Marie Chum

L.L.M. Europäisches Recht und Rechtsvergleich

Balancing GDPR requirements for the protection of data subjects with the policy goal of strengthening AI uptake and innovation under the European Commission's 'AI Regulation' proposal of April 2021

Unter der Betreuung von **Prof. Dr. iur. Dipl.-Biol. Herbert Zech**

Lehrstuhl für Bürgerliches Recht, Technik- und IT-Recht an der Humboldt-Universität zu Berlin

und **Dr. Lucas Lasota**

Wissenschaftlicher Mitarbeiter

Verteidigt am **6. Juli 2022**

Acknowledgements

I would like to thank my supervisor for his constant support and feedback. His insight was invaluable to my research.

TABLE OF CONTENTS

BIBLIOGRAPHY

Albinati F, 'Glossary' (*European Data Protection Supervisor - European Data Protection Supervisor* 13 December 2016) https://edps.europa.eu/data-protection/data-protection/glossary_en accessed 22 May 2022.

Article 19, *Privacy and Freedom of Expression in the Age of Artificial Intelligence* (Article 19 2018)

Article 29 Data Protection Working Party, 'Opinion 3/2010 on the Principle of Accountability [WP 173]' (2010)

——, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks [WP 218]' (2014)

——, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 [WP 251]' (2017)

Bishop ET and others, 'Racial Disparities in the Massachusetts Criminal System' (Criminal Justice Policy Program 2020) https://hls.harvard.edu/content/uploads/2020/11/Massachusetts-Racial-Disparity-Report-FINAL.pdf accessed 16 May 2022

Bryson JJ, Diamantis ME and Grant TD, 'Of, For, and by the People: The Legal Lacuna of Synthetic Persons' (2017) 25 Artificial Intelligence and Law 273

Campbell Black H and West Publishing Company, *Black's Law Dictionary : Containing Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern, and Including the Principal Terms of International, Constitutional, Ecclesiastical and Commercial Law, and Medical Jurisprudence, with a Collection of Legal Maxims, Numerous Select Titles from the Roman, Modern Civil, Scotch, French, Spanish, and Mexican Law, and Other Foreign Systems, and a Table of Abbreviations* (2nd edn., West Publishing Co 1933)

Castets-Renard C, 'Quel Droit de l'Intelligence Artificielle Dans l'Union Européenne ? Ou Les Multiples Ambitions Normatives de l'AI Act' (2022) 2 Dalloz IP/IT

Chander S and Jakubowska E, 'EU's AI Law Needs Major Changes to Prevent Discrimination and Mass Surveillance' (*European Digital Rights (EDRi)* 28 April 2021) https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/ accessed 12 May 2022

Coeckelbergh M, *AI Ethics* (The MIT Press 2020)

D'Amato A, 'The Moral and Legal Basis for Sanctions' (Northwestern University School of Law Scholarly Commons 2010) http://scholarlycommons.law.northwestern.edu/facultyworkingpapers/95 accessed 23 May 2022

De Terwangne C, *Le Règlement Général Sur La Protection Des Données (RGPD/GDPR) : Analyse Approfondie* (Larcier 2018)

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)' https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf accessed 19 May 2022

EDPS, 'Transparency | European Data Protection Supervisor' (*edps.europa.eu*) https://edps.europa.eu/data-protection/our-work/subjects/transparency_en accessed 22 May 2022

European Commission, '[Archived Content] Opinions and Recommendations – European Commission' (*ec.europa.eu*) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm accessed 17 May 2022

European Council on Refugees and Exiles, 'The EU Charter of Fundamental Rights; an Indispensable Instrument in the Field of Asylum' (2017) https://www.ecre.org/wp-content/uploads/2017/02/The-EU-Charter-of-Fundamental-Rights.pdf accessed 19 May 2022

European Parliament, 'Report with Recommendations to the Commission on Civil Law Rules on Robotics [2015/2103(INL)]' (2015)

Ferrand F, 'Genèse', *Droit et pratique de la procédure civile 2021/2022* (Dalloz 2021)

Fjeld J and others, 'Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI' (Berkman Klein Center Research Publication 2020)

Haas G and Astier S, *Intelligence Artificielle : Enjeux Éthiques et Juridiques* (Éditions Eni 2021)

Hamilton A and others, *The Federalist Papers : A Collection of Essays Written in Support of the Constitution of the United States : From the Original Text of Alexander Hamilton, James Madison, John Jay* (Johns Hopkins University Press 1981)

Hidvegi F, Leufer D and Massé E, 'The EU Should Regulate AI on the Basis of Rights, Not Risks' (*Access Now* 17 February 2021) https://www.accessnow.org/eu-regulation-ai-risk-based-approach/ accessed 12 May 2022

Hijmans H, Kranenborg H and Hustinx PJ, *Data Protection Anno 2014 : How to Restore Trust? : Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*(Intersentia, Portland, Or, Usa 2014)

Informationssicherheit Datenschutz Compliance, 'AI & GDPR: Minimise Compliance Costs with Anonymisation and Pseudonymisation!' (*ISiCO Datenschutz* 17 July 2019) https://www.isico-datenschutz.de/en/ai-gdpr-anonymisation-and-pseudonymisation/ accessed 22 May 2022

Institute of Electrical and Electronics Engineers Standards Association, 'The Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)' (*IEEE Standards Association*) https://standards.ieee.org/industry-connections/ecpais/ accessed 18 May 2022

Joao Silva Sequeira MI and others, *A World with Robots International Conference on Robot Ethics: ICRE 2015.* (Cham Springer International Publishing Springer 2018)

Kesa A and Kerikmäe T, 'Artificial Intelligence and the GDPR: Inevitable Nemeses?' (2020) 10 TalTech Journal of European Studies 67 https://journals.scholarsportal.info/pdf/26744619/v10i0003/68_aiatgin.xml accessed 21 May 2022

Köbler G and Verlag Vahlen F, *Juristisches Wörterbuch Für Studium Und Ausbildung* (München Vahlen, Franz 2022)

Law J and Martin EA, 'Repugnancy'

Lee K-F and Qiufan Chen, *Ai 2041* (Currency 2021)

Lee O, 'Artificial Intelligence and Data Protection – How the GDPR Regulates AI' (Centre for Information Policy Leadership 2020) https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf accessed 14 May 2022

Lee P and Powers L, 'Data Protection Issues in AI' (*www.youtube.com* 23 April 2021) https://www.youtube.com/watch?v=aV4BpDpEWg0 accessed 16 May 2022

Limbach F and Ferrand F, *Le Consentement Contractuel à l'Épreuve Des Conditions Générales : De l'Utilité Du Concept de Déclaration de Volonté* (LGDJ 2004)

Markus Dirk Dubber, Pasquale F and Sunit Das, *The Oxford Handbook of Ethics of AI* (Oxford University Press 2020)

Müller VC, 'Ethics of Artificial Intelligence and Robotics' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Metaphysics Research Lab 2020) https://plato.stanford.edu/archives/sum2021/entries/ethics-ai/ accessed 7 May 2022

Owen R, Bessant JR and Heintz M, *Responsible Innovation : Managing the Responsible Emergence of Science and Innovation in Society* (John Wiley & Sons Inc 2013)

'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance)'

‘Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and Repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA Relevance.)’

Rochel J and Evéquoz F, ‘Getting into the Engine Room: A Blueprint to Investigate the Shadowy Steps of AI Ethics’ (2020) 36 AI & SOCIETY

Russell S and Norvig P, *Artificial Intelligence : A Modern Approach* (3rd edn., Pearson 2010)

Sartor G and Lagioia F, ‘The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence’ (Scientific Foresight Unit (STOA) EPRS | European Parliamentary Research Service 2020) https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf accessed 22 May 2022

Schuett J, ‘A Legal Definition of AI’ (2019) 3 https://www.researchgate.net/publication/335600149_A_Legal_Definition_of_AI accessed 21 May 2022

Stilgoe J, Owen R and Macnaghten P, ‘Developing a Framework for Responsible Innovation’ (2013) 42 Research Policy 1568 https://www.sciencedirect.com/science/article/pii/S0048733313000930 accessed 17 May 2022

Taylor NP, ‘Notified Bodies Join Chorus of Criticism of Proposed European AI Regs’ (*MedTech Dive*6 October 2021) https://www.medtechdive.com/news/notified-bodies-EU-proposed-artificial-intelligence-ai-regulation/608880/ accessed 10 May 2022

The European Association Medical Devices - Notified Bodies, ‘Position Paper on European Artificial Intelligence Regulation’ (2021) https://www.team-nb.org/wp-content/uploads/2021/10/Team-NB-PositionPaper-Artificial-Intelligence.pdf accessed 14 May 2022

The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, ‘Embedding Values into Autonomous and Intelligent Systems’, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (2019)

Van de Poel I and Sand M, ‘Varieties of Responsibility: Two Problems of Responsible Innovation’ (2018) 198 Synthese

Van den Hoven van Genderen R, ‘Do We Need New Legal Personhood in the Age of Robots and AI?’ in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), *Robotics, AI and the Future of Law* (Springer, Singapore 2018)

Villaronga EF, Kieseberg P and Li T, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2018) 34 Computer Law & Security Review 304 http://tiffanyli.com/wp-content/uploads/2018/08/Humans-Forget-Machines-Remember_Final-PDF.pdf
accessed 22 May 2022

Voss A, 'DRAFT REPORT on Artificial Intelligence in a Digital Age' (Special Committee on Artificial Intelligence in a Digital Age 2021)

Wolford B, 'What Is GDPR, the EU's New Data Protection Law?' (*GDPR.eu* 7 November 2018) https://gdpr.eu/what-is-gdpr/
accessed 9 May 2022

Wouters J, 'Revisiting Art. 2 TEU: A True Union of Values?' (2020) 5 European Papers 255
NV Algemene Transporten Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration (European Court of Justice)

Consolidated version of the Treaty on European Union

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Ethics Guidelines for Trustworthy AI 2019

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

Rome Declaration on Responsible Research and Innovation in Europe 2014

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AIA	Artificial Intelligence Act
Art. 29 WP	Article 29 Data Protection Working Party
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights advocacy group
EU	European Union
EUDPR	Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018
GDPR	General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
IEEE	Institute of Electrical and Electronics Engineers association
IVDR	In-Vitro medical devices Regulation - Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017
LED	Law Enforcement Directive - Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016
MDR	Medical Devices Regulation - Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017
TFEU	Treaty on the Functioning of the European Union (consolidated version)

"Whenever regulation is mentioned with respect to AI development and use, usually two issues are mentioned: firstly, the fear that regulation will stifle innovation and progress; and secondly, the issue of whether current laws and regulations are at all sufficient to deal with the complexities of AI. In my opinion, both are too short-sighted."[1]

- *Virginia Dignum, 2020*

INTRODUCTION

The relationship between artificial intelligence (AI) and data protection is a recent albeit increasingly significant issue of contemporary society. Its fostering debates are largely caused by the very definition of AI, around which the general lack of consensus[2] was effectively resumed according to contemporary understanding by philosopher Vincent C. Müller, as "any kind of artificial computational system that shows intelligent behaviour, i.e., complex behaviour that is conducive to reaching goals".[3] Intelligent behaviour translates into algorithm trains with data sets to achieve the goals aforementioned, hence implying, in the era of Big Data, the collection and use of mass personal information.[4] The European Parliament and the Council of the European Union have regulated the processing of personal data through

[1] Virginia Dignum, 'Responsibility and Artificial Intelligence', in Markus D. Dubber, Frank Pasquale and Sunit Das (eds.), *The Oxford Handbook of Ethics of AI* (2020)

[2] Jonas Schuett, 'A Legal Definition of AI' (2019), 3

[3] Vincent C Müller, 'Ethics of Artificial Intelligence and Robotics' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Metaphysics Research Lab 2020) <https://plato.stanford.edu/archives/sum2021/entries/ethics-ai/>.

[4] Giovanni Sartor and Francesca Lagioia, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (Scientific Foresight Unit (STOA) EPRS | European Parliamentary Research Service 2020), 1, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

three main legal acts: the Law Enforcement Directive (LED), which was adopted on the 27th April 2016 and had to be transposed into national law by the 6th May 2018,[5] the Data Protection Regulation for the European Union institutions, offices, bodies and agencies (EUDPR), which was adopted on the 23rd October 2018 and was enforceable as of its publication,[6] and the General Data Protection Regulation (GDPR), which was adopted on the 27th April 2016 and became enforceable on the 25th May 2018.[7] Whereas both LED and the EUDPR are integral parts of the data protection framework in the EU adopted on the basis of a general right to the protection of personal data,[8] their scope is specific to the processing of personal data in law enforcement[9] and by EU institutions, bodies, offices and agencies[10] respectively. That is why this essay will only focus on the GDPR, the provisions of which apply to the processing and free movement of personal data generally and broadly concern the actors in the field of AI.[11] Replacing Directive 95/46/CE or the Data Protection Directive of 1995[12] and Convention 108,[13] the GDPR now holds the legal basis for some of the most significant principles of data protection and rights of data subjects, including fairness, lawfulness and transparency of processing[14] and the respective rights to rectification and erasure of personal data[1516]. In short, the GDPR aims to ensure that the uses of data are lawful on one hand, and that individuals have an ability to control such use of their personal data on the other.

---

[5] Directive (EU) 2016/680

[6] Regulation (EU) 2018/1725

[7] Regulation (EU) 2016/679

[8] Consolidated Version of the Treaty on European Union [2012] OJ C326/1, Art. 16

[9] Directive (EU) 2016/680, Art. 1 (1)

[10] Regulation (EU) 2018/1725, Art. 1 (1)

[11] Regulation (EU) 2016/679, Art. 2

[12] Directive 95/46/EC

[13] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108

[14] Regulation (EU) 2016/679, Art. 5

[15] Regulation (EU) 2016/679, Art. 16

[16] Regulation (EU) 2016/679, Art. 17

Deemed to be the "toughest privacy and security law in the world",[17] the GDPR was generally welcomed by advocates of a more extensive approach to data protection, as it effectively implemented stringent substantial provisions in defence of privacy and security and was of broad application:[18] particularly, personal data under the GDPR is an expansive term, defined as information that can be used to distinguish one person from another.[19] The vaster aspect of the concept held the consequence that it could easily be used to control the flow of personal data into the European market. However, some dissatisfaction was noted in sectors relating to artificial intelligence. In December 2016, the University of Oxford published a paper calling attention to a potential doubt in "both the legal existence and the feasibility" of the right of data subjects to information and particularly explanation for automated decisions under the GDPR.[20] The same concern was raised by Professor Robert van den Hoven van Genderen, who deemed this insufficiency to be caused by the "non-technological orientation and the hinge on conventional directions of thinking" of the GDPR.[21] The GDPR's lack in explicitly addressing AI may have been due to its aim primarily pertaining rather to issues raised by the Internet, as the place of AI on contemporary society had yet to be assessed.[22]

---

[17] Ben Wolford, 'What Is GDPR, the EU's New Data Protection Law?' (GDPR.eu7 November 2018) <https://gdpr.eu/what-is-gdpr/>.

[18] Jessica Fjeld and others, 'Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI' (Berkman Klein Center Research Publication 2020), 21.

[19] Regulation (EU) 2016/679, Art. 4

[20] Mark Coeckelbergh, *AI Ethics* (The MIT Press 2020).

[21] Robert Van den Hoven van Genderen, 'Do We Need New Legal Personhood in the Age of Robots and AI?' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), *Robotics, AI and the Future of Law*(Springer, Singapore 2018), 51.

[22] Giovanni Sartor and Francesca Lagioia, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (Scientific Foresight Unit (STOA) EPRS | European Parliamentary Research Service 2020), 35, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

What Timnit Gebru called a "rapid permeation of AI into society"[23] coupled with the affirmed role of legislation in embedding values into AI systems[24] formed the basis for a subsequent adoption of AI-specific legislation on the level of the European Union. In April 2021, the European Commission published the 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, hereinafter referred to as 'the Proposal', currently ongoing a first reading before the Council of the European Union.[25] It defines artificial intelligence under Article 3 (1) as "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".[26] The significance of this definition for data protection, which was touched on above, will be developed further in the course of this essay. For now, it serves to underline the legal basis given by the European Commission to the contemporary majority view of AI as an "intelligent agent".[27] Additionally, the Proposal bases its provisions on four policy goals listed in its Explanatory Memorandum:

- *"ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;*

[23] Timnit Gebru, 'Race and Gender', in Markus D. Dubber, Frank Pasquale and Sunit Das (ed.), *The Oxford Handbook of Ethics of AI* (2020)

[24] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 'Embedding Values into Autonomous and Intelligent Systems', *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (2019), 169.

[25] COM/2021/206 final

[26] COM/2021/206 final, Art. 3

[27] Stuart Russell and Peter Norvig, *Artificial Intelligence : A Modern Approach* (3rd edn., Pearson 2010).

- *ensure legal certainty to facilitate investment and innovation in AI;*

- *enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;*

- *facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation."*[28]

Because of both the data-intensive nature of AI systems and the highly protective approach of the GDPR concerning principles of data protection and the rights of data subjects, the objective of compatibility with fundamental rights safeguarded by existing law and specifically the GDPR would naturally be expected to conflict with that of AI uptake and innovation.[29] In the context of the recently issued Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), in the version of April 2021, an adequate legal analysis of the issue would translate into contrasting the provisions of the Proposal that effectively, whether implicit or express, support AI uptake and innovation, with those of the GDPR that successfully implement data protection rights and principles in the interest of data subjects. Thus, this essay will concern points specifically made in the Proposal in support of AI uptake and innovation and subsequently susceptible to cause friction with the provisions of the GDPR for the protection of data subjects, as well as safeguards implemented in the Proposal that may allude to the GDPR.

[28] Explanatory Memorandum to COM/2021/206 final, para 1.1

[29] Aleksandr Kesa and Tanel Kerikmäe, 'Artificial Intelligence and the GDPR: Inevitable Nemeses?' (2020) 10 TalTech Journal of European Studies, 67-90. <https://journals.scholarsportal.info/pdf/26744619/v10i0003/68_aiatgin.xml>

Rendering conspicuous the complexities faced by the European Commission in balancing the need for adequate protection of personal data and that of efficient AI development served as the primary motivation behind this essay. It aims to show the extent to which the provisions in support of AI uptake and innovation put forth by the Proposal are sufficiently compatible with data protection requirements under the GDPR, clearly identifying their role in the larger strides to safeguard an adequate data protection framework in the context of AI. It endeavours to demonstrate how, despite not fully reconciling AI and the GDPR, the European Commission gives a satisfactory formula to provide the latter with a predominant role in regulating AI. As the argumentation developed throughout this essay will therefore be highly prospective, the qualitative analysis of legislation and doctrine solely will be paramount to its demonstration.

This essay has two main topics of discussion: the operational framework envisioned between the General Data Protection Regulation and the Artificial Intelligence Act Proposal, and the substantial tensions between promoting AI uptake and innovation and safeguarding the protection of data subjects under the GDPR. The first section will analyse the interaction envisioned by the European Commission for the Proposal and the GDPR. The criticism outlined would pertain to the explicit references and, concerning the specific point of the lacking mention of data subjects, the lack of reference in some parts, to the general place given to the framework of the GDPR as effectively set out in the AI Act Proposal. It will explain the potential paradox between the visible intent for the Proposal to complement the GDPR, inferred essentially from the language of the Proposal by the European Commission, and the lack of clarity surrounding the extent to which the regulations would be meant to operate together: such would notably be supposed by disharmonised enforcement mechanisms pertaining to the GDPR and the envisioned AI Act respectively. This section further endeavours to explicate the personal speculation that this inconsistency

may be intentional and reflect a call of the European Commission for supplementary discussions, aimed at resolving prevailing complex issues of AI and data protection.

The second section will review the substantive choices made by the European Commission in relation to the promotion of AI uptake and innovation, contrasting them with the relevant GDPR requirements and discussing the extent of potential issues subsequently raised. The disparity between the risk-based approaches envisioned by the GDPR and the Proposal respectively serves as an excellent illustration of the core friction point between the data protection framework safeguarded by the first and the goal of AI uptake and innovation aimed for by the second, outlining the vital role policy plays in regulating AI in a manner that is consistent with the protection of personal data. Furthermore, the Proposal saw the tailored application of GDPR principles to AI development, namely data protection by design and by default, accountability and the right not to be subject to a decision based solely on automated processing. This section will explain their roles and effectiveness, arguing that they formed a fairly satisfactory illustration of effective balance between the development of an efficient AI system and the adequate safeguard of core data protection principles.

PART ONE: The operational framework envisioned between the General Data Protection Regulation and the Artificial Intelligence Act Proposal

The provisions of the Proposal emphasise an intent of the European Commission for the envisioned Artificial Intelligence Act (AIA) to complement the GDPR (I). However, the extent of their proximity in their interaction has yet to be determined (II).

I. The complementary nature of the AI Act Proposal to the GDPR

Although a minute hierarchy placing the importance of the GDPR above that of the Proposal may be drawn from criteria specific to the nature of both pieces of legislation as regulations (A), explicit references to the GDPR (B) and the absence of references to data subjects (C) in the Proposal constitute the most significant indications of the complementary nature of the envisioned Artificial Intelligence Act to the GDPR.

A. Minimal hierarchy

The choice of a regulation as a legal instrument in the fields concerned by the GDPR and the Proposal, namely data protection and artificial intelligence, was generally deemed to be the most adequate to both promote AI uptake and innovation and regulate AI throughout the EU broadly,[303][132] and appears to place the issues raised on a similar level: whereas the Treaty for the Functioning of the European Union (TFEU) places the binding nature of a directive merely on specific objectives to be reached, hence leaving the choice in means used to attain these

[30] Explanatory Memorandum to COM/2021/206 final, para 2.4

[31] Explanatory Memorandum to Regulation (EU) 2016/679, para 13

[32] Cécile De Terwangne, 'Le choix d'un Règlement', in *Le Règlement Général Sur La Protection Des Données (RGPD/GDPR) : Analyse Approfondie* (Larcier 2018).

objectives to the Member-States,[33] it defines regulations as being "binding in their entirety", including in the means implemented, and as having direct applicability in all Member-States.[34] It is worth noting that the immediate enforceability induced by direct applicability implies a stronger protection of subjects concerned, including data subjects.[35] Professor Frédérique Ferrand described the advantage of a regulation as that of leading to a more comprehensive and apparent legislation;[36] naturally, where a field of issues would be too consequential to allow for disparities between the national legislations, the adoption of a regulation would be preferred over that of a directive. Severity in the potential consequences of an absence of harmonisation in the European Union is relevant to both data protection and artificial intelligence: the stipulations of the GDPR aim to provide "legal certainty and transparency for economic operators" and "the same level of legally enforceable rights and obligations and responsibilities for controllers and processors" to data subject, as well as effective monitoring and sanctions, tracing the necessity for such provisions to "a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market".[37] Such considerations would be agreeable: disparities in the core characteristics of data protection would considerably hinder the internal market: data would not be able to move freely, as the competent authorities would stop the processing of data from another Member-State with data protection legislation deemed insufficient, and the data subjects would not be willing to allow their data to be processed in such Member-States.

---

[33] Consolidated Version of the Treaty on European Union [2012] OJ C326/1, Art. 288, S.3

[34] Consolidated Version of the Treaty on European Union [2012] OJ C326/1, Art. 288, S.2

[35] Case 26-62, *NV Algemene Transporten Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration* [1963], ECLI:EU:C:1963:1

[36] Frédérique Ferrand, 'Genèse', Droit et pratique de la procédure civile 2021/2022 (Dalloz 2021), 261.41

[37] Explanatory Memorandum to Regulation (EU) 2016/679, para 13

Similarly, the Proposal justifies its choice of the legal instrument of a regulation by its capacity to "reduce legal fragmentation and facilitate the development of a single market for lawful, safe and trustworthy AI systems", speaking of the "the need for a uniform application of the new rules, such as definition of AI, the prohibition of certain harmful AI-enabled practices and the classification of certain AI systems".[38] The choice of the European Commission to be binding on all Member-States regarding the means implemented to regulate AI in the EU would be greatly appreciated by the IEEE Global Initiative, who heavily defended the insufficiency of universal rights in devising an AI system that would conform to the norms of its community.[39] The criticism would only be emphasized when considering that the European Union's nature as a union of values continues to be heavily discussed;[40] directives based on guidance on values would be insufficient, as disparities between Member-States would be likely to have been major and therefore constitute a consequential hinderance on the development of artificial intelligence in the European Union. For example, in relation to the risk-based approach utilised by the Proposal, if the European Commission had proposed a directive instead of a regulation, Member-States could have been able to draft their own classifications: specific AI technologies, for example the one used to create deep fakes, could have been classified as high risk in Germany and low risk in France, hindering the internal market in the same way a disparity between the level of protection of data in two Member-States would have.

[38] Explanatory Memorandum to COM/2021/206 final, para 2.4

[39] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 'Embedding Values into Autonomous and Intelligent Systems', *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (2019), 169.

[40] Wouters, Jan, "Revisiting Art. 2 TEU: A True Union of Values?" (2020), *Re-conceptualizing Authority and Legitimacy in the EU*, European Papers, Vol. 5, 2020, No 1, pp. 255-277, ISSN 2499-8249 - doi: 10.15166/2499-8249/376

The respective territorial scopes of the GDPR and the Proposal, however, diverge and may constitute a hint of the European Union's greater concern for safeguarding data protection in comparison to regulating AI. The GDPR clearly applies to any and all processing of personal data that bears any relationship to the European Union, as the territorial requirements it explicitly states are inherently broad:[41] "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not", the "processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union", or the "processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law" all call for the application of the GDPR.[42] Although it does exclude the processing of personal data for the purpose of law enforcement from its application, the gap is remedied by LED, which was issued on the same day as the GDPR.[43] By contrast, while the Proposal's territorial scope appears otherwise similar to that of the GDPR, it holds the notable nuance of an exclusion to its application for "public authorities in a third country" and "international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States."[44] A substantial criticism of

[41] Cécile De Terwangne, 'Champ d'application territorial du règlement', in *Le Règlement Général Sur La Protection Des Données (RGPD/GDPR) : Analyse Approfondie* (Larcier 2018), para 30.

[42] Regulation (EU) 2016/679, Art. 3

[43] Directive (EU) 2016/680, Art. 2

[44] COM/2021/206 final, Art. 2 (4)

this exclusion will be made further in this essay;[45] for now, it serves to show the lesser importance of AI regulation compared to the protection of personal data considering the common observance that the extent of the territorial scope of legislation reflects its significance to European authorities: international organisations, human rights and national constitutions, which are often held to have the higher standing in the hierarchy of norms, have an extensive territorial reach.[46]

B. Presence of explicit references to the GDPR in the AI Act Proposal

One of the most notable links to be drawn between the GDPR and the Proposal stands in the latter's Explanatory Memorandum, in which the European Commission explicitly states its intention for the Proposal to be without prejudice to and complement the GDPR in AI uptake and development.[47] A study made by the Scientific Foresight Unit (STOA) of the European Parliamentary Research Service, although carried out prior to the publication of the Proposal in April 2021, effectively demonstrated that the GDPR was not incompatible with the data-intensive nature of artificial intelligence.[48] However, a significant amount of works has argued the contrary, including a recent report published in November 2021 by the Special Committee on Artificial Intelligence in a Digital Age of the European Parliament: its rapporteur, Axel Voss, considers autonomous AI systems to inherently conflict

[45] *infra pp. 44-45*

[46] European Council on Refugees and Exiles, 'The EU Charter of Fundamental Rights; an Indispensable Instrument in the Field of Asylum' (2017), 3. <https://www.ecre.org/wp-content/uploads/2017/02/The-EU-Charter-of-Fundamental-Rights.pdf>.

[47] Explanatory Memorandum to COM/2021/206 final, para 1.2

[48] Giovanni Sartor and Francesca Lagioia, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (Scientific Foresight Unit (STOA) EPRS | European Parliamentary Research Service 2020), 76. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

with the substantial provisions laid down in the GDPR, including information duties, purpose limitation, data minimisation and restrictions on secondary use.[49] The conclusion of the STOA that the compatibility between AI and GDPR provisions is highly dependent on specific interpretations such as a "flexible application of the idea of compatibility" and of the principle of data minimisation, coupled with the alleged natural conflict between major data protection requirements and AI systems, would indicate that new provisions supporting the development of efficient AI may easily be understood as derogations to former law supporting data protection in the sense of *lex posterior derogat legi priori*: the legal maxim that settles cases of contradiction between two norms of the same legal value by stating that the application of the later one should prevail and therefore repeal that of the earlier one.[50] The unwanted application of *lex posterior derogate legi priori* may be partially remedied through interpretation guidance. In that sense, the European Commission's specific indications according to which the Proposal "is without prejudice and complements the General Data Protection Regulation (Regulation (EU) 2016/679)"[51] should be understood as excluding the conditions for the application of the maxim aforementioned, namely express repeal (1) or manifest repugnance (2).[52] An express repeal of the GDPR does not come into question in the Proposal, as no mention explicitly states that any of the provisions of the GDPR should be repealed; manifest repugnance

[49] Axel Voss, 'DRAFT REPORT on Artificial Intelligence in a Digital Age' (Special Committee on Artificial Intelligence in a Digital Age 2021), 17.

[50] Gerhard Köbler, *Juristisches Wörterbuch. Für Studium und Ausbildung*. 17. Auflage. Vahlen, München 2018, ISBN 978-3-8006-5881-7, S. 277

[51] Explanatory Memorandum to COM/2021/206 final, para 1.2

[52] Henry Campbell Black and West Publishing Company, *Black's Law Dictionary : Containing Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern, and Including the Principal Terms of International, Constitutional, Ecclesiastical and Commercial Law, and Medical Jurisprudence, with a Collection of Legal Maxims, Numerous Select Titles from the Roman, Modern Civil, Scotch, French, Spanish, and Mexican Law, and Other Foreign Systems, and a Table of Abbreviations* (2nd edn., West Publishing Co 1933).

points to substantial incompatibilities between norms that would be evident to a reasonable person.[53] As mentioned prior, such could be the case for provisions supporting AI efficiency and provisions supporting extensive data protection. However, the use of the term "without prejudice to" would mean that provisions under the Proposal would not hinder those of the GDPR.[54] Similarly, the complementary nature of the Proposal explicitly envisioned should reasonably be understood as guiding the interpretation of the Proposal to be aligned with the provisions of the GDPR, thus excluding manifest repugnance.

Not all explicit references to the GDPR in the Proposal are conceptual. The second may be drawn through the active role given by the Proposal to the European Data Protection Supervisor (EDPS). In its Article 63, the Proposal designates the EDPS as "market surveillance authority".[55] This supervisory duty should be applied to institutions, agencies and bodies of the European Union that fall within the scope of the proposed Artificial Intelligence Act (AIA).[56] Pursuant to the title of market surveillance authority and specifically to effectively implement supervision, the EDPS would hold a power to impose fines,[57] may establish AI regulatory sandboxes[58] and would be a leading authority of the European Artificial Intelligence Board.[59] A power to impose fines demonstrates effective sanctions of provisions, necessary for the

[53] Jonathan Law and Elizabeth A. Martin (2014), 'Repugnancy', *A Dictionary of Law* (7th ed.), Oxford University Press.

[54] 'What Is PREJUDICE? Definition of PREJUDICE (Black's Law Dictionary)' (*The Law Dictionary*7 November 2011) <https://thelawdictionary.org/prejudice/> accessed 22 May 2022.

[55] COM/2021/206 final, Art. 63 (6)

[56] Explanatory Memorandum to COM/2021/206 final, para 5.2.6 & COM/2021/206 final, Art. 59 (8)

[57] COM/2021/206 final, Art. 72

[58] COM/2021/206 final, Art. 53 (1)

[59] COM/2021/206 final, Art. 56 & Art. 57 (1)

successful implementation of a law;[60] sandboxes test AI systems in prospect of their development and placing on the market, therefore providing effective supervision of the system;[61] a leading role in the European Artificial Intelligence Board, which would ensure the effective application of the envisioned provisions of the AI Act, would highlight a consequential influence of the EDPS in the advice and assistance to be provided to the European Commission.[62]

The European Data Protection Board (EDPB) and the EDPS showed appreciation for these provisions but called for further clarification to be made within the Proposal, deeming the explanations concerning the role of the EDPS to be insufficient.[63] In ruling the absence of details as insufficiency, however, the EDPB and the EDPS may be failing to take into account that the influence and objectives of the EDPS are already established by the GDPR and could be applied by analogy, reinforcingly so considering the complementary nature to the GDPR intended by the European Commission in drafting the Proposal. Under the GDPR, the role of the EDPS is considerably intelligible: defined as a supervisory authority "responsible for monitoring and ensuring the implementation of Regulation (EU) No 2018/1725",[64] its tasks and powers are listed in Articles 57 and 58 of the GDPR respectively. A number of these tasks would be applicable to the regulation of AI, particularly:

[60] Anthony D'Amato, 'The Moral and Legal Basis for Sanctions' (Northwestern University School of Law Scholarly Commons 2010), 5. <http://scholarlycommons.law.northwestern.edu/facultyworkingpapers/95>.

[61] *infra p. 56*

[62] COM/2021/206 final, Art. 56 (2)

[63] 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)', 13.

[64] EDPS, 'E | European Data Protection Supervisor' (*edps.europa.eu*) <https://edps.europa.eu/data-protection/data-protection/glossary/e_en#edps>.

Tasks relating to the information of the rights of actors and subjects. "The promotion of public awareness and understanding of the risks, rules, safeguards and rights in relation to processing",[65] "the advice […] on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing",[66] "the promotion of the awareness of controllers and processors of their obligations"[67] and "the provision of information to any data subject concerning the exercise of their rights under the GDPR"[68] are tasks given to the EDPS by the GDPR, applicable to AI regulation as envisioned by the Proposal due to the intrinsic role of the processing of personal data in developing AI systems. This applicability is strengthened when considering that, as a consequence of that intrinsic role, the actors and subjects of the GDPR and those of the Proposal may be identical.[69]

Tasks relating to the harmonisation of regulation surrounding fields involving data protection. The obligations of "cooperating with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of the GDPR",[70] of "encouraging the drawing up of codes of conduct",[71] of "encouraging of the establishment of data protection certification mechanisms"[72] and of "fulfilling of any other tasks related to the protection of personal data"[73] call for the involvement of the EDPS in regulating domains that may require a special application of the GDPR, AI being the prime

[65] Regulation (EU) 2016/679, Art. 57 (b)

[66] Regulation (EU) 2016/679, Art. 57 (c)

[67] Regulation (EU) 2016/679, Art. 57 (d)

[68] Regulation (EU) 2016/679, Art. 57 (e)

[69] *infra pp. 29-30*

[70] Regulation (EU) 2016/679, Art. 57 (g)

[71] Regulation (EU) 2016/679, Art. 57 (m)

[72] Regulation (EU) 2016/679, Art. 57 (n)

[73] Regulation (EU) 2016/679, Art. 57 (v)

example.[74] Particularly, under the Proposal, the EDPS should bring such assistance to the national supervisory authorities referred to in Article 57,[75] with a focus on data protection requirements set out in the GDPR.

Additionally, the tasks of the European Artificial Intelligence Board set out in Article 58 would not conflict with those of the EDPS provided under both the Proposal and the GDPR,[76] further increasing the possibility of interpreting the EDPS' role under the Proposal as complementary to those implemented by the GDPR.

C. Absence of reference to data subjects in the AI Act Proposal

The European Commission's AI Act Proposal limits the scope of its applicability to providers and users of AI systems. The former would refer to the developers of such systems and the latter to those using AI in a non-personal or professional activity.[77] "Users" of AI systems, as defined by the Proposal, do not include data subjects to the extent that they would be exposed to artificial intelligence in a personal, non-professional context. Rather, as was identified by the European Digital Rights association (EDRi), the definition would be confined to those deploying AI;[78] data subjects affected by such systems would in contrast be included in the "natural persons" with which an AI system is intended to interact and must therefore meet specific transparency requirements.[79] The EDRi was highly critical of the reference to the

[74] Gérard Haas and Stéphane Astier, *Intelligence Artificielle : Enjeux Éthiques et Juridiques* (Éditions Eni 2021).

[75] COM/2021/206 final, Art. 57 (1)

[76] COM/2021/206 final, Art. 58

[77] COM/2021/206 final, Art. 3 (2), (4)

[78] Sarah Chander and Ella Jakubowska, 'EU's AI Law Needs Major Changes to Prevent Discrimination and Mass Surveillance' (*European Digital Rights (EDRi)*28 April 2021) <https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/>.

[79] COM/2021/206 final, Art. 52

natural persons, which Sarah Chander and Ella Jakubowska generally designated as "harmed by AI systems", being confined to a single article within the Proposal, particularly drawing attention to the otherwise-absence of mechanisms providing such victims with the possibility to seek recourse and redress from a user.[80]

Concerning data subjects, however, the 'harm' envisioned that would stem from the placing on the market of an AI system could be deemed sufficiently covered by the GDPR. Providers of AI inherently carry out operations of processing of personal data as defined in the GDPR. Therefore, obligations befalling data processors would automatically apply to providers. In some cases, providers may furthermore determine the purposes and means of such processing, hence also acting as controllers.[81] A paper published by Harvard researchers considers the quality of 'controller' to extend to operators of AI,[82] defined as users by the Proposal, a vision that was confirmed by the EDPB and the EDPS in a joint opinion. Whereas the joint opinion in question deems the relationship between the actors of the Proposal (namely providers, users, importers and distributors) and those of the GDPR (namely data controllers and data processors) to be incongruent, it nevertheless implies that providers and users of AI systems would necessarily be

[80] Sarah Chander and Ella Jakubowska, 'EU's AI Law Needs Major Changes to Prevent Discrimination and Mass Surveillance' (*European Digital Rights (EDRi)*28 April 2021) <https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/>.

[81] Olivia Lee, 'Artificial Intelligence and Data Protection – How the GDPR Regulates AI' (Centre for Information Policy Leadership 2020), 5. <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf>.

[82] Jessica Fjeld and others, 'Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI' (Berkman Klein Center Research Publication 2020), 25.

either processors or controllers of personal data.[83] As such, any claim held by a data subject relating to the violation of the obligations befalling controllers or processors of personal data would necessarily be enforceable against the actors of the Proposal and the absence of the mechanisms of recourse and redress referred to by the EDRi would be effectively balanced by the transposition of those set out in the GDPR, generally deemed appropriate.[84]

II. The lack of clarity surrounding the extent of the AI Act Proposal's complementary nature

The European Commission's intent for the envisioned Artificial Intelligence Act to complement the GDPR is, in itself, established by the Proposal. However, the extent to which the AIA and the GDPR would operate in proximity to each other remains unclear: the mechanisms implemented by both regulations to safeguard the provisions of the Proposal and those of the GDPR respectively lack in harmonisation (A), although this lack of clarity may be intentional (B).

A. A lack of harmonisation between the mechanisms to safeguard the AI Act Proposal and those to safeguard GDPR requirements

The Joint Opinion aforementioned illustrates a significant concern from the EDPB and the EDPS as to the lack of harmonisation in the mechanisms for the enforcement of the GDPR and the Proposal respectively.[85] The criticism made to the lack of detail surrounding the

[83] 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)', para 20, 9.

[84] *supra p. 19*

[85] 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)', para 3.5, 20.

role of the EDPS as market surveillance authority set aside,[86] the joint opinion further opposed what it seemed to believe would be the generalised designation of competent authorities, calling for data protection authorities (DPAs) to be designated as national supervisory authorities under the Proposal in the view that DPAs are already enforcing the GDPR and other relevant data protection legislation such as LED on currently implemented AI systems.[87] Further fitting in the criticism made that the Proposal is not clear on how it might apply to AI systems currently on the market,[88] such as deep fakes,[89] the European Commission's choice to designate competent authorities generally instead of establishing specific authorities other than the European Artificial Intelligence Board does not inherently exclude the application of GDPR provisions on one hand; on the other hand, it leaves a possibility for such authorities to differ from those put forth by the GDPR. As such, the extent of the role carried out by the competent authorities enforcing GDPR provisions in the field of AI as envisioned by the Proposal is not clear. Another example would be that of the notifying authorities and notified bodies designated by the Proposal, responsible for issuing certification attesting to an AI system's compliance with the envisioned AIA.[90] Notified bodies would have to satisfy the requirements of verifying the conformity of high-risk AI systems through a specific procedure concerning predominantly the quality management system,[91] of an organisational structure based essentially on ensuring the efficient carrying out of their tasks, and of

[86] *supra p. 11*

[87] 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)', para 48, 15.

[88] 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)', para 2.4.2.

[89] Explanatory Memorandum to COM/2021/206 final, para 1.1, 5.2.4

[90] COM/2021/206 final, Art. 30-33

[91] Annexes VI and VII to COM/2021/206 final

independence from the provider of the system analysed.[92] The European Association for Medical Devices of Notified Bodies (Team-NB) was highly critical of this potential approach, issuing in a position paper that "a possibility to split the Medical AI System by having the AI part evaluated by an AI-notified-body and the medical device part by an MDR/IVDR notified body should be avoided […] to ensure that the special characteristic of medical devices and the general safety and performance requirements of a medical device are considered during the AI assessment, for which the non-MDR-accredited notified body does not have the respective expertise". Instead, it suggested to expand the "designation scope covering AI related aspects under relevant NLF regulations", hence requiring for the notified bodies already competent in the field of medical devices to further show competency for assessing AI system-requirements in the field of medical devices.[93] The question of whether the notified bodies set out in the AIA differ from those set out in other relevant European legislation with which the Proposal may overlap, such as medical devices and data protection, is unanswered by the Proposal,[94] although it is worth noting that concerning the field of data protection, requirements of a quality management system mention "systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems".[95] This mention, however, appears insufficient to resolve the question

[92] COM/2021/206 final, Art. 33

[93] The European Association Medical Devices - Notified Bodies, 'Position Paper on European Artificial Intelligence Regulation' (2021), 3. <https://www.team-nb.org/wp-content/uploads/2021/10/Team-NB-PositionPaper-Artificial-Intelligence.pdf>.

[94] Nick Paul Taylor, 'Notified Bodies Join Chorus of Criticism of Proposed European AI Regs' (*MedTech Dive* 6 October 2021) <https://www.medtechdive.com/news/notified-bodies-EU-proposed-artificial-intelligence-ai-regulation/608880/>.

[95] COM/2021/206 final, Art. 17 (1) (f)

prior, as although the notified bodies under the AIA would have to look at the field of data protection, the Proposal chose not to designate the notified bodies put forth by the GDPR as competent to exercise such control. This blurs the role of data protection authorities implemented by the GDPR in AI. Hence, both interpretations of the provisions of the AIA envisioned by Team-NB may be correct and expand to the field of data protection: the extent of the role of the certification bodies under the GDPR in the field of AI, as envisioned by the Proposal, remains unclear.

This lack of clarity concerns not only the competent authorities meant to issue compliance certification with the GDPR and the AIA respectively, but also the relationship between data protection compliance certification and AI compliance certification itself. The EDPB and the EDPS show concern regarding what they call "misalignments" between the certification process under the GDPR and that under the AIA.[96] Particularly, the implications of a certification of conformity issued under the AIA for data protection requirements remains unclear: the example used by the EDPB and the EDPS is that of "AI systems, certified under the Proposal and marked with a CE marking of conformity, once placed on the market or put into service, [which] might be used in a way which is not compliant with the rules and principles of data protection".[97] Concerning certifications, the Proposal's choice to remain vague as to the extent of the proximity between GDPR compliance and AIA compliance makes it difficult to determine its position compared to AI certification processes envisioned by prior doctrine, such as that of the Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS) held to "advance transparency, accountability and reduction in algorithmic bias

[96] 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)', para 74-75, 20.

[97] *Ibid.*

in Autonomous and Intelligent Systems"[98] or of the EU's Guidelines for Trustworthy AI, which listed the requirements of human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination, and fairness, societal and environmental well-being and accountability.[99] Certificates issued under the AIA appear to be as likely to attest *per se* to compliance with data protection requirements of an AI system as to require further GDPR certification.

B. The choice of leaving the determination of such extent to future amendments

Speaking in the context of AI, Professor Joanna Bryson deemed law to be "primarily designed to maintain social order by dissuading people from doing wrong […] by making it clear what actions are considered wrong and then determining the costs and penalties for committing these wrong acts."[100] Applied to data protection and artificial intelligence, the legal certainty required by Professor Bryson's definition of law would appear to conflict with the vagueness of the provisions envisioned by the Proposal. This lack of clarity, however, may be intentional. In 2020, Professor Florian Evéquoz and researcher Johan Rochel shed light on the practical implementation of GDPR requirements in the standard process of data mining for the development of AI systems. Although the paper raised issues largely focused on the ethics of artificial intelligence rather than on the legal requirements themselves, it stemmed its reasoning from the lack of clarity concerning the extent of the principles of specified, explicit and

---

[98] Institute of Electrical and Electronics Engineers Standards Association, 'The Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)' (*IEEE Standards Association*) <https://standards.ieee.org/industry-connections/ecpais/>.

[99] High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI, 2019

[100] Joanna Bryson, 'The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation', in Markus D. Dubber, Frank Pasquale and Sunit Das (eds.), *The Oxford Handbook of Ethics of AI* (2020)

legitimate purposes for data processing, of responsibility and of accountability with regards to AI engineers.[101] In parallel to the significant practical difficulties of implementing data protection mechanisms in AI systems, ARTICLE 19 and Privacy International highlighted a consensus in transnational regulatory frameworks, to the extent that the right to privacy is conferred, that data protection in the development of AI should intrinsically be maximised.[102] The GDPR, however protective, does not suffice to remedy these practical difficulties and, according to professor Robert van den Hoven van Genderen, cited earlier in this paper, should not be enforced on all AI applications because of the significant hinderance on the development of AI such an application would ensue.[103] All these works support a single consensus: the GDPR should apply to AI systems, but only to an undetermined extent. When shedding light on this context, the lack of clarity surrounding the provisions of the Proposal as to their complementary nature to the GDPR may be analysed as potential call for discussion as to how closely the GDPR and the Proposal should operate, particularly as the ordinary legislative procedure it is currently undergoing comprehends many stages of discussion[104] and its published status allows for significant feedback to be made by the experts in the field of data protection and AI respectively.

Generally, two interactions between the GDPR and AI could be envisioned. The first would be a separative approach, encompassing Professor van den Hoven van Genderen's view that the GDPR's application to AI systems should remain scarce. Virginia Dignum, although remaining fairly neutral, touched on the possibility that the

[101] Johan Rochel and Florian Evéquoz, 'Getting into the Engine Room: A Blueprint to Investigate the Shadowy Steps of AI Ethics' (2020) 36 AI & SOCIETY.

[102] Article 19, *Privacy and Freedom of Expression in the Age of Artificial Intelligence* (Article 19 2018), 22.

[103] Robert Van den Hoven van Genderen, 'Do We Need New Legal Personhood in the Age of Robots and AI?' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), *Robotics, AI and the Future of Law* (Springer, Singapore 2018), 51.

[104] Procedure 2021/0106/COD

specifics of AI, combined with its potential, could justify it following a different approach to data protection than the one currently implemented by the GDPR: she highlighted the potential claims in "economic losses and delay on development" stemming from an incompatibility between a highly-restrictive legislation conferring a full right of explanation of an automated decision upon data subjects with the current approaches based on neural networks and deep learning.[105] Such stringency, particularly in the conferring of a full right of explanation for decisions based on automated-decision-making systems to data subjects, was raised as a characteristic of the GDPR,[106] hence a position, often defended by AI developers, that data protection issues in AI should be regulated by means other than the provisions of the GDPR.[107] This would, on one hand, undoubtedly facilitate innovation; on the other hand, it could lead to results that Professor Vincent C. Müller called "arguably a scandal" in terms of profiling.[108]

The second view would be for the GDPR and the AIA to operate closely together. However, in a technology analysis provided for the scientific fiction short story 'Isle of Happiness', computer scientist Kai-Fu Lee deemed the GDPR requirements of transparency, explicit consent, specific purpose, protection from unauthorised use, explainability of automated decisions, human oversight and data minimisation, in their current implementation, to be an impediment to AI significant enough

---

[105] Virginia Dignum, 'Responsibility and Artificial Intelligence', in Markus D. Dubber, Frank Pasquale and Sunit Das (eds.), *The Oxford Handbook of Ethics of AI* (2020)

[105] Jonas Schuett, 'A Legal Definition of AI' (2019), 3

[106] Mark Coeckelbergh, '10 POLICY PROPOSALS,' in *AI Ethics* (The MIT Press 2020), 154.

[107] Robert Van den Hoven van Genderen, 'Do We Need New Legal Personhood in the Age of Robots and AI?' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), *Robotics, AI and the Future of Law* (Springer, Singapore 2018), 51.

[108] Vincent C Müller, 'Ethics of Artificial Intelligence and Robotics' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Metaphysics Research Lab 2020), 5. <https://plato.stanford.edu/archives/sum2021/entries/ethics-ai/>.

to call the application of the current version of the GDPR on AI systems "counterproductive in many ways" and "dysfunctional".[109] A specific point raised by Kai-Fu Lee was that purpose limitation would be difficult, if not impossible, to implement, as the multiple purposes for which data would be collected in the development on an AI system could not all be foreseen. Virginia Dignum, however, saw the challenges posed by a closely-operating together approach of the GDPR and artificial intelligence, here the envisioned AIA, less as an impossibility and more as a challenge that may push scientific progress in the field of AI, stating that "researchers need to go back to the drawing board to come up with novel learning and reasoning techniques that ensure explainability and sustainable use of data without compromising efficiency".[110]

[109] Kai-Fu Lee and Chen Qiufan, 'Isle of Happiness', in *AI 2041* (Currency 2021), 396.

[110] Virginia Dignum, 'Responsibility and Artificial Intelligence', in Markus D. Dubber, Frank Pasquale and Sunit Das (eds.), *The Oxford Handbook of Ethics of AI* (2020), 10.

PART TWO: A partial answer to the substantial tensions between promoting AI uptake and innovation and safeguarding the protection of data subjects under the GDPR

In drafting the Proposal, the European Commission has opted for the envisioned AIA to operate on the basis of risks, an approach which may conflict with that of the GDPR (I). However, the Proposal addresses some of the most significant general data protection principles deemed to cause friction in the field of AI with a degree of adequacy (II).

I. The choice of a risk-based approach

"The Working Party is concerned that both in relation to discussions on the new EU legal framework for data protection and more widely, the risk-based approach is being increasingly and wrongly presented as an alternative to well-established data protection rights and principles, rather than as a scalable and proportionate approach to compliance."[111]

Although a general consensus concerning the definition of a risk-based approach in EU legislation was established (A), the essence of the envisioned AIA may induce a divergence between the risk-based approach of the GDPR and that of the Proposal (B).

A. Definition of a risk-based approach

The Article 29 Data Protection Working Party (Art. 29 WP) defined the general mechanism of the risk-based approach, in the context of the GDPR, as "strengthened obligations [resulting] from processing which is considered risky for the persons concerned".[112] Although Art. 29 WP

[111] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' [WP 218] (2014), 2.
[112] *Ibid.*

was set up by the Data Protection Directive[113] and ceased to exist with the entry into force of the GDPR,[114] the opinions and recommendations it has issued in the fields of privacy and data protection are consequential, reaching the number of 240 between 1997 and 2016.[115] The GDPR does indeed follow a risk-based approach: for example, the measures implemented to safeguard the security of processing, imposed on controllers and processor, should "ensure a level of security appropriate to the risk".[116] This proportionality is further required of the controller with regards to provisions of the GDPR generally[117] and the concept of risks is clarified under Recital 75, which enumerates a number of indicators of risk such as discrimination, the vulnerability of the person of the data subject and the amount of personal data processed.[118]

The proportionality induced by the risk-based approach has led Art. 29 WP to clarify that it was, by no means, a mitigation of rights: citing Art. 29 WP, "rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved".[119] The working party further insisted that such rights had to be as strong low-risk processing as in high-risk processing; the mitigation would only affect compliance mechanisms, which would be less stringent on controllers whose processing is low-risk.[120] This clarification was welcomed by the

[113] Directive 95/46/EC, Art. 29

[114] Regulation (EU) 2016/679, Art. 94

[115] European Commission, '[Archived Content] Opinions and Recommendations - European Commission' (*ec.europa.eu*) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm>.

[116] Regulation (EU) 2016/679, Art. 32 (1)

[117] Regulation (EU) 2016/679, Art. 24 (1)

[118] Regulation (EU) 2016/679, Recital 75

[119] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' [WP 218] (2014), 3.

[120] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' [WP 218] (2014), 2.

organisation Access Now, which considered the GDPR to be "based on rights and making them operational" despite the risk-based approach.[121]

The risk-based approach under the Proposal calls for a clear classification of AI systems based on risks to fundamental rights: the Explanatory Memorandum of the Proposal indicates that the envisioned AIA "seeks to ensure a high level of protection for those fundamental rights and aims to address various sources of risks through a clearly defined risk-based approach", explicitly referring to the right to respect to private life and personal data.[122] The implementation of the risk-based approach is then centred around high-risk AI systems, which are indeed strongly regulated: the Proposal provides for a clear definition as to when a system is considered high-risk, further clarifying that the placing on the market of an AI system must be understood broadly;[123] the development of high-risk AI systems which involve training data sets must use data sets meeting specific quality criteria outlined in the Proposal;[124] the transparency obligation befalling high-risk AI systems is explained as requiring to "enable users to interpret the system's output and use it appropriately" and to comply with a more extensive transparency set out in Article 52;[125] furthermore, the obligations of the providers and users of high-risk AI systems are well-detailed.[126] By contrast, the provisions relating to low-risk AI systems are minimal. This absence of provisions surrounding AI systems which do not present a high risk under the Proposal cast doubt, raised by the EDPB and the EDPS, as to whether the risk-based approach under the Proposal was identical to that under the GDPR: both authorities therefore called for a clarification of the risk-based approach under the envisioned AIA

[121] Fanny Hidvegi, Daniel Leufer and Estelle Massé, 'The EU Should Regulate AI on the Basis of Rights, Not Risks' (*Access Now* 17 February 2021) <https://www.accessnow.org/eu-regulation-ai-risk-based-approach/>.

[122] Explanatory Memorandum to COM/2021/206 final, para 3.5

[123] COM/2021/206 final, Art. 7 & Art. 8

[124] COM/2021/206 final, Art. 10

[125] COM/2021/206 final, Art. 13

[126] COM/2021/206 final, Chapter III

and for the alignment of the concept of 'risk to fundamental rights' with that of the GDPR.[127]

B. The essence of the envisioned Artificial Intelligence Act: a nuance to the safeguards of a risk-based approach

In an article entitled "The EU should regulate AI on the basis of rights, not risks", briefly mentioned above, Fanny Hidvegi, Daniel Leufer and Estelle Massé talked extensively about the problems of the risk-based approach envisioned by the European Commission and highlighted a difference with the risk-based approach under the GDPR.[128] Although the article originally refers to the European Commission's White Paper on AI of February 2020 and was written before the Proposal was issued, such criticism could reasonably be extended to the envisioned AIA in view that the Proposal effectively retains a risk-based approach as set out in the White Paper.[129] Substantially, it paints the risk-based approach as opposing operational risks for those developing and deploying AI and fundamental rights, notably stating:

"*Rather than focusing on fundamental rights, the Commission's stated approach to regulating AI has been to place innovation and increased AI uptake as its primary concern. Protecting rights is acknowledged as a secondary concern, with the worrying proviso that it must only be done in a manner that does not risk stifling innovation.*"[130]

This criticism fails to take into account the full scope of the Art. 29 WP's statement, which extends its definition of a risk-based approach

[127] 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)', para 18, 8.

[128] Hidvegi, Leufer, Massé, 'The EU Should Regulate AI on the Basis of Rights, Not Risks' (2021)

[129] Explanatory Memorandum to COM/2021/206 final, para 1.

[130] Hidvegi, Leufer, Massé, 'The EU Should Regulate AI on the Basis of Rights, Not Risks' (2021)

as a "scalable and proportionate approach to compliance" rather than a mitigation of rights beyond the EU's data protection framework.[131] Hence, it could be argued that Art. 29 WP's vision of the risk-based approach should be retained for the Proposal.

Casting aside the Proposal's minimal regulation of low-risk AI systems,[132] the envisioned AIA however holds essential differences with the EU's data protection framework, namely the unpredictable nature of AI and the principal goal of AI uptake and innovation. These differences may bring a fundamental nuance to risks and subsequently to the compatibility between a risk-based approach and established data protection rights and principles.

1. The unpredictable nature of artificial intelligence

"The EU should regulate AI on the basis of rights, not risks" notably states that the risk presented by an AI system is inherently deepened by the unpredictability of artificial intelligence in terms of both operation and consequences.[133] A well-known example is that of unforeseen bias in training data sets, particularly with regards to predictive justice: a report published by the Criminal Justice Policy Program of the Harvard Law School in 2020 found that there were racial disparities in the length of incarceration sentences given, with African American and Latin American offenders facing longer sentences that their Caucasian counterparts.[134] Were an AI system to be developed for the purpose of predictive justice, it could be trained on data incorporating this factual

---

[131] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' [WP 218] (2014), 2.

[132] *supra pp. 40-41*

[133] Hidvegi, Leufer, Massé, 'The EU Should Regulate AI on the Basis of Rights, Not Risks' (2021)

[134] Elizabeth Tsai Bishop and others, 'Racial Disparities in the Massachusetts Criminal System' (Criminal Justice Policy Program 2020), 34. <https://hls.harvard.edu/content/uploads/2020/11/Massachusetts-Racial-Disparity-Report-FINAL.pdf>.

longer sentencing of African American and Latin American offenders stemming from multiple decisions, hence developing bias towards a specific ethnicity. The EDPB and the EDPS confirmed the view that unpredictability of AI systems could constitute a significant nuance to risk, particularly with regards to the risk assessment made by the provider under the Proposal: because it could not be reasonably expected of the provider to assess all uses of an AI system developed, a further data protection impact assessment (DPIA) should be carried out by the user of the system to determine whether the AI in question is to be considered high-risk under the EU's data protection framework.[135] The independence of a high-risk classification of an AI system under the Proposal from that under the GDPR is likely to only bring a partially more complete assessment of the uses of an AI system: in a webinar conducted by the multinational law firm Fieldfisher, privacy law specialists Phil Lee and Leonie Powers highlighted that DPIAs also require to "explain any relevant variation or margins on error and address concept drifts", the latter referring to a potential change in the behaviour of what Lee and Powers call the "target population" which would lead to a re-examination of the relevant DPIA.[136] As such, although the user of an AI system would, as a deployer, provide a notably more accurate prediction of its operational use, the significant probability of unexpected consequences stemming from the unpredictable nature of AI remains a substantial issue and could pose further issues for the legal basis of legitimate interest in the processing of personal data: it would appear significantly complex to determine whether an interest is legitimate if the proportionality to the risk to the protection of personal data cannot be clearly assessed, as it may be the case for AI.[137]

---

[135] 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)', para 21, 9.

[136] Phil Lee and Leonie Powers, 'Data Protection Issues in AI' (*www.youtube.com* 23 April 2021) <https://www.youtube.com/watch?v=aV4BpDpEWg0>.

[137] *Ibid.*

2. The principal goal of AI uptake and innovation

In response to the publication of the Proposal, the Council of the European Union proposed to include a paragraph in the envisioned AIA, which would state that the Regulation "should not affect research and development activities concerning AI systems to the extent that such activities do not lead to or involve the placing on the market or putting into service of an AI system".[138] Generally introducing a field where the AIA would not be applied, the proposition of the Council of the European Union reflects the general mindset that the goal of AI uptake and innovation holds a primary place in the framework of the Proposal. Some of the provisions envisioned by the Proposal in support of AI uptake and innovation, already established in the version of April 2021, indeed allow significant circumventions of rights, therefore appearing to depart from the Art. 29 WP's vision of the risk-based approach.

Exemption envisioned for public authorities in a third country and international organisations. The Proposal explicitly excludes from the scope of its application "public authorities in a third country [and] international organisations […] where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States".[139] This would mean that third countries and international organisations using AI systems which would normally be considered high-risk in the EU and would therefore require the application of the provisions relevant to such systems, would not be required to meet the provisions of the AIA to the extent that the systems are used in the context of law enforcement, although they may affect

[138] Céline Castets-Renard, 'Quel Droit de l'Intelligence Artificielle Dans l'Union Européenne ? Ou Les Multiples Ambitions Normatives de l'AI Act' (2022) 2 Dalloz IP/IT, 67.

[139] COM/2021/206 final, Art. 2 (4)

natural persons, including data subjects, within the EU. The EDPB and the EPDS were highly critical of this exemption, particularly with regards to the example of "third countries or international organisations operating high-risk applications relied on by public authorities in the EU".[140] Such criticism is particularly relevant considering that the GDPR does not, in itself, apply to the processing of personal data for the purpose of law enforcement,[141] and could only be remedied if LED was deemed to provide a sufficient protection of the rights of data subjects with regards to AI used in law enforcement.

'Real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement. The Proposal generally lists the use of "real-time" remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement as a prohibited AI practice.[142] However, its allows for three notable exceptions to this prohibition: "the targeted search for specific potential victims of crime", "the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack", or "the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence" in the context of a European arrest warrant "and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State".[143] Although the EDRi welcomed the ban, it deemed the exceptions aforementioned to be "wide" and "ripe for abuse", further considering the prohibition to be insufficient in regulating biometric systems generally, such as systems processing

[140] 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)', para 14, 8.

[141] Regulation (EU) 2016/679, Art. 2 (2) (d)

[142] COM/2021/206 final, Art. 4 (1) (d)

[143] COM/2021/206 final, Art. 4 (1) (d) (i) (ii) (iii)

biometric data other than "real-time" biometric data.[144] Both the EDRi paper and the EDPB-EDPS Joint Opinion systematically contrast the appreciation for the ban with the insufficiency concerning operations of "categorisation" from biometric data. According to the EDPB and the EDPS, such categorisation should be prohibited when the AI systems places data subjects into clusters according to "ethnicity, gender, as well as political or sexual orientation".[145] The violation of the right to non-discrimination claimed, by the EDRi, to be engendered, had led Sarah Chander and Ella Jakubowska to call for a broad ban on biometric mass surveillance AI systems, specifically "a full prohibition on all forms of biometric mass surveillance practices in publicly accessible spaces by all public authorities and private actors".[146] A parallel insufficiency was noted by the EDPB and the EDPS concerning the prohibition of social scoring under the Proposal, further prompting both authorities to call for a full prohibition of all forms of social scoring.[147]

The primary goal of AI uptake and innovation, as implemented by the provisions previously mentioned, appears to bring a fundamental difference to the risk-based approach envisioned by the Proposal compared to that established by the GDPR, as the goal itself seems dependant on a mitigation of rights in certain fields.

---

[144] Sarah Chander and Ella Jakubowska, 'EU's AI Law Needs Major Changes to Prevent Discrimination and Mass Surveillance' (*European Digital Rights (EDRi)* 28 April 2021) <https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/>.

[145] 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)', para 33, 12.

[146] Chander, Jakubowska, 'EU's AI Law Needs Major Changes to Prevent Discrimination and Mass Surveillance' (2021).

[147] 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)', para 29, 10.

II. Arrangement of GDPR principles to fit the framework of artificial intelligence

The Proposal specifically addresses three significant principles of general data protection, namely data protection by design and by default (A), accountability (B) and the right not to be subject to decisions based solely on automated processing (C) with a certain degree of adequacy to fit the framework of artificial intelligence.

A. The place of data protection by design and by default

The concepts of data protection by design and by default in AI may be seen as two of the many concepts deriving from those of *Value-Sensitive Design* and *Responsible Innovation*. Professor Jeroen van der Hoven defined *Value-Sensitive Design* as "a way of engaging ICT that aims at making moral values part of technological design, research and development", ICT referring to information and communications technology which, according to Professor Van der Hoven, remains the primary area of application of the concept.[148] In the field of AI, *Value-Sensitive Design* may be echoed by the Proposal's Explanatory Memorandum, which calls attention to the necessity for the EU to develop AI that is consistent with Union values.[149] On a practical basis, *Value-Sensitive Design* is to be implemented by the effective computational expression of an operator's intention on one hand, and by "transparency for the accountability of those intentions" on the other.[150] This is done through the expression of obligations and

[148] Jeroen van der Hoven, 'Value sensitive design and responsible innovation', in Richard Owen, JR Bessant, & Maggy Heintz (eds.), *Responsible innovation* (2013), 75–84.

[149] Explanatory Memorandum to COM/2021/206 final, para 1

[150] Joanna Bryson, 'The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation', in Markus D. Dubber, Frank Pasquale and Sunit Das (eds.), *The Oxford Handbook of Ethics of AI* (2020)

prohibitions.[151] *Responsible Innovation* is a broader concept: according to the European Commission, it calls for a general alignment of innovation with the values of society,[152] hence not referring specifically to the implementation of values in the design of a system. According to a research paper published in 2013, Responsible Innovation implies a line of questioning in relation to the "uncertainty (in its multiple forms), purposes, motivations, social and political constitutions, trajectories and directions of innovation", generally leading to "embedding deliberation on these within the innovation process".[153] The concept is explicitly referred to in the Proposal, which calls attention to its implementation of *Responsible Innovation* for high-risk AI systems, through restrictions imposed on freedoms relating to research development in order to safeguard public interest.[154] The reasons of public interest broadly listed by the Proposal are notably "health, safety, consumer protection and the protection of other fundamental rights".[155] As such, the concept would be understood as relating to legal requirements.

In line with the theoretical guidance of Value-Sensitive Design and Responsible Innovation, the GDPR lays down the requirements of data protection by design and by default.[156] The first imposes on the controller to integrate measures of data protection into the processing, specifically indicating "both at the time of the determination of the

---

[151] B. F. Malle, M. Scheutz, and J. L. Austerweil. 'Networks of Social and Moral Norms in Human and Robot Agents,' in Maria Isabel Joao Silva Sequeira and others (eds.), *A World with Robots: International Conference on Robot Ethics: ICRE 2015*, (Cham, Switzerland: Springer International Publishing, 2017), 3-17.

[152] European Commission, Rome declaration on responsible research and innovation in Europe 2014

[153] Jack Stilgoe, Richard Owen and Phil Macnaghten, 'Developing a Framework for Responsible Innovation' (2013) 42 Research Policy 1568 <https://www.sciencedirect.com/science/article/pii/S0048733313000930>.

[154] Explanatory Memorandum to COM/2021/206 final, para 3

[155] *Ibid.*

[156] Regulation (EU) 2016/679, Art. 25

means for processing and at the time of the processing itself".[157] The second, arguably more complex to implement in the field of AI, requires the controller to "ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed" through implementation measures.[158] Data may therefore not be retained for future uses that have yet to be determined, possibly rendering the implementation of data protection by default difficult for an AI developer:[159] as mentioned prior, the latter could not reasonably assess all potential uses of a system but would still have to feed the AI system a significant amount of data for its development.[160]

According to the GDPR, the implementation measures of data protection by design and by default may include data minimisation, pseudonymisation, transparency with regard to the functions and processing of personal data, enabling monitoring of the processing from the data subject, and enabling the controller to create and improve security features.[161] Although the EDPB and the EDPS criticised the Proposal's lack of reference to data protection by design and by default,[162] determining the extent to which the implementation measures aforementioned are advanced in the Proposal may bring out an implicit safeguard to the requirements in the envisioned AIA.

Data minimisation. The EDPS defines data minimisation as a requirement befalling a data controller to "limit the collection of personal information to what is directly relevant and necessary to

[157] Regulation (EU) 2016/679, Art. 25 (1)

[158] Regulation (EU) 2016/679, Art. 25 (2)

[159] Giovanni Sartor and Francesca Lagioia, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (Scientific Foresight Unit (STOA) EPRS | European Parliamentary Research Service 2020), 67.

[160] *supra p. 37*

[161] Regulation (EU) 2016/679, Recital 78

[162] 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)', para 8, 6.

accomplish a specified purpose" and "retain the data only for as long as is necessary to fulfil that purpose",[163] echoing the provisions of the GDPR.[164] In the Proposal, references to the concept of data minimisation may be found under two articles: the first is article 29, which provides that a user that has control over input data must "ensure that input data is relevant in view of the intended purpose of the high-risk AI system".[165] This meets the criteria of data minimisation requiring that data processing be relevant to achieve a specified purpose. The second is article 54, which provides that data lawfully processed for another purpose may be reused in the context of an AI regulatory sandbox if such processing would be necessary to fulfil requirements for high-risk AI systems set out in the Proposal, where "anonymised, synthetic or other non-personal data" would be insufficient.[166] The processing of personal data would again be limited to what is necessary to achieve a specific purpose. The further requirement of retaining data processed only for as long as is necessary to achieve a specified purpose, however, may be void of all effect in the field of AI. Particularly, in a paper published by the Boston University School of Law, researchers highlighted that data removal could have consequences in machine-learning algorithms that allow a system to learn from analysing a mass amount of data in order to draw a standard from these observations and apply it to another set of data. Thus, it may be argued that an AI system would retain the data initially processed for as long as it effectively operates.[167] A similar view may be drawn from the requirement of enabling monitoring from data subjects, which

[163] Francesco Albinati, 'D | European Data Protection Supervisor' (*edps.europa.eu*) <https://edps.europa.eu/data-protection/data-protection/glossary/d_en>.

[164] Regulation (EU) 2016/679, Art. 5 (1) (c)

[165] COM/2021/206 final, Art. 29 (3)

[166] COM/2021/206 final, Art. 54 (1) (b)

[167] Eduard Fosch Villaronga, Peter Kieseberg and Tiffany Li, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2018) 34 Computer Law & Security Review 304 <http://tiffanyli.com/wp-content/uploads/2018/08/Humans-Forget-Machines-Remember_Final-PDF.pdf>.

would raise issues in the event of a withdrawal of consent to the processing of personal data.

Pseudonymisation. The GDPR defines pseudonymisation as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual".[168] While in the general data protection framework of the EU, pseudonymisation tends to be promoted as an effective means to protect personal data and is often pushed for,[169] the Proposal seems to call for its application rather when processing special categories of personal data than when processing personal data in general in the context of high-risk AI systems. Particularly, the envisioned AIA provides that safeguards to fundamental rights such as pseudonymisation should be ensured in the processing of special categories of personal data, such as sensitive data, allowed in the context of bias monitoring, detection and correction in relation to the high-risk AI systems.[170]

Transparency. The GDPR requires that personal data be "processed […] in a transparent manner in relation to the data subject".[171] This is known as transparency, defined by the EDPS as "the right [of data subjects] to know which of [their] personal data are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed."[172] In the context of AI, the transparency

[168] Regulation (EU) 2016/679, Art. 4 (3) (b)

[169] Informationssicherheit Datenschutz Compliance, 'AI & GDPR: Minimise Compliance Costs with Anonymisation and Pseudonymisation!' (*ISiCO Datenschutz* 17 July 2019) <https://www.isico-datenschutz.de/en/ai-gdpr-anonymisation-and-pseudonymisation/>.

[170] COM/2021/206 final, Art. 10 (5)

[171] Regulation (EU) 2016/679, Art. 5 (1) (a)

[172] EDPS, 'Transparency | European Data Protection Supervisor' (edps.europa.eu) <https://edps.europa.eu/data-protection/our-work/subjects/transparency_en>.

requirement was generally deemed to involve traceability, verifiability, honest design and intelligibility.[173] It could be argued that transparency is the GDPR requirement that holds the most significant establishment in the envisioned AIA in comparison to other provisions of the GDPR. Particularly, article 52, mentioned prior, explicitly requires all AI systems, regardless of their risk classification, to operate transparently in relation to natural persons interacted with, especially in ensuring the information of the natural persons in question that they are interacting with an AI system or with content generated by automated means.[174] The Proposal brings further efficacy to this requirement by stating that it should be met in view to allow such natural persons "to make informed choices or step back from a given situation".[175] This general requirement balances out the mitigation of compliance mechanisms in proportion to the risk classification of the AI system outlined in the Proposal, bringing forward elements of the risk-based approach as envisioned by the Art. 29 Data Protection Working Party.[176] It is worth noting that, although Article 13 mentions that the developer of an AI system should ensure that the system in question meets sufficient transparency requirements "to enable users to interpret the system's output and use it appropriately",[177] this article is not an adequate safeguard to transparency in the sense of the GDPR, as it relates only to transparency for deployers of AI systems and not for those further interacting with those systems. In addition, the same article provides for an appropriate type and degree of transparency to be ensured "with a view to achieving compliance with the relevant obligations of the user and of the provider" set out in the Proposal.[178] These obligations have

[173] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 'Embedding Values into Autonomous and Intelligent Systems', Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems (2019), 181-182.

[174] COM/2021/206 final, Art. 52

[175] Explanatory Memorandum to COM/2021/206 final, para 5.2.4

[176] *supra pp. 38-40*

[177] COM/2021/206 final, Art. 13 (1)

[178] *Ibid.*

previously been analysed as providing an ambiguous protection of data subjects,[179] hence why the article on its own may not be deemed as a strong protection to the transparency requirement under the GDPR. Lastly, the European Commission calls for further transparency in placing an obligation on the providers of AI systems to register such systems in an EU database destined "to increase public transparency and oversight and strengthen ex post supervision by competent authorities."[180] Transparency will hold a predominant role in allowing the envisioned AIA to operate within the data protection framework of the GDPR, as a greater transparency is more likely to provide for the specific and informed consent of data subjects to the processing of their personal data: consent is, indeed, one of the three bases that legitimises such processing.[181] The practical difficulty of providing intelligibility of an AI system to natural persons, however, may vitiate this consent in the same way that the unintelligibility of general terms and conditions are raised as a current legal issue.[182] Furthermore, it is likely that trade-offs will be made in order to minimise the risk of cyber-attacks, which increases with an AI system's transparency.[183]

Enabling the controller to create and improve security features. Concerning the additional creation and improvement of security features after an AI system is developed and deployed, the Proposal focuses on broad monitoring and withdrawal possibilities,[184] and requires for the provider to be able to take corrective actions "to bring the system into conformity" if a high-risk AI system that has been

---

[179] *supra p.43*

[180] Explanatory Memorandum to COM/2021/206 final, para 5.2.3

[181] Regulation (EU) 2016/679, Art. 7 (3)

[182] Francis Limbach and Frédérique Ferrand, *Le Consentement Contractuel à l'Épreuve Des Conditions Générales : De l'Utilité Du Concept de Déclaration de Volonté* (LGDJ 2004).

[183] Phil Lee and Leonie Powers, 'Data Protection Issues in AI' (*www.youtube.com23 April 2021*) <https://www.youtube.com/watch?v=aV4BpDpEWg0>.

[184] COM/2021/206 final, Art. 65 (2)

placed on the market no longer conforms with the envisioned AIA.[185] It notably imposes on the provider to set up a "post-market monitoring system" as well as "procedures related to the reporting of serious incidents and of malfunctioning".[186] These requirements would reasonably be expected to accommodate the possibility to create further security features or improve the ones currently implemented.

Considering the points developed above, it would appear that the mechanisms that serve data protection by design and by default under the GDPR are effectively implemented throughout the Proposal, although some to a lesser extent. The weight of the issues engendered by this last observation will heavily depend of the determination of how close to the GDPR the envisioned AIA will effectively operate.

B. The place of accountability

The principle of accountability is one of the arguably most significant strengths of the EU's data protection framework under the GDPR: according to Professor Ibo Van de Poel and Doctor Martin Sand, "accountability is a first step in (incremental) learning, which is crucial for responsible innovation."[187] In a broad sense, accountability is a subcategory of responsibility and particularly relates to what Professor Van de Poel and Doctor Sand called "backward-looking" attribution of responsibility. Backward-looking responsibility generally serves to identify a person that is to be held responsible for an act prior to the act itself.[188] Under the GDPR, the notion of accountability is to be drawn from Article 24, which imposes on the controller to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with

[185] COM/2021/206 final, Art. 16 (g) & Art. 65 (4)

[186] COM/2021/206 final, Art. 17 (h) (i)

[187] Ibo Van de Poel and Martin Sand, 'Varieties of Responsibility: Two Problems of Responsible Innovation' (2018) 198 Synthese, 16.

[188] *Ibid.*

this Regulation".[189] This double requirement for the controller to implement the necessary measures and to hold the capacity to demonstrate that the processing in question is compliant with the GDPR is the essence of accountability. The article does not explicitly mention accountability, rather placing the requirements aforementioned under the responsibility of the controller. However, there is a general consensus that, while accountability and responsibility are closely related, they are not the same thing: the Article 29 Data Protection Working Party notably drew the difference where the emphasis of accountability is on "showing how responsibility is exercised and making this verifiable", hence being a necessity for the implementation of responsibility.[190] Article 24 is often cited as the basis of accountability in the GDPR, with further measures reflecting the implementation of the principle, such as the obligation to carry out DPIAs.[191]

In the field of AI, the questions of responsibility and accountability were hotly debated amongst researchers.[192] In the envisioned AIA, the European Commission appeared to show preference for generally placing accountability relating to data protection on the user of an AI system. For example, the Proposal explicitly addresses the user's obligation to carry out DPIAs.[193] This may be seen as a reinforcement of the GDPR, considering that the EDPB and the EDPS have specified

[189] Regulation (EU) 2016/679, Art. 24 (1)

[190] Article 29 Data Protection Working Party, 'Opinion 3/2010 on the Principle of Accountability [WP 173]' (2010), para 21.

[191] Cécile De Terwangne, 'L'« accountability » en tant qu'obligation générale pour le responsable du traitement' in *Le Règlement Général Sur La Protection Des Données (RGPD/GDPR) : Analyse Approfondie* (Larcier 2018), para 24.

[192] *See, eg.* Joanna J Bryson, Mihailis E Diamantis and Thomas D Grant, 'Of, For, and by the People: The Legal Lacuna of Synthetic Persons' (2017) 25 Artificial Intelligence and Law 273, *or* European Parliament, 'Report with Recommendations to the Commission on Civil Law Rules on Robotics' [2015/2103(INL)] (2015), § 59 (f)

[193] COM/2021/206 final, Art. 29 (6)

that users were more likely to be data controllers than providers.[194] Generally, accountability should effectively be transposed from the GDPR to cases falling within the scope of the Proposal.

A notable point of friction, however, was raised in the context of regulatory sandboxes, as put forth by the envisioned AIA. Sandboxes are often described through their objectives: the Proposal defines them as a controlled environment designed to develop, test and validate AI systems before their placing on the market,[195] a definition that was confirmed by the EDPB and the EDPS.[196] The concern raised by the EDPB and the EDPS concerning sandboxes and accountability was specific to the special provisions of Article 54, which enable the reuse of personal data under specific conditions listened, the most significant ones being the objective of "safeguarding substantial public interest" in dealing with criminal offences, public health and public safety and / or high-level protection and improvement of the quality of the environment; the requirements of necessity; the further effective protection through data isolation and deletion and the proof of justified or legitimate aim for processing such data.[197] The EDPB and the EDPS argued that the predominant role played by the competent authorities in enabling this reuse of data shifted the accountability placed on the data controller by the GDPR to the competent authorities.[198] Such concern would be agreeable: under Article 53 of the Proposal, sandboxes "take

[194] 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)', para 20, 9.

[195] Explanatory Memorandum to COM/2021/206 final, para 5.2.5 & COM/2021/206 final, Art. 53 (1)

[196] 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)', para 66, 18.

[197] COM/2021/206 final, Art. 54

[198] 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)', para 65, 18.

place under direct supervision and guidance by the competent authorities with a view to ensuring compliance with the requirements of this Regulation".[199] In the context of the reuse of data, the direct supervision and particularly the direct guidance befalling the competent authorities, coupled with the role played by such authorities in determining whether the reuse of data falls within the requirement of the significant public objectives listed prior, could be seen as a factual placing of the accountability on the competent authorities, as they may imply that such authorities hold a duty to implement specific measures attesting to the compliance with the GDPR in relation to this requirement. Article 53, which, relating to regulatory sandboxes in general, indicates that the provisions set out in the envisioned AIA should not affect the liability of the participants under other EU legislation for "harm inflicted on third parties as a result from the experimentation taking place in the sandbox",[200] holds a general idea of reaffirming the liability of the participants of the regulatory sandboxes for the AI systems developed. A similar provision safeguarding the accountability of the data controller under the GDPR would be greatly appreciated, as it "shifts much of the burden of policing against bad actors and irresponsible data use from individuals to the organisations that derive value from data".[201]

C. Human oversight as a safeguard to Article 22 of the GDPR

Article 22 of the GDPR confers the right of data subjects "not to be subject to a decision based solely on automated processing […] which produces legal effects concerning him or her or similarly significantly affects him or her", unless the decision is taken on the basis of consent

[199] COM/2021/206 final, Art. 53 (1)

[200] COM/2021/206 final, Art. 53 (4)

[201] R Thomas, 'Accountability – A modern approach to regulating the 21st century data environment' in Hielke Hijmans, H Kranenborg and PJ Hustinx (eds.), *Data Protection Anno 2014 : How to Restore Trust? : Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014) (Intersentia, Portland, Or, Usa 2014)*, 147.

from the data subject, performance of a contract between the data subject and the data controller, or authorisation by EU or Member-State law.[202] The applicability of such exceptions, however, is subject to restrictive safeguards, particularly that of the data subject's access to human intervention.[203] The Article 29 Data Protection Working Party highlighted that the human intervention set out as an implementation to the right not to be subject of decisions based solely on automated processing had to be efficient, specifying that "any review must be carried out by someone who has the appropriate authority and capability to change the decision."[204] Article 22 of the GDPR is highly relevant to AI, to the extent that automated decision-making is central to AI designs in many instances.[205] The European Commission's High-Level Expert Group on AI echoed its provision in 2019, stating that "humans interacting with AI systems must be able to keep full and effective self-determination over themselves".[206]

Article 14 of the Proposal gives a commendable importance to human oversight: it provides for high-risk AI systems to inherently require human oversight before data subjects are exposed to them,[207] particularly, to the extent that the following is technically feasible, through the implementation of specific measures before exposure of data subjects to high-risk AI system.[208] It further confirms that the individual in charge of human oversight must hold the power to

[202] Regulation (EU) 2016/679, Art. 22 (1) (2)

[203] Regulation (EU) 2016/679, Art. 22 (3)

[204] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' [WP 251] (2017), 27.

[205] Phil Lee and Leonie Powers, 'Data Protection Issues in AI' (*www.youtube.com* 23 April 2021) <https://www.youtube.com/watch?v=aV4BpDpEWg0>.

[206] High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI (2019), para 2.2, 12.

[207] COM/2021/206 final, Art. 14 (1)

[208] COM/2021/206 final, Art. 14 (3)

overturn the automated decision.[209] The EDPB and the EDPS, however, found fault in Article 14 in relation to the quality of the human oversight, stating that "real human centrality should leverage on highly qualified human oversight and a lawful processing as far as such systems are based on the processing of personal data or process personal data to fulfil their task so as to ensure that the right not to be subject to a decision based solely on automated processing is respected."[210]

Such statement would be agreeable to the extent that some requirements placed on the individuals responsible for the human oversight may be insufficient in demonstrating that they hold appropriate authority and capability to change the decision: for example, the capacities to detect "anomalies, dysfunctions and unexpected performance"[211] or to be aware of "automation bias"[212] are highly limitative: while they may suffice to determine that the AI system should not be used, the same cannot be said about effectively changing the decision. However, Article 14 does call for the quality of human oversight in stating that the individual appointed must "be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available".[213] This provision indeed requires of the individual to understand the reasons why the system came to that decision. Thus, it may indicate that the individual must have sufficient knowledge to understand the different situations and reasoning that might lead to a decision. It is nevertheless unclear whether this point should be interpreted so, or that it would simply mean that the natural person must be able to understand what the automated decision means for its subject.

[209] COM/2021/206 final, Art. 14 (4) (d)

[210] 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)', para 7, 6.

[211] COM/2021/206 final, Art. 14 (4) (a)

[212] COM/2021/206 final, Art. 14 (4) (b)

[213] COM/2021/206 final, Art. 14 (4) (c)

In the former interpretation, Article 14 would provide enough safeguards under Article 22 of the GDPR; not in the latter. The EDPB-EDPS may be choosing a safer approach in calling for specific statements that explicitly require and guide the quality of human oversight.

CONCLUSION

Establishing an effective balance between legal provisions in support of AI uptake and innovation and the requirements of the GDPR plays a vital role in the development of a data protection framework adequate to regulating AI. It has been frequently remarked that the stringent demands of the GDPR, which aim to provide data subjects with a rigorous protection of their personal data, would be intrinsically incompatible with maintaining EU competitivity in the field of AI development: such competitivity would require the enhancement of AI efficiency, based on the mass-processing of training data-sets. If any truth were to be drawn from the remark throughout this essay, it would be that of the complexities faced by the legislative authorities when setting the legal foundations for AI systems as protective of the rights of data subjects as they are efficient. This paper endeavoured to give a satisfactory answer to the objections raised against the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), in the version of April 2021, pertaining to the protection of personal data, anchored in both the recognition of prevailing issues and the demonstration of an efficient equation to resolve them in the progress of future discussion. In consonance with the original thesis formulated in the introduction to this essay, it would appear that a central issue remains, around which the assessment of all others would gravitate: the determination of the amplitude within which the envisioned AIA and the GDPR would operate in synchronicity. To refer to the particulars previously developed, such amplitude would have been considerably easier to determine on the sole basis that the language of the Proposal unequivocally entails its complementary nature to the GDPR, had the European Commission not paradoxically denied the European Parliament and the Council of the European Union the adequate harmonisation in implementation mechanisms which would have been required to give practical effect to this complementarity. Furthermore, it is certain that this ambiguity has caused frequent struggles, within

this essay, between a prospective interpretation based on close proximity and one based on a more distant operation framework when attempting to determine whether the provisions of the Proposal successfully address the data protection issues raised by AI. Among the difficulties are the consequences of the mitigation of rights under the Proposal's approach to risk, the intricacy of effective transparency allowing quality consent, the accountability of data controllers in the context of regulatory sandboxes and the quality of human oversight in safeguarding the right not to be subject to a decision based exclusively on automated processing. A sole guidance was the personal speculation, heavily defended, that the convoluted aspect of the material provided by the European Commission in this regard may be calculated to bring about, through supplementary discussions, resolutions to the prevailing issues of AI and data protection that would be adequate to their technical complexity. In light of this possibility, it would appear suitable to conjecture that the proposed AIA may have been vindicated from claims of its incompatibility with the principles of the GDPR: although it does not resolve all of the outlined issues, it certainly provides a great formula to do so. It is not impossible, and, in fact, it is rather probable, that the final version of the Artificial Intelligence Act will not be a perfect regulation and will eventually require further amendments. In this regard, it would seem appropriate to quote the eighty-fifth Federalist Paper as a closing statement:

"No advocate of the measure can be found, who will not declare as his sentiment, that the system, though it may not be perfect in every part, is, upon the whole, a good one; is the best that the present views and circumstances of the country will permit; and is such an one as promises every species of security which a reasonable people can desire."[214]

[214] Alexander Hamilton and others, 'Federalist No. 85' in *The Federalist Papers : A Collection of Essays Written in Support of the Constitution of the United States : From the Original Text of Alexander Hamilton, James Madison, John Jay* (Johns Hopkins University Press 1981).

CERTIFICATE OF ORIGINALITY

I hereby certify that this research paper submitted by me is an outcome of my independent and original work. I have duly acknowledged all the sources from which the ideas and extracts have been taken. The project is free from any plagiarism and has not been submitted in Germany or elsewhere for publication.

29.05.22