs and Communications, 'Vastus Justiitsministeeriumi algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsusele ("krati VTK")' (2020) <https://eelnoud.valitsus.ee/main/mount/docList/93ebe63d-de8c-4662-9908-3232aa7f987c> accessed 1 July 2021.

118 See, for example, Ministry of Foreign Affairs, 'Algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsuse kooskõlastamine' (2020) 2 <https://eelnoud.valitsus.ee/main/mount/docList/93ebe63d-de8c-4662-9908-3232aa7f987c> accessed 1 July 2021.

119 Liisi Jürgen, Tea Kookmaa, and Tanel Kerikmäe, 'Jürgen, Kookmaa, Kerikmäe: kratiseadus pandi ootele' *ERR* (1 December 2020) <www.err.ee/1192069/jurgen-kookmaa-kerikmae-kratiseadus-pandi-ootele> accessed 1 July 2021.

120 Commission, 'Artificial Intelligence – Ethical and Legal Requirements' (initiative document) < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements_en> accessed 1 July 2021.

4. Conclusion

The discussion above was aimed at examining, from an Estonian perspective, the extent to which it is possible to develop and employ AI while complying with the rules for data protection within the EU.

A closer look at the legal regulations shows that the development and application of AI systems within the EU is limited by numerous provisions of data-protection law. It remains clear that many of these requirements, among them that of following the principle of consent, are subject to exceptions – especially in the context of public law. There is clearly a need for debate pertaining to their content and scope of application. The use of AI by the private sector, to which the GDPR's opening clauses do not apply, likewise requires further evaluation. On account of their unclear wording, many of the legal exceptions raise several questions of their own, and their potential scope remains unclear. The complexity of the legal requirements, in combination with the risk of potential liability under data-protection law when one is using AI, poses a risk that the development and use of AI in Europe will not be able to proceed at an unbridled pace. It is important to remember that, in a global world, the race to develop AI best and the most rapidly is one with global scale. Countries in which compliance with democratic principles and the protection of fundamental rights does not pose meaningful restrictions for the simple reason that no such rights apply are certainly at a technical advantage. Therefore, democratic states must consider that lagging behind non-democratic states in the technological race could itself pose concrete threats to public safety and security.

However, it must also not be forgotten that the EU is a community of values. It is precisely these values that guarantee the quality of life and well-being of the people in the EU. As Art. 2 of the Treaty of the EU states, the Union is founded on the values of respect for human dignity and human rights, freedom, democracy, equality, and the rule of law. For this reason, data-protection law must not simply be abolished on the argument that it 'inhibits innovation'. On the contrary, EU data protection can light the way for others, as the example of the GDPR shows: it is one of the most successful legal acts of the EU, one that has influenced many non-European countries and served as a worldwide model – e.g. for Canada and the US state of California.[*121] As the political priorities under newly appointed European Commission President von der Leyen confirm, the EU is now also claiming a leading role in the field of AI.[*122]

As with data protection, the biggest challenge in regulating AI systems is finding the right balance between openness to innovation and protection of fundamental rights. The constant analysis of data-protection regulations and, where required, their legal amendment together form a necessary condition for maintaining this balance in an environment of constant technological development. Also, it is to be hoped that legal practice and scholarship, along with the European Data Protection Supervisor and/or the European Commission by means of guidelines on the interpretation of the GDPR in relation to AI, will, over time, fill in the gaps and clarify the uncertainties inherent to the GDPR's vague and sometimes unclear formulation. In this respect, the objective behind this paper has been to contribute to the necessary legal discussion by providing an overview of the most relevant data-protection rules connected with the application of AI systems in the EU.

[121] See also Martin Ebers and Marta Cantero Gamito, 'Algorithmic Governance and Governance of Algorithms: An Introduction' 1, 8ff in Ebers and Cantero (eds), *Algorithmic Governance and Governance of Algorithms: Legal and Ethical Challenges* (Springer 2020). – DOI: https://doi.org/10.1007/978-3-030-50559-2.

[122] Ibid.