sciendo

Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation

Rafael Brown, Jon Truby and Imad Antoine Ibrahim[*]

Summary: The European Union (EU) is leading in the regulation of data privacy and artificial intelligence through the General Data Protection Regulation (GDPR), the proposed European Commission (EC) regulation, and the proposed European Parliament (EP) regulations concerning Artificial Intelligence (AI). The EU also regulates AI through ethical aspects and Intellectual Property Rights as well as the Council of Europe's conclusions concerning the use of sandboxes regulations and experimentation clauses. This article highlights the EU's missed opportunities to create synergies between the GDPR and the proposed AI regulations, given that in several instances they deal with issues that must be regulated from an AI perspective, while simultaneously ensuring data protection of EU citizens. In particular, the EU's ad hoc approach to AI regulation creates lacunas because of its failure to fully integrate the essential components of AI data and algorithm within a regulatory framework.

Keywords: artificial intelligence, data, GDPR, privacy, strict liability

Citation: BROWN, R.; TRUBY, J.; IBRAHIM, I. Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation. *European Studies – the Review of European law, Economics and Politics*. 2022, vol. 9, no. 1, pp. 61–90, DOI: 10.2478/eustu-2022-0003

1. Introduction

The European Union (EU) is one of the most important players in the field of artificial intelligence (AI) and data privacy. In the last few years, the various organs of the EU have adopted numerous documents and mechanisms, binding and non-binding, addressing both data protection and AI.[1] The EU aims to as-

[*] College of Law, Qatar University, Doha, Qatar. Corresponding author: Imad Antoine Ibrahim; email: imad.ibrahim@qu.edu.qa.

[1] See generally, REDING, V. The Upcoming Data Protection Reform for the European Union. *International Data Privacy Law.* 2011, vol. 1, no. 1, pp. 3; LOENEN, B., KULK, S., PLOEGER, H. Data Protection Legislation: A Very Hungry Caterpillar: The Case of Mapping

sume a global role while simultaneously protecting its citizens from any potential risks.[2] To that end, one can notice the ambitious but cautious approach embraced by the EU when addressing the various aspects of AI and data development, regulation, and use. This approach has resulted in the adoption of several recent regulations and proposals tackling AI and data privacy in the EU that in turn have been the subject of vigorous scholarly debate.[3]

The EU in the data domain adopted the General Data Protection Regulation (GDPR) in 2016, aiming to update rules for the protection of data privacy throughout the EU.[4] The GDPR replaced the Data Protection Directive (DPD),[5] which governed data privacy since 1995.[6] In simple terms, the GDPR's objective is to grant EU citizens more control over their personal data and the way this data is being used, making the citizen's consent a cornerstone on the basis of which companies can collect and process personal data.[7] Since its adoption, the GDPR has been either hailed as a model for future data protection regulations to be adopted in the EU and globally, or as a regulation suffering from numerous shortcomings requiring its amendment.[8]

Data in the European Union. *Government Information Quarterly*. 2016, vol. 33, no. 2, pp. 338; HILDEBRANDT, M. The Artificial Intelligence of European Union Law. *German Law Journal*. 2020, vol. 21, no. 1, pp. 74.

[2] See generally, VEALE, M. A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence. *European Journal of Risk Regulation*. 2020, vol. 11, no. 1, pp. 1; PURTOVA, N. The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. *Law, Innovation and Technology*. 2018, vol. 10, no. 1, pp. 40.

[3] See generally, VESNIC-ALUJEVIC, L., NASCIMENTO, S., PÓLVORA, A. Societal and Ethical Impacts of Artificial Intelligence: Critical Notes on European Policy Frameworks. *Telecommunications Policy*, 2020, vol. 44, no. 6:101961, pp. 1; KOSTA, E. *Consent in European Data Protection Law*. Leiden: Martinus Nijhoff Publishers, 2013; REDING, V. The European Data Protection Framework for the Twenty-First Century. *International Data Privacy Law*, 2012, vol. 4, no. 3, pp. 119; KOOPS, B.-J. The Trouble with European Data Protection Law. *International Data Privacy Law*. 2014, vol. 4, no. 4, pp. 250.

[4] FEFER, R. F. *EU Data Protection Rules and U.S. Implications* [online]. Available at: https://fas.org/sgp/crs/row/IF10896.pdf

[5] VOSS, W. G. European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. *The Business Lawyer*. 2017, vol. 72, no. 1, pp. 221.

[6] European Commission, *Fundamental Rights* [online]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

[7] SHEIKH, S. *Understanding the Role of Artificial Intelligence and Its Future Social Impact.* Hershey: IGI Global, 2020, pp. 269.

[8] See generally, VOIGT, P., VON DEM BUSSCHE, A. *The EU General Data Protection Regulation (GDPR): A Practical Guide.* Cham: Springer, 2017; BHAIMIA, S. The General Data Protection Regulation: the Next Generation of EU Data Protection. *Legal Information Management*. 2018, vol. 18, no. 1, pp. 21–28.; TIKKINEN-PIRI, C., ROHUNEN, A., MARKKULA, J. EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies. *Computer Law & Security Review*. 2018, vol. 34, no. 1, pp. 134;

In the AI field, EU institutions have issued various documents outlining their main priorities. These priorities include (1) boosting the technological and industrial capacity of the Union and the dissemination of AI in the various economic sectors; (2) preparing for the various expected changes resulting from AI – mainly socio and economic ones; and (3) the development of suitable ethical and legal rules.[9] The EU adopted a coordinated approach to benefit from opportunities emerging from AI while addressing existing challenges. The goal is to lead the way in AI based on EU values and strengths that led, for instance, to the launch of an EU initiative on AI in 2017.[10] The combined efforts of the various institutions led to the recent adoption of several propositions for EU regulations concerning harmonised rules on AI civil liability by the European Commission, and AI ethical aspects and Intellectual Property Rights (IPRs) by the European Parliament (EP).

The analysis in this Article will highlight the EU's missed opportunities to create synergies between the GDPR and the proposed AI regulations, given that in several instances they deal with issues that must be regulated from an AI perspective, while simultaneously ensuring data protection of EU citizens. In particular, this paper argues that the EU's *ad hoc* approach to AI regulation creates lacunas because of its failure to connect the essential components of AI data and algorithm within a regulatory framework.

The paper begins in Part II by providing the necessary background on the EU's General Data Protection Regulation (GDPR).[11] Part II provides a background on the brief history, the types of data covered, and protected rights under the GDPR. The background on the GDPR is necessary for a discussion on the extent of the GDPR's application to AI. Part III provides a brief overview of the proposed AI regulations by the EC, EP and the EU Council. It will examine the proposed EC proposal concerning the harmonised rules on artificial intelligence, EP regulations concerning civil liability, ethical aspects, and IPRs. Part IV discusses the gaps in the GDPR for regulating AI, and the gaps in the proposed AI regulations.

For purposes of this paper, AI is defined "as a suite of autonomous self-learning and adaptively predictive technologies that enhances the ability to perform

HOOFNAGLE, C. J., VAN DER SLOOT, B., BORGESIUS, F. Z. The European Union General Data Protection Regulation: What It is and What It Means. *Information & Communications Technology Law*. 2019, vol. 28, no. 1, pp. 65.

[9] OECD, *Artificial Intelligence in Society*. Paris: OECD Publishing, 2019, pp. 138.

[10] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Artificial Intelligence for Europe {SWD(2018) 137 final}.

[11] See Commission Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O. J. (L 119) 87 [online]. Available at: https://op.europa.eu/s/omni [GDPR].

tasks".[12] This definition is not far from the definition of AI systems in the EP's Resolution on the civil liability regime for artificial intelligence, which defines an AI system under Article 3(a) as "either software-based or embedded in hardware devices, and that displays behaviour simulating intelligence by, inter alia, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals."[13] The definition of AI used in this paper is essentially that of machine learning AI,[14] rather than the type of AI that is considered as strong AI[15] or true AI, which some predict could happen when AI achieves singularity[16] or human-level intelligence.[17]

2. EU's GDPR

Before discussing the applicability of the GDPR[18] to AI, this Section provides a necessary brief overview of the GDPR. It begins with a brief history of the

[12] TRUBY, J., BROWN, R., DAHDAL, A. Banking on AI: Mandating a Proactive Approach to AI Regulation in the Financial Sector. *Law and Financial Markets Review*. 2020, vol. 14, no. 2, pp. 110. The High Level Expert Group on AI (AI HLEG) arguable provides the broadest definition of AI when it defines an AI system as follows: software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. European Commission, *AI-HLEG, High-Level Expert Group on Artificial Intelligence. A definition of AI: Main capabilities and Scientific Disciplines* [online]. Available at: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

[13] European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), Art. 3(a) [online]. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html

[14] BROWN, R. Property Ownership and the Legal Personhood of Artificial Intelligence. *Information & Communications Technology Law*. 2021, vol. 30, no. 2, pp. 208 (stating that what people call AI today is actually machine learning).

[15] Ibid., p. 208; SEARLE, J. R. Minds, Brains, and Programs. *Behavioral and Brain Sciences*. 1980, vol. 3, no. 3, pp. 417 (first coining the terms weak AI and strong AI).

[16] GOOD, I. J. Speculations Concerning the First Ultra Intelligent Machine. In: ALT, F., Rubinoff, M. (eds.). *Advances in Computers*. New York: Academic Press, 1965, vol 6.

[17] PRESCOTT, T. J. The AI Singularity and Runaway Human Intelligence. In: LEPORA, N., MURA, A., KRAPP, H. (eds.). *Biomimetic and Biohybrid Systems*. Heidelberg: Springer-Verlag, 2013, vol. 8064, pp. 438. (arguing that "AI should be measured against the collective intelligence of the global community of human minds brought together and enhanced be smart technologies that include AI").

[18] See GDPR., op. cit., p. 87.

GDPR, and its precursor, the Data Protection Directive (DPD).[19] Further, this Section identifies the key provisions of the GDPR, including the types of data covered within its scope, entities covered, and the various individual rights protection provided by the GDPR. Finally, this Section discusses the extraterritorial reach of the GDPR for organizations and businesses located outside of the EU.

2.1. Brief History of the GDPR

Prior to the GDPR, the EU protected data privacy under the DPD,[20] a directive passed by the EP that took effect in 1995.[21] The DPD regulated the processing of digital personal data and its free movement within the EU.[22] Over the next decade since the enactment of the DPD, the EU recognized the new challenges brought by technological developments, including the widespread use of big data, and the need for further protections.[23] Further, the DPD did not create one uniform data protection law across the EU, but rather created twenty-eight different data protection laws among the EU member states.

The GDPR, proposed in 2012, aims to harmonize data protection laws in the EU as a regulation, rather than as a directive such as the DPD. The GDPR has a wider territorial scope, and is enforceable across all EU member states and even outside the EU.[24] In addition, the GDPR aims to keep pace with evolving technology, and offers greater protection to digital transactions of EU citizens.[25]

In 2016, the EU Parliament approved the GDPR's final text, and it took effect in 2018 after a two-year transition period, ultimately supplanting the DPD.[26] Compared to the DPD, the GDPR creates additional rights to EU data subjects, imposes obligations to controllers and processors of data, and creates supervisory authorities with specific enforcement powers.[27]

[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

[20] Ibid.

[21] PETERSEN, K. GDPR: What (and Why) You Need to Know About EU Data Protection Law. *AUG Utah Bar Journal*. 2018, vol. 31, no. 4, pp. 12; MEDDIN, E. The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement On Trade in Services. *American University International Law Review*. 2020, vol. 35, no. 4, pp. 997.

[22] Ibid.

[23] MONAJEMI, M. Privacy Regulation in the Age of Biometrics that Deal with a New World Order of Information. *University of Miami International & Comparative Law Review*. 2018, vol. 25, no. 2, pp. 371. MEDDIN, E., op. cit., p. 997.

[24] PETERSEN, K., op. cit., p. 12; MEDDIN, E., op. cit., p. 997.

[25] Ibid; MONAJEMI, M., op. cit., p. 371.

[26] Ibid., p. 12.

[27] MONAJEMI, M., op. cit., p. 371.

2.2. Types of Data Covered under the GDPR

To better understand the GDPR, it is important to delineate to whom the GDPR applies, what types of data it protects, and to what extent the GDPR protects personal data.

2.2.1. Controller or Processor

The GDPR covers two groups of people with separate and distinct roles: controllers and processors.[28] The GDPR defines a controller as a person,[29] who "alone or jointly with others, determines the purpose and means of processing data".[30] A processor, on the other hand, is a person who "processes personal data on behalf of a data controller."[31] The word "processing" is defined broadly to include operations "performed on personal data or on sets of personal data".[32] The examples given include, among others, collecting, organizing, recording, storage, use, erasure or destruction of personal data, regardless of whether it was done by persons or automated means.[33] The GDPR deems controllers as the principal, while the processor as the agent.[34] In this regard, the burden of showing compliance is placed upon the controller.[35] The GDPR, therefore, requires controllers to "implement appropriate technical and organisational measures" and policies to ensure and demonstrate compliance with the GDPR.[36]

2.2.2. Personal Data and Special Category Data

The GDPR, as a layered regime, also divides the types of data it covers into two categories: personal data and special category data.[37] Article 4(1) defines personal data as "any information relating to an identified or identifiable natural person ('data subject')".[38] Further, whether a person is identifiable is broadly defined to include direct or indirect reference to the "name, an identification

[28] Ibid., p. 371; MEDDIN, E., op. cit., p. 997.

[29] The GDPR more specifically refers to "a natural or legal person, public authority, agency, or other body". GDPR., Art. 4(7–8).

[30] GDPR., Art. 4(7); MEDDIN, E., op. cit., p. 371.

[31] Ibid., Art. 4(8); MONAJEMI, M., op. cit., p. 371; MEDDIN, E., op. cit., p. 997.

[32] Ibid., Art. 4(2).

[33] Ibid., Art. 4(2), Art. 5, and Art. 9; MONAJEMI, M., op. cit., p. 371.

[34] MONAJEMI, M., op. cit., p. 371.

[35] GDPR., Art. 5(2).

[36] Ibid., Art. 24(1–2); MEDDIN, E., op. cit., p. 997.

[37] Ibid., Art. 4(1); MONAJEMI, M., op. cit., p. 371; ZARSKY, T. Z. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*. 2017, vol. 47, no. 2, pp. 996.

[38] Ibid., Art. 4(1).

number, location data, an online identifier" or other factors that specifically identify a person's "physical, physiological, genetic, mental, economic, cultural or social identity."[39] According to this definition, the GDPR covers web data like IP addresses and user names.[40]

Following the approach of the DPD, the GDPR creates a special category of data under Article 9 that includes the following: race, ethnic origin, political views, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, and data concerning a natural person's sex life or sexual orientation.[41] Special category data requires more stringent protection than personal data.[42] In essence, processing of special category data is plainly prohibited save for a few exceptions.[43] The exceptions include the processing of data that is consented to, already made public by the person, and other specific exceptions covering the need to exercise a legal right, public health, and substantial public interest.[44] Another specific exception that is pertinent to this paper is the exception for purely internal use by a non-profit organization.[45]

2.2.3. Purpose and Necessity of Data

The processing of personal data under the GDPR must also follow two requirements that shape the scope of the data being processed: the purpose and the necessity. Processing of personal data must be done according to a "specified, explicit, and legitimate" purpose.[46] Personal data cannot be processed if the processing contravenes or is "incompatible" with the originally specified purpose.[47]

Additionally, the processing of data must adhere to the data minimization principle, which requires that the data be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[48] In short, data must only be processed when necessary. The data minimization principle applies to both the scope, duration, and types of data being processed.[49]

[39] Ibid., Art. 4(1); MEDDIN, E., op. cit., p. 997.

[40] MONAJEMI, M., op. cit., p. 371.

[41] GDPR., art 9(1); MEDDIN, E., op. cit., p. 997; ZARSKY, T. Z., op. cit., p. 996.

[42] Ibid., Art. 9; MONAJEMI, M., op. cit., p. 371.

[43] Ibid., Art. 9(1).

[44] Ibid., Art. 9(2); ZARSKY, T. Z., op. cit., p. 996.

[45] Ibid., Art. 9(2); MEDDIN, E., op. cit., p. 997.

[46] Ibid., Art. 5(1)(b); ZARSKY, T. Z., op. cit., p. 996.

[47] Ibid.

[48] Ibid., Art. 5(1)(c); ZARSKY, T. Z., op. cit., p. 996.

[49] ZARSKY, T. Z., op. cit., p. 996.

2.3. Protected Rights under the GDPR

In addition to the rights covered by the DPD, the GDPR introduces new concepts of rights with regards to personal data.[50] Among the individual personal data rights covered by the GDPR are (1) the right to consent and the right to withdraw consent, (2) the right to erasure, (3) the right to rectification and restriction, (4) the right to object, (5) the right to right to access, and (6) the right to portability.[51]

2.3.1. Right to Consent and Right to Withdraw Consent

One of the most important rights protected under the GDPR is the need to obtain consent prior to the processing of personal data.[52] Notably, the GDPR requires an "opt-in" rather than an "opt-out" consent.[53] An "opt-in" consent places the burden on the company to establish that the person has consented, as stated in Article 7(1).[54] "Opt-out" consent, on the other hand, allows companies to assume consent unless the person opts-out.[55] The GDPR does not allow opt-out consent because it requires written consent to use clear and plain language,[56] that the consent be freely given,[57] that the person can withdraw the consent,[58] and places the burden on the controller to demonstrate that person consented.[59] Article 4(11) more specifically defines consent as a "freely given, specific, informed and unambiguous indication" that the person agrees to the processing of the personal data.

A corollary to the right to consent is the right to withdraw the consent. According to the preamble, "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".[60] Therefore, the GDPR gives a person the right to

[50] See European Data Protection Supervisor, *The History of the General Data Protection Regulation* [online]. Available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [hereinafter History of GDPR].

[51] Ibid.

[52] GDPR., Art. 7; MEDDIN, E., op. cit., p. 997; MONAJEMI, M., op. cit., p. 371.

[53] Ibid.

[54] Ibid., Art. 7(1).

[55] MEDDIN, E., op. cit., p. 997 (stating that "opt-in consent is a more affirmative manner of obtaining consent; no longer able to rely on a subject's silence or on pre-checked boxes that are not easily seen, known as opt-out consent, companies must actively seek and receive consent.")

[56] GDPR., Art. 7(2).

[57] Ibid., Art. 7(4).

[58] Ibid., Art. 7(3).

[59] Ibid., Art. 7(1); MEDDIN, E., op. cit., p. 997.

[60] Ibid., preamble, par. 42.

withdraw consent "at any time", and making it as easy to give and withdraw consent under Article 7(3).[61]

2.3.2. Right of Erasure or the Right to be Forgotten

The GDPR also give a person the right to be forgotten through the right of erasure.[62] Under Article 17, a person has the right to ask the controller to erase personal data affecting him or her without undue delay.[63] The right to erasure applies primarily in situations that do not comply with the GDPR when the processing is no longer necessary for the purpose, the person withdraws consent, the person object to the processing, unlawful processing, and for legal compliance.[64]

2.3.3. Right to Rectification and Restriction

The GDPR also gives persons the right to rectify and restrict the processing of personal data. Under Article 16, persons can ask the controller to rectify inaccurate personal data without undue delay.[65] This right also includes the right to have incomplete data completed.

A similar right is the right for a person to ask the controller to restrict the processing of personal data under Article 18 when the data's accuracy is contested, the processing is unlawful but the person objects to erasure, when the data is no longer necessary for the purpose, and when the person has objected to the processing.[66]

2.3.4. Right to Access

The GDPR also gives persons the right to access their personal data under Article 15, which gives persons the right to ask controllers to confirm whether their data is being processed.[67] If so, the person has the right to access and get a copy

[61] Ibid., Art. 7(3); MONAJEMI, M., op. cit., p. 371 (noting that an organization may be able to argue a "compelling legitimate ground" though it has the burden of showing specified and legitimate reason, and public authorities cannot rely on this argument).

[62] See European Data Protection Supervisor., op. cit. Before the GDPR, the Court of Justice of the European Union (CJEU) in a 2104 decision held that Google was "obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person." *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González, ECLI:EU:C:2014:131/12, par. 88 [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

[63] GDPR., Art. 17.

[64] Ibid., Art. 17 (a–f); MONAJEMI, M., op. cit., p. 371.

[65] Ibid., Art. 16.

[66] Ibid., Art. 18.

[67] Ibid., Art. 15.

of the personal data, including information about the purpose of the processing; categories of data; recipients; period of storage; right to restrict, rectify, and erase data; right o complaint; source of the data; and use of automation.[68]

2.3.5. Right to Portability

One of the novel rights introduced by the GDPR is the right to portability under Article 20.[69] The right of portability, in essence, gives the person the right to receive a copy of the personal data provided to a controller and have that data transferred to another controller.[70] The right of portability, according to De Hert, actually consists of three distinct rights: the right to receive a copy of the data, (2) the right to transmit the data to another controller, and (3) the right to have the data transmitted directly from one controller to another.[71]

2.4. Extraterritorial Reach

Another salient feature of the GDPR is its broad extraterritorial reach. The GDPR, as a regulation rather than a directive, applies to all EU member states. Further, the GDPR applies to persons and activities located outside of the EU in three circumstances. First, the GDPR applies to controllers and processors located in EU member states whose processing of personal data takes place outside of the EU.[72]

Second, the GDPR applies to controllers or processors located outside of the EU when processing the personal data of persons who are located in the EU whenever the processing activities relates to (1) the offering of good and service, and (2) monitoring of behavior that takes place in the EU.[73] The GDPR will only apply, however, if it is foreseeable that the processing activities will be directed towards an EU member state.[74]

Third, the GDPR applies to controllers and processors not located in the EU, but EU Member State law applies under international law.[75] The practical effect

[68] Ibid., Art. 15 (a–h); MONAJEMI, M., op. cit., p. 371; DE HERT, P., PAPAKONSTANTINOU, V. The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services. *Computer Law & Security Review*. 2018, vol. 34, no. 2, pp. 193.

[69] Ibid., Art. 20; DE HERT, P., et al., op. cit., p. 193.

[70] Ibid., Art. 20.

[71] DE HERT, P., et al., op. cit., p. 193.

[72] GDPR., Art. 3(1).

[73] Ibid., Art. 3(2); MONAJEMI, M., op. cit., p. 371. In this scenario, an EU representative must be appointed. MEDDIN, E., op. cit., p. 997.

[74] MONAJEMI, M., op. cit., p. 371.

[75] GDPR., Art. 3(3).

of the GDPR is that every entity located anywhere in the world with a digital presence in the EU will fall under the GDPR's scope.[76] This is especially true when the subject of the data is from the EU.[77]

3. EU Proposed AI Regulations

Several documents have been adopted recently by the EC, EP and the Council of the EU advocating for the adoption of specific AI regulations. The EC adopted a proposal in April 2021 laying down harmonised rules on artificial intelligence.[78] The EP adopted three documents in October 2020 which are: the framework of ethical aspects of artificial Intelligence, robotics and related technologies;[79] civil liability regime for artificial intelligence,[80] and intellectual property rights for the development of artificial intelligence technologies.[81] The Council adopted in November 2020, the conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age.[82] All these documents will be examined briefly in this Section.

3.1. Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts

The European Commission's Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial

[76] MEDDIN, E., op. cit., p. 997.

[77] MONAJEMI, M., op. cit., p. 371.

[78] European 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 (2021/0106) (COD) COM (2021) 206 Final.

[79] European Parliament, Framework of ethical aspects of artificial intelligence, robotics and related Technologies. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)).

[80] European Parliament Resolution., Art. 3(A).

[81] European Parliament, Intellectual property rights for the development of artificial intelligence Technologies. European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI)).

[82] Council of the European Union, Council Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age, Brussels, Nov. 16, 2020.

Intelligence ("EC Proposal") focuses on laying down "harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union"[83] as well as prohibiting specific AI practices and establishing certain requirements related to high-risk AI systems and their operators.[84] It also aims to ensure the adoption of harmonised rules related to transparency for AI systems interacting with "natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content";[85] and laying down rules applicable to market monitoring and surveillance.[86]

The proposal covers providers of AI systems even when they are located in third countries as long as the AI system product or output is used in the EU. It also covers users of the AI systems. Specific categories are not covered within the proposal such as military use of these systems.[87] The proposal prohibits specific AI practices when such practices exploit for instance the vulnerability of specific group of persons having age, physical or mental disability.[88]

The proposal lays down detailed rules applicable to high-risk AI systems. These rules are related to the classification of these high-risk AI systems; requirements including the establishment of a risk management system, technical documentation, transparency and provision of information to users, human oversight…[89] It also lays down the obligations of providers and users of high-risk AI systems and other parties including product manufacturers, authorised representatives, importers, distributors and any third party.[90]

The proposal includes specific procedural provisions related to the notification of the authorities and other bodies,[91] related to standards, conformity assessment, certificates, registration.[92] It also covers transparency obligations for certain AI systems and measures in support of innovation.[93] Likewise, specific governance provisions related to the European artificial intelligence board, national competent authorities,[94] EU database for stand-alone high-risk AI systems and post-market monitoring, information sharing, market surveillance are

[83] European Commission Proposal., op. cit., Art. 1(a).

[84] Ibid., Art. 1 (a) (b).

[85] Ibid., Art. 1(c).

[86] Ibid., Art. 1(d).

[87] Ibid., Art. 2.

[88] Ibid., Art. 5.

[89] Ibid., Art. 6–15.

[90] Ibid., Art. 16–29.

[91] Ibid., Art. 30–39.

[92] Ibid., Art. 40–51.

[93] Ibid., Art. 52–55.

[94] Ibid. Art. 56–59.

stipulated.[95] Finally, the proposal allows the establishment of a code of conducts, imposes penalties and rules for delegation of power and committee procedure.[96]

These are the main provisions of this proposal which aim at achieving the following objectives: "1) ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values; 2) ensure legal certainty to facilitate investment and innovation in AI; 3) enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems and 4) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation".[97]

3.2. Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies

This framework establishes legal principles that must be respected, and which include inter alia human dignity, autonomy and safety[98] as well as "social inclusion, democracy, plurality, solidarity, fairness, equality and cooperation".[99] The framework imposes specific regulations for high-risk AI technologies emphasizing the need to comply with its ethical principles when developing, deploying or using these technologies.[100] It also adopts a human-centric and human-made approach to AI explicitly stating that the development of high risk AI technologies must always remain under human oversight and allowing humans to regain control when needed for various purposes such as changing these technologies.[101]

The framework also emphasises the importance of complying with safety, transparency and accountability provisions. These include for instance developing, deploying and using these technologies while considering the potential safety and security risks by adopting safeguards that comprise a fall-back plan and action,[102] and by emphasising on transparency and traceability by documenting the various elements, processes and phases.[103]

The framework explicitly states that high risk AI technologies must be unbiased and must not create discrimination based on a long list of topics that

[95] Ibid., Art. 60–68.

[96] Ibid., Art. 69–74.

[97] Ibid., p. 3.

[98] European Parliament Framework, Art. 5(1).

[99] Ibid., Art. 5 (3).

[100] Ibid., Art. 6 (2).

[101] Ibid., Art. 7 (1) (2).

[102] Ibid., Art. 8(1) b.

[103] Ibid., Art. 8(2).

include “race, gender, sexual orientation, pregnancy, disability, physical or genetic features, age…”[104] A high-risk AI technology also according to this framework is not supposed to influence elections or promote misinformation. Rather, the framework must protect the rights of workers, encourage high quality education as well as digital literacy, ensure equal opportunities to avoid increasing gender pay gap and comply with IPR rules.[105]

High-risk AI technologies must also consider the environment in their activities as national authorities will evaluate the environmental impact of these activities. Other national or European bodies may perform this task when the law states that. The objective of the environmental assessment in both cases is tackling various environmental issues and problems such as natural resources management, climate change, environmental pollution, energy consumption…[106]

Other rights that must be protected in accordance with the framework include the respect for privacy and protection of personal data particularly the “use and gathering of biometric data for remote identification purposes in public areas, as biometric or facial recognition”[107] and the right to redress according to which an injury or harm caused to natural and legal persons as a result high-risk AI technologies can be redressed by those persons.[108]

These are the main rights protected under the framework where the rest of the provisions are procedural (risk assessment; compliance assessment; European certificate of ethical compliance) and institutional (governance standards and implementation guidance; supervisory authorities; reporting of breaches and protection of reporting persons; coordination at Union level; Exercise of delegation).[109]

3.3. Civil Liability Regime for Artificial Intelligence

The regime makes a distinction between high-risk AI-systems and other AI-systems. The framework imposes on the operator strict liability for high-risk AI-systems in case of damage or harm caused by a “physical or virtual activity, device or process driven by that AI-system”.[110] The European Commission is authorized in this context to include new types of high-risk AI-systems in the scope of this framework as well as delete and change existing high-risk AI-systems.[111]

[104] Ibid., Art. 9(1).

[105] Ibid., Art. 10.

[106] Ibid., Art. 11.

[107] Ibid., Art. 12.

[108] Ibid., Art. 13.

[109] Ibid., Art. 14–21.

[110] European Parliament Resolution., Art. 4(1).

[111] Ibid., Art. 4(2) a, b, c.

Operators in accordance with this framework cannot be exonerated from liability even if they acted with due diligence or if an "autonomous activity, device or process driven by their AI-system" was the cause of damage or harm,[112] but shall not assume responsibility in case of force majeure.[113] In this context, the frontend operator has a responsibility to purchase liability insurance while the backend operator must purchase business liability or product liability insurance covering its services. Existing compulsory insurance or voluntary corporate insurance funds of the frontend operator and the backend operator are considered sufficient if they cover the amount of compensation mentioned in this regulation.[114] Finally, and given the primacy of EU law over national laws, this liability regime will have primacy over national liability regimes in case of conflict concerning "strict liability classification of AI-systems".[115]

The fault-based liability for other AI-systems is mentioned in Article 8 of the framework.[116] In this case, the operator is exonerated from liability if 1) despite taking all the measures for avoiding the activation of AI-system, he did not know that this system was activated; 2) he observed due diligence by performing specific actions mentioned in the framework such as ensuring the selection of a suitable AI-system for the task, monitoring the work and constantly updating these systems. Similarly, to high-risk AI-systems and other AI-systems, the autonomous nature of the activity, device or process cannot be used as a justification for exonerating the operator from liability while force majeure allows him to escape such liability.[117] The operator must even pay compensation when a third party causes the damage in case its untraceable or impecunious,[118] while the producer of an AI-system must cooperate with the operator or the affected person for the identification of the liabilities.[119]

The rest of the provisions of this framework set the necessary rules in the context of strict and fault-based liability such as the rule of compensation and so on.

3.4. Intellectual Property Rights for the Development of Artificial Intelligence Technologies

The EP in this document did not include a draft regulation regarding IPRs in the context of AI. Rather, it stressed the importance of addressing the interplay

[112] Ibid., Art. 4(3).

[113] Ibid.

[114] Ibid., Art. 4(4).

[115] Ibid., Art. 4(5).

[116] Ibid., Art. 8(1).

[117] Ibid., Art. 8(2).

[118] Ibid., Art. 8(3).

[119] Ibid., Art. 8(4).

between IPRs and AI. This is mainly because AI technologies may negatively affect IPRs by complicating the ability to trace IPRs and IPRs application affecting and even preventing the remuneration of human creators that made original work powering AI technologies.[120] Another reason for addressing this interplay is the need for an effective IPR system tailored to the digital age in the general framework of EU's global leadership in AI enabling the introduction of new products on the market and the protection of the Union's patent system.[121]

The EP explicitly stresses the importance of protecting IPRs associated with AI technologies in a multidimensional manner and the need to create legal certainty and trust to promote investments in this field and ensure consumers use of AI technologies in the long term.[122] To that end, it considers the need to continuously reflect on the interaction between AI and IPRs[123] where the focus should be on the implication of each sector and type of IPR on AI technologies. In this context, several factors must be considered mainly "the degree of human intervention, the autonomy of AI, the importance of the role and the origin of the data and copyright-protected material used…".[124]

For instance, among the suggestions, the EP recommended the focus on the way AI technologies would affect existing regulatory framework associated with various IPR issues such as patent law, copyright, trademark, the protection of databases and computer programs...[125] It also for instance calls the commission to explore the idea of testing products while avoiding risks for IPR holders and trade secrets.[126]

The EP made a distinction between "AI-assisted human creations and AI-generated creations".[127] The latter creates new legal challenges related to issues such as "ownership, inventorship and appropriate remuneration".[128] A distinction was made between IPRs used for the creation of AI technologies and IPRs that may be granted for new creations made by AI technologies. The EP stressed the applicability of existing IPR framework when AI is used only to assist an author who is seeking to create something new.[129] Additionally, the EP stressed that AI can be used for IPR enforcement under the condition that a human review and guarantee the transparency of the decisions.[130]

[120] European Parliament, Intellectual property rights., D, p. 3.

[121] Ibid., E, p. 3.

[122] Ibid., 6, p. 5.

[123] Ibid., 7, p. 5.

[124] Ibid., 9, p. 5.

[125] Ibid., 10, p. 6.

[126] Ibid., 12, p. 6.

[127] Ibid.

[128] Ibid.

[129] Ibid., 14, p. 7.

[130] Ibid., 17, p. 8.

These were some of the examples of the many recommendations, statements and recognitions made by the EP in this document highlighting the seriousness granted to the interplay between IPRs and AI while calling the commission to adopt rules that consider all the variables mentioned in this document.

3.5. Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as Tools for an Innovation-Friendly, Future-Proof and Resilient Regulatory Framework that masters Disruptive Challenges in the Digital Age

Through these conclusions, the Council is advocating for the use of regulatory sandboxes and experimentation clauses. It justifies the use of experimentation clauses by highlighting the need for an "agile, innovation-friendly, future-proof, evidence-based and resilient regulatory framework". Such a system will create several benefits such as fostering competitiveness and growth in addition to the technological sovereignty and leadership of Europe in the digital age.[131] It also justifies the use of sandbox regulations by stating that this legal mechanism is already used in various sectors such as finance, health and energy where these sectors often include the use of emerging technologies like AI and blockchain.[132]

In fact, the Council in a series of paragraphs within the document advocated for the use of regulatory sandboxes and experimentation clauses showing the importance given to these mechanisms. For instance, the Council acknowledges that experimentation clauses provide flexibility to the regulatory authorities allowing the testing of innovative technologies, products and services.[133] It also highlighted the benefits of regulatory sandboxes mainly granting the regulators the needed knowledge to regulate innovations at an early stage which is extremely important given the uncertainties and challenges surrounding the new digital technologies.[134]

Nevertheless, the council imposed certain requirements on the use of regulatory sandboxes and experimentation clauses mainly the need to respect important principles primarily subsidiarity, proportionality and the precautionary principle.[135]

In this context, the Council in this document made several recommendations to the Commission regarding regulatory sandboxes and experimentation clauses. For instance, regarding experimentation clauses, the Council calls

[131] Council of the European Union, op. cit., 4, p. 3.

[132] Ibid., 5, p. 3.

[133] Ibid., 9, p. 5.

[134] Ibid., 10, p. 5.

[135] Ibid., 12, p. 5.

the Commission to use experimentation clauses when drafting and reviewing laws in each case and evaluate such use later on.[136] It also calls the Commission to disclose the experimentation clauses that exist within EU law[137] and to provide a list of laws and policies where new experimentation clauses can be applied.[138] Concerning regulatory sandboxes, the Council calls the Commission to exchange information and good practices with member states regarding regulatory sandboxes[139] for various purposes such as establishing an idea of the use of this legal mechanism within the EU[140] and "identifying experiences regarding the legal basis, implementation and evaluation of regulatory sandboxes".[141]

4. AI Data and Algorithm: Lacunas in the EU's GDPR and the AI Regulations

This paper argues that the EU could make its approach to AI regulation more robust by explicitly connecting the regulation of AI data under the GDPR and the proposed AI regulations to create a more meaningfully comprehensive set of AI regulations. Instead, the EU's *ad hoc* approach to AI leaves lacunas that create uncertainties in both mitigating risks and fostering innovation. In particular, this Section explores to what extent the GDPR has failed to regulate AI, and in return how the proposed AI regulations fail to make an explicit attempt to bind to the GDPR.

4.1. Lacunas in Regulation of AI Data

The EU currently regulates data protection under the comprehensive and jurisdictionally extensive regime of the GDPR, as discussed above. While some provisions of the GDRP are relevant to AI, the GDPR does not explicitly refer to AI.[142] Further, the GDPR has been criticized as incompatible with the realities

[136] Ibid., 13 (a), p. 5.

[137] Ibid., 13 (e), p. 6.

[138] Ibid., 13 (f), p. 6.

[139] Ibid., 14, p. 6.

[140] Ibid., 14 (a), p. 6.

[141] Ibid., 14 (b), p. 6.

[142] See SARTOR, G. *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence'* (2020) European Parliamentary Research Service, Panel for the Future of Science and Technology (June 2020) 6 [online]. Available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf>

of big data, which is a necessary component of AI.[143] It is, therefore, important to explore the extent to which the GDPR regulates AI and big data.

Not only does the GDPR not mention AI, but the new ways in which AI processes data in neural networks, challenges the assumptions behind the GDPR.[144] The data protection principles embodied in the GDPR like categories of sensitive data, purpose and necessity (purpose limitations, data minimization), and limits on automated decision-making run counter with the use of data in AI.[145] More specifically, there are a number of issues raised by AI's use of data that remain uncertain and should be addressed by the GDPR or through the proposed AI regulations.[146] These issues include (1) the application of the GDPR's purpose and necessity requirements (purpose limitation and data minimisation); (2) GDPR's coverage of re-identified and inferred data, including in the right to erasure; (3) automated decision-making and profiling in AI; (4) the requirements for specific consent, and (5) the right to know information on automated decision-making and logic used.

First, controllers of big data used by AI will find it hard to comply with the GDPR's purpose and necessity requirements. Commentators like Zarsky have noted that the GDPR is adverse to the prevailing use and practice of big data, and stifles the potential for big data analytics.[147] This is specifically true with regards to the purpose and necessity requirements of the GDPR. Big data often requires the use of methods and usage patterns that may be unforeseeable.[148] Monitoring whether the use of big data analytics complies with the GDPR's purpose and necessity requirements would by expensive, difficult, and perhaps impossible.[149] One can imagine such impossibility when black box algorithms are involved, which some argue should be replaced with explainable algorithms.[150] Under the GDPR, controller and processors of big data would need to inform data subjects of the specific of these unforeseen forms of processing activities.[151]

[143] ZARSKY, T. Z., op. cit., p. 996; ROUVROY, A. *Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data* (2016) 11 [online]. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a6020

[144] SARTOR, G., op. cit., p. 6.

[145] Ibid. Sartor argues that it is still possible to reconcile the GDPR's aim of protecting data privacy and AI.

[146] Ibid (Sartor stating that "a number of AI-related data protections issues are not explicitly answered in the GDPR, which may lead to uncertainties and costs, and may needlessly hamper the development of AI applications").

[147] ZARSKY, T. Z., op. cit., p. 996; ROUVROY, A., op. cit., p. 11.

[148] ZARSKY, T. Z., op. cit., p. 996.

[149] Ibid.

[150] ADADI, A., BERRADA, M. Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*, 2018, vol. 6, pp. 52138.

[151] ZARSKY, T. Z., op. cit., p. 996.

Second, AI raises issues concerning the "re-identification of new personal data from existing de-identified data" through automated or non-automated inference,[152] which may not fall under the GDPR. The GDPR is not explicit in its coverage of AI-inferred data.[153] The GDPR provisions on the rights to erasure, for example, does not explicitly mention AI-based processing, including the erasure of AI-inferred data, which remains unclear.[154]

Third, the GDPR, in a number of provisions, explicitly regulates automated decision-making and profiling, both of which Sartor sees as essential in AI.[155] The GDPR gives data subjects the right not to be subject to a decision based solely on automated decision-making, including profiling. Profiling personal data, however, is necessary in training sets. Applying the GDPR's prohibition on profiling to AI's profiling of training sets would make it difficult and costly to train AI. Sartor argues that a distinction should be made between the use of profiling in training and decision-making, the latter being subject to GDPR rules in processing of new data, even when AI inferred or re-identified.[156]

Article 22(2) of the GDPR, however, allows the data subject to waive the right not to be subject to automated decision-making based on contract and consent. Article 22(2) is an example of an exception that is swallowing the rule since a vast number of consumers are trading their data in exchange for free or convenient digital services, a phenomenon that Zuboff terms "surveillance capitalism."[157] Additionally, Sartor does not foresee a use of AI that does not rely on profiling, but that instead creates individualized profiles. Others argue that the GDPR would essentially allow and potentially encourage the creation of individualized consumer behaviour digital twins that they call 'digital thought clones'.[158]

Fourth, the specific consent requirement under Article 4(11) of the GDPR is difficult to employ in the context of AI's use and processing of big data. Scholars like Sartor view consent as almost always insufficient for AI under the GDPR as a practical matter, and that AI's use of data would have to be justified under Article 6(1)(f), when the processing is "necessary for the purposes of legitimate

[152] SARTOR, G., op. cit., p. 88.

[153] Ibid. Sartor argues that re-identified data should fall within the scope of the GDPR. He also suggest possibly distinguishing between inferences used for decision-making and inferences used for inconsequential activities like computational rather than decision-making.

[154] Ibid., p. 89.

[155] Ibid., p. 88.

[156] Ibid., p. 95.

[157] ZUBOFF, S. *You are Now Remotely Controlled* [online]. Available at: https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html TRUBY, J., BROWN, R. Human Digital Thought Clones: The Holy Grail of Artificial Intelligence for Big Data. *Information & Communications Technology Law*. 2021, vol. 30, no. 2, pp. 140.

[158] Ibid.

interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject."[159] It is unlikely, however, that an AI's use of data would become more legitimate than privacy, which in itself is a fundamental right. Article 6(1)(f), in practice, would like only apply to data not already covered by the GDPR because it is not personal data.

Finally, Articles 13(2)(f), 14(2)(g), and 15(1)(h) of the GDPR require a controller to inform or give access to a data subject of a list of information, and of most relevance to AI is information on the use of automated-decision-making, including the logic used and consequences. According to Sartor, what logic and consequence means, and whether a controller must disclose such information at an individualized level, remains uncertain concerning AI. Additionally, it remains unclear how a programmer could explain the consequence of a black-box neural network's processing of data.

According to Sartor, the GDPR should be more explicit on "what standards should apply to AI processing of personal data, particularly to ensure the acceptability, fairness and reasonability of decisions on individuals."[160]

4.2. Lacunas in the Regulation of AI

While the GDPR regulates the use of data, its data-specific scope makes it untenable for meaningfully regulating the algorithm that in turn regulates the use of data. It is, therefore, no surprise that the GDPR makes no mention of algorithm. Still, the GDPR's regulation of data privacy, inevitably implicates algorithms, albeit in a limited sense. First, it gives a data subject the right to not be subject to decisions based solely on automated decision-making. Second, it gives a data subject the right to know if automated decision-making is used and the logic and consequence of such use. Finally, Article 25 requires controllers to implement data protection principles in the design, which in turn implicates the training of algorithms. The above tangential regulations of algorithm, however, remain substantially lacking because they do not directly affect how an algorithm ought to be designed.

Perhaps, the most significant component of the GDPR in this regard is Article 35(1), which subjects high-risk processing operations, especially those that are large scale and likely to be the case with AI, to mandatory data protection assessment. While the provision is promising and follows a human-centred approach, the term "high-risk" in the GDPR has a limited scope to the rights and freedoms

[159] SARTOR, G., op. cit., p. 88.

[160] Ibid., p. 95.

of natural persons. In contrast, the term high risk carries a different meaning under the civil liability regime for AI. In Article 3(c), the term "high risk" is defined more broadly as "a significant potential…to cause harm or damage to one or more persons in a manner that is random and goes beyond what can reasonably be expected".[161] This creates a double liability for processors of AI data that does not exist for non-AI data, since there are instances when the high risk is in both the processing and the harm. The AI regulation should, therefore, consider those instances when the high-risk exists in both the data and the algorithm.

The EP's civil liability regime regulation only mentions the GDPR in two instances. First, the regulation mentions the GDPR with regards to the designation of an AI-liability representative akin to the GDPR.[162] Second, the regulations requires compliance with the GDPR and other data protection laws whenever the operator uses data generated by the AI system to prove contributory negligence. The use of AI generated data is interesting since it remains unclear under the GDPR whether all AI generated data, specifically inferred or re-identified data, is even covered by the GDPR.[163] According to Sartor, it remains uncertain whether AI-inferred or re-identified personal data even falls under the GDPR.[164] Further, since the GDPR's regulation of AI, and inferred data in particular, remains unclear, it also remains uncertain whether the GDPR would govern such a situation. The issue here, it seems, is the lack of an explicit connection between the GDPR and AI civil liability regulation. Yet, the bigger issue is the failure to regulate the algorithm itself.

The more recent EC Proposal is an improvement on the EP's civil liability regime. Under the Explanatory Memorandum, it addresses the issue of harmonisation with the GDPR, and states that the EC Proposal aims to complement the GDPR "with a set of harmonised rules applicable to the design, development and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems."[165] It also states that the EC Proposal aims to complement laws on non-discrimination, including the design and quality of data used. In other words, the EC Proposal attempts to harmonise the algorithm regulation with the data regulation. It requires "high quality data" for high-risk AI,[166] and recognises the risks posed by divergent national rules and the need for a Union level regulation of AI due to the characteristics of big data.[167]

[161] European Parliament Resolution., Art. 3(c).

[162] Ibid., Preamble 19.

[163] See SARTOR, G., op. cit., p. 88.

[164] Ibid., p. 95.

[165] European Commission Proposal., op. cit., Explanatory Memorandum, Section 1.2.

[166] Ibid., Explanatory Memorandum, Section 2.3 and Preamble Section 44.

[167] Ibid., Explanatory Memorandum, Section 2.2.

The preamble to the EC Proposal in Section 44 states more specifically the role of data in AI and sets a high bar for the quality of data sets being "sufficiently relevant, representative and free of errors" for training, validation and testing.[168] When aimed at avoiding discrimination, Section 44 of the preamble explains the need for an exception to the more stringently regulated special category data under the GDPR. [169] It states that "providers should be able to process also special categories of personal data, as a matter of substantial public interest, in order to ensure the bias monitoring, detection and correction in relation to high-risk AI systems." This is then embodied in Article 10)(5) of the EC Proposal, which states that "To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data… subject to appropriate safeguards for the fundamental rights and freedoms of natural persons…"[170]

However, the EC Proposal creates a large exception to Article 9 of the GDPR that would allow the collection of special category data under the substantial public interest exception. It would be applicable for every use of high-risk AI since it would be for "bias monitoring, detection and correction", an ongoing process within the high-risk AI. In other words, the EC Proposal could potentially eliminate the special category protection of personal data when used in high-risk AI systems so long as the purpose for the collection and use is for bias monitoring, detection, and correction.

While the language of Article 10(5) tries to limit the application of this exception to strict necessity, it becomes questionable whether this exception could be subject to abuse when it does not occur due to an exceptional event but will likely be applied to a regular ongoing process of bias monitoring and detection. In practice, a special category data would have to be collected, and its use allowed, under the Article 10(5) exception for constant bias monitoring and detection without the consent of the data owner. In other words, high-risk AI providers could collect and use data on race for the purported reason of monitoring bias or discrimination based on race.

A question then is how the fundamental rights and freedoms of natural persons would be safeguarded under the broad use of the substantial public interest exception of Article 10(5). Article 10(5) states that safeguards may include "technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation

[168] Ibid., Preamble Section 44.

[169] Ibid., Preamble Section 44.

[170] Ibid., Art. 10(5).

may significantly affect the purpose pursued."[171] In other words, the use of special category data may need to be pseudonymised and may need to have added security. Additionally, Article 17 requires a quality management system for high-risk AI that applies to the management, collection, analysis, labelling, storage, filtration, mining, aggregation, retention and any other operation of data.[172]

However, what remains unclear under Article 10(5) whether persons are allowed to exercise their rights to withdraw consent, the right to erasure, the right to rectification and restriction, the right to object, and the right to access under the GDPR. Article 9(2)(g) of the GDPR allows for the substantial public interest exception but also requires that such an exception shall respect the essence of the right to data protection. Under Article 64, market surveillance authorities are given access to the data and documentation of training, validation and testing datasets and to assess conformity with Title III, Chapter 2, which includes Article 10.[173] This could mean that persons could also be given access to the special category data collected and used for purposes of bias monitoring and detection under Article 10(5). If the substantial public interest exception under Article 10(5) can be done without consent, as it seems to do, then it is treated like the public health/public interest exception of the GDPR that could be accomplished without consent. Since there are different types and uses of AI, however, Article 10(5) should also require AI providers to justify why consent is unnecessary and to explain the risk of bias weighed against the risk of data privacy violation. Article 10(5) should not allow a blanket termination of consent for a purported reason of bias monitoring and detection without weighing the risk of bias in a specific AI application.

In addition, while Articles 40–43 of the GDPR, which encourages the use of codes of conduct and certifications, applies to the application of data protection principle, it does not explicitly refer to AI. For example, it could more explicitly refer to codes of conduct for writing algorithm and use of training sets for AI. It could also include as part of its code of conduct and certification, the prohibition on the use of personal data in algorithms that are designed for manipulative or behaviour influencing purposes, which should at least be disclosed and transparent to data subjects. Some scholars, for example, warn against the normalized use of a digital thought clone.[174] A digital thought clone is made possible because of unregulated (1) design of behaviour manipulative algorithms and (2) data. However, it is not sufficient to regulate data to protect the principles of data privacy because an algorithm designed to manipulate behaviour could still comply with

[171] Ibid., Art. 10(5).

[172] Ibid., Art. 17 (1)(f).

[173] Ibid., Art. 64 and Art. 10(5).

[174] TRUBY, J., BROWN, R., op. cit., p. 140.

data protection principles, yet manipulate the ultimate freedom of all – choice. It is also important to regulate the algorithm and those who design the algorithm. As Sartor states, the GDPR should be more clear on "what applications are to be barred unconditionally, and which may instead be admitted only under specific circumstances".[175] This is especially so because the GDPR "does not take the broader social impacts of mass processing into account".[176]

Moreover, that the committee draft report and the European Parliament's resolution on the civil liability of AI focuses on adopting a high risk/low risk classification of AI's liability risks stands in disconnect from risks that may arise from AI's data use. The use of data by an AI may be difficult to categorize into high risk or low risk. For example, the high risk aspects of AI may not come from the fault of the deployer or programmer, but from an AI's unforeseen or unknown inference of the data. This is especially concerning with regards to black-box neural networks. Article 4(3) of the EP's civil liability regime, however, states that "Operators of high-risk AI-systems shall not be able to exonerate themselves from liability by arguing that they acted with due diligence or that the harm or damage was caused by an autonomous activity, device or process driven by their AI-system".[177] Applying a strict liability standard to such neural networks, while arguably beneficial for a civil liability regime, would create a chilling effect on innovative AI that requires the use of neural networks or that would require the use of an AI that programmers do not fully understand.

The EP's references to human-centred AI in the EP's Framework of ethical aspects of artificial intelligence, robotics and related technologies[178] is perhaps the most promising feature of the EU civil liability regime for AI. The EP Framework addresses human oversight, and prohibits known issues with AI such as discrimination, bias, and uses that would compromise human dignity. AI regulation, however, must go further and directly regulate both the data and the algorithm. For instance, the EP resolution must address explicitly the failure in the design phase, which includes the training of the algorithm, where such biases and discrimination usually arise.

Finally, an AI regulatory framework should include the regulation of the people writing the algorithms and training the algorithms with data. Regulating the profession of programming[179] is as important as regulating the medical and legal profession. It would also set into practice and create a culture of ethical programming. Yet, it is also important to not only think of ethics in terms of

[175] SARTOR, G., op. cit., p. 95.

[176] Ibid., p. 95.

[177] European Parliament Resolution., Art. 4(3).

[178] Ibid.

[179] TRUBY, J., BROWN, R., op. cit., p. 140.

algorithm programming, AI deployment, and the intended use behind AI, but also in terms of data. This is especially true when data privacy is now seen as a fundamental human right. In this regard, there must be regulation of the profession as to what constitutes ethical uses of data for AI.[180] Questions arise here concerning the use of data to create mindclones for digital immortality or the creation of digital thought clones for consumer behaviour tracking. It also raises issues with regards to the use of data on black-box algorithms. Should data be used in AI algorithms that the programmer does not fully understand?

5. Conclusion

Despite the novelty of the regulations examined in this Article be it the GDPR or the various proposals from the EC, EP and the European Council for the establishment of new AI regulations, the discussion concerning the interplay between various regulatory frameworks is one of the traditional and most important topics examined in the legal sphere in particular in the international context. Indeed, there is a huge literature addressing the fragmentation of the law especially international law across various regulatory frameworks due to various factors mainly the increasing technicalities of each field, the technological developments and the need for expertise.[181] At the same time, there is a need to address fragmentation especially when various legal fields develop in parallel while addressing similar issues from a different legal perspective. This is the case for instance in this Article where data protection law and AI rules of the EU are being developed

[180] TRUBY, J. Governing Artificial Intelligence to benefit the UN Sustainable Development Goals. *Sustainable Development*. 2020, vol. 28, no. 4, pp. 946–959.

[181] See generally, KOSKENNIEMI, M., LEINO, P. Fragmentation of International Law? Postmodern Anxieties. *Leiden Journal of International Law*. 2002, vol. 15, no. 3, pp. 553. HAFNER, G. Pros and Cons Ensuing from Fragmentation of International Law. *Michigan Journal of International Law*. 2004, vol 25, no. 4, pp. 849; WELLENS, K. Fragmentation of International Law and Establishing an Accountability Regime for International Organizations: The Role of the Judiciary in Closing the Gap. *Michigan Journal of International Law.* 2004, vol. 25, no. 4, pp. 1159; SIMMA, B. Universality of International Law from the Perspective of a Practitioner. *European Journal of International Law*. 2009, vol. 20, no. 2, pp. 265; GOURGOURINIS, A. General/Particular International Law and Primary/Secondary Rules: Unitary Terminology of a Fragmented System. *European Journal of International Law*. 2011, vol. 22, no. 4 , pp. 993; STARK, B. International Law from the Bottom Up: Fragmentation and Transformation. *University of Pennsylvania Journal of International Law*. 2013, vol. 34, no. 4, pp. 687; BROUDE, T. Keep Calm and Carry On: Martti Koskenniemi and the Fragmentation of International Law. *Temple International & Comparative Law Journal*. 2013, vol. 27, no. 2, pp. 279; MEGIDDO, T. Beyond Fragmentation: On International Laws Integrationist Forces. *The Yale Journal of International Law*, vol. 44, no. 1, pp. 115.

in parallel even though and as highlighted in the analysis, both are addressing similar issues requiring the creation of synergies and the harmonization of the rules within the legal frameworks that are being developed.

In that sense, the authors in a way examined an old problem applied to new regulations attempting this time to bring new suggestions to solve it. Indeed, after the analysis of the lacunas in the regulation of AI Data and the lacunas in the regulation of AI, the authors proceeded to provide suggestions on how to address these lacunas by providing concrete suggestions to that end. These suggestions focused on the inclusion of specific texts and provisions within both the GDPR and the proposed AI regulations to address the shortcomings as well as the creation of a much-needed synergy between these regulatory frameworks that are developing in parallel but are interdependent. The authors hope from the analysis and the suggestions made that not only these recommendations are taken into account but that rather also the future regulations to be adopted concerning data protection and AI at the EU level as well as the international level to consider the need to create synergies between these two legal fields given their interdependence.

List of references

ADADI, A., BERRADA, M. Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*. 2018, vol. 6, pp. 52138–52160.

BHAIMIA, S. *The General Data Protection Regulation: the Next Generation of EU Data Protection. Legal Information Management*. 2018, vol. 18, no. 1, pp. 21–28.

BROUDE, T. Keep Calm and Carry On: Martti Koskenniemi and the Fragmentation of International Law. *Temple International & Comparative Law Journal*. 2013, vol. 27, no. 2, pp. 279–292.

BROWN, R. Property Ownership and the Legal Personhood of Artificial Intelligence. *Information & Communications Technology Law*. 2021, vol. 30, no. 2, pp. 208–234.

Commission Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119). [online]. Available at: https://op.europa.eu/s/omni [GDPR].

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Artificial Intelligence for Europe {SWD(2018) 137 final}.

Council of the European Union, Council Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age, Brussels, Nov. 16, 2020.

DE HERT, P., PAPAKONSTANTINOU, V. The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services. *Computer Law & Security Review*. 2018, vol. 34, no. 2, pp. 193–203.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

European Commission, AI-HLEG, High-Level Expert Group on Artificial Intelligence. A definition of AI: Main capabilities and Scientific Disciplines [online]. Available at: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

European Commission, *Fundamental Rights* [online]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

European 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 (2021/0106) (COD) COM (2021) 206 Final.

European Data Protection Supervisor, The History of the General Data Protection Regulation. [online]. Available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [hereinafter History of GDPR].

European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). [online]. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html

European Parliament, Framework of ethical aspects of artificial intelligence, robotics and related Technologies. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)).

European Parliament, Intellectual property rights for the development of artificial intelligence Technologies. European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI)).

FEFER, R. F. *EU Data Protection Rules and U.S. Implications* [online]. Available at: https://fas.org/sgp/crs/row/IF10896.pdf

GOOD, I. J. Speculations Concerning the First Ultra Intelligent Machine. In ALT, F., RUBINOFF, M. (eds). *Advances in Computers*. New York: Academic Press, 1965. vol 6, pp. 31–88.

Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:131/12 [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

GOURGOURINIS, A. General/Particular International Law and Primary/Secondary Rules: Unitary Terminology of a Fragmented System. *European Journal of International Law*. 2011, vol. 22, no. 4, pp. 993–1026.

HAFNER, G. Pros and Cons Ensuing from Fragmentation of International Law. *Michigan Journal of International Law*. 2004, vol 25, no. 4, pp. 849–863.

HILDEBRANDT, M. The Artificial Intelligence of European Union Law. *German Law Journal* 2020, vol. 21, no. 1, pp. 74–79.

HOOFNAGLE, C. J., VAN DER SLOOT, B., BORGESIUS, F. Z. The European Union General Data Protection Regulation: What It is and What It Means. *Information & Communications Technology Law*. 2019, vol. 28, no. 1, pp. 65–98.

KOOPS, B.-J. The Trouble with European Data Protection Law. *International Data Privacy Law*, 2014, vol. 4, no. 4, pp. 250–261.

KOSKENNIEMI, M., LEINO, P. Fragmentation of International Law? Postmodern Anxieties. *Leiden Journal of International Law*. 2002, vol. 15, no. 3, pp. 553–579.

KOSTA, E. *Consent in European Data Protection Law*. Martinus Nijhoff, 2013.

LOENEN, B., KULK, S., PLOEGER, H. Data Protection Legislation: A Very Hungry Caterpillar: The Case of Mapping Data in the European Union. *Government Information Quarterly*. 2016, vol. 33, no. 2, pp. 338–345.

MEDDIN, E. The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement On Trade in Services. *American University International Law Review*. 2020, vol. 35, no. 4, pp. 997–1036.

MEGIDDO, T. Beyond Fragmentation: On International Laws Integrationist Forces. *The Yale Journal of International Law*. vol. 44, no. 1, pp. 115–147.

MONAJEMI, M. Privacy Regulation in the Age of Biometrics that Deal with a New World Order of Information. *University of Miami International & Comparative Law Review*. 2018, vol. 25, no. 2, pp. 371–408.

OECD, *Artificial Intelligence in Society*. Paris: OECD Publishing, 2019.

PETERSEN, K. GDPR: What (and Why) You Need to Know About EU Data Protection Law. *AUG Utah Bar Journal*. 2018, vol. 31, no. 4, pp. 12–16.

PRESCOTT, T. J. The AI Singularity and Runaway Human Intelligence. In: LEPORA, N., MURA, A., KRAPP, H. (eds.). *Biomimetic and Biohybrid Systems*. Heidelberg: Springer-Verlag, 2013.

PURTOVA, N. The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. *Law, Innovation and Technology*. 2018, vol. 10, no. 1, pp. 40–81.

REDING, V. The Upcoming Data Protection Reform for the European Union. *International Data Privacy Law*. 2011, vol. 1, no. 1, pp. 3–5.

ROUVROY, A. Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data (2016) 11 [online]. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a6020

SARTOR, G. The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (2020) European Parliamentary Research Service, Panel for the Future of Science and Technology (June 2020) 6 [online]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

SEARLE, J. R. Minds, Brains, and Programs. *Behavioral and Brain Sciences*. 1980, vol. 3, no. 3, pp. 417–424.

SHEIKH, S. *Understanding the Role of Artificial Intelligence and Its Future Social Impact.* Hershey: IGI Global, 2020.

SIMMA, B. Universality of International Law from the Perspective of a Practitioner. *European Journal of International Law*. 2009, vol. 20, no. 2, pp. 265–297.

STARK, B. International Law from the Bottom Up: Fragmentation and Transformation. *University of Pennsylvania Journal of International Law*. 2013, vol. 34, no. 4, pp. 687–742.

TIKKINEN-PIRI, C., ROHUNEN, A., MARKKULA, J. EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies. *Computer Law & Security Review*. 2018, vol. 34, no. 1, pp. 134–153.

TRUBY, J., BROWN, R., DAHDAL, A. Banking on AI: Mandating a Proactive Approach to AI Regulation in the Financial Sector. *Law and Financial Markets Review*. 2020, vol. 14, no. 2, pp. 110–120.

TRUBY, J. Governing Artificial Intelligence to benefit the UN Sustainable Development Goals. *Sustainable Development*. 2020, vol. 28, no. 4, pp. 946–959.

TRUBY, J., BROWN, R. Human Digital Thought Clones: The Holy Grail of Artificial Intelligence for Big Data. *Information & Communications Technology Law*. 2021, vol. 30, no. 2, pp. 140–168.

VEALE, M. A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence. *European Journal of Risk Regulation*. 2020, vol. 11, no. 1, pp. 1.

VESNIC-ALUJEVIC, L., NASCIMENTO, S., PÓLVORA, A. Societal and Ethical Impacts of Artificial Intelligence: Critical Notes on European Policy Frameworks. *Telecommunications Policy*. 2020, vol. 44, no. 6, pp. 101961.

VOIGT, P., VON DEM BUSSCHE, A. *The EU General Data Protection Regulation (GDPR): A Practical Guide.* Cham: Springer, 2017.

VOSS, W. G. European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. *The Business Lawyer*. 2017, vol. 72, no. 1, pp. 221–233.

WELLENS, K. Fragmentation of International Law and Establishing an Accountability Regime for International Organizations: The Role of the Judiciary in Closing the Gap. *Michigan Journal of International Law.* 2004, vol. 25, no. 4, pp. 1159–1181.

ZARSKY, T. Z. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*. 2017, vol. 47, no. 2, pp. 995–1020.

ZUBOFF, S. You are Now Remotely Controlled [online]. Available at: https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html