European Journal of Risk Regulation (2024), **15**, 757–771
doi:10.1017/err.2024.13

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Groups of Persons in the Proposed AI Act Amendments

Liubomir Nikiforov

Vrije Universiteit Brussel Faculteit Recht en Criminologie, Brussels, Belgium
Email: Lyubomir.Nikiforov@vub.be

Abstract

This article explores the proposed amendments to the AI Act, which introduce the concept of "groups of persons". The inclusion of this notion has the potential to broaden the traditional individual-centric approach in data protection. The analysis explores the context and the challenges posed by the rapid evolution of technology, with an emphasis on the role of artificial intelligence (AI) systems. It discusses both the potential benefits and challenges of recognising groups of people, including issues such as discrimination prevention, public trust and redress mechanisms. The analysis also identifies key challenges, including the lack of a clear definition for "group", the difficulty in explaining AI architecture concerning groups and the need for well-defined redress mechanisms. The article also puts forward recommendations aimed at addressing these challenges in order to enhance the effectiveness and clarity of the proposed amendments.

Keywords: AI; biases; data protection; discrimination; EU; group privacy; groups of persons; redress; trust

I. Introduction

The rapid advancement of artificial intelligence (AI) has ushered in a transformative era, impacting diverse aspects of society and individuals' lives. It already influences the way we interact, work, learn and do business. Nevertheless, algorithms pose several societal, economic and legal challenges. In this context of change, the European Union (EU) has taken actions in order to regulate this technology and the risks thereof. From one side, the ambition is to create a trustworthy, human-centric, secure and ethical AI. From the other, the ambition is to prevent fragmentation of the European market by ensuring legal certainty.

The purpose of this article is to explore those proposed amendments to the AI Act that introduce the notion of group or "groups of persons" as potentially adversely affected parties by an AI-powered system. This is a major novelty that has the potential to shift current data protection approach in a new direction. The review of the proposed amendments referring to "groups of persons" shows that the changes are concentrated into three main categories. According to the intended remedy they provide to an identified concern, those categories are adverse effects, public trust and redress mechanisms. Despite those intentions, the lack of definition of the notion of "group", the challenge of providing a description of the involved AI's logic and the unclear redress mechanism concerning harms suffered by groups of persons are challenges that need to be addressed by the legislator.

The methodology employed in this analysis involves a comprehensive review and critical evaluation of the AI Act's proposed amendments, incorporating legal analysis, historical review and consideration of technological advancements. The structure of this research article includes an introduction to the topic (Section I), followed by a brief review of the societal impacts of AI (Section II) and, within in this context, the AI Act proposal (Section III). Next, I discuss concretely the categories and challenges around the amendments envisaging groups of persons (Section IV) in order to provide specific recommendations for improvement of the proposed texts (Section V). (Section VI) concludes, and (Section VII) lists some limitations of this analysis.

II. AI in context

AI promises more efficient supply chains and workflows, faster and more customised services, optimised administration, better healthcare and new professional opportunities.[1] Despite the promising future AI technology paints for us, some have voiced concerns about the pace and scope of this technology.[2] Algorithm-based technologies pose important social, economic and ethical challenges.

First, in terms of social interaction, AI has already changed the ways we interact on the Internet, relate with others or choose our leaders.[3] Take, for example, platforms like Facebook, Twitter (now X),[4] LinkedIn[5] and Tinder,[6] which use AI for content moderation, creation and analysis as well as for advertisement.

Second, algorithms influence the ways we work and trade due to its integration into business operations and commercial strategies.[7] One of its main advantages but also concerns is its deployment in customer monitoring and online behaviour tracking. Although it is true that AI enables companies to personalise clients' experiences, this poses critical pitfalls when it comes to the misuse of this technology and possible discrimination based on biased data, amongst other potential issues.

Third, AI raises several ethical challenges related to the human implications in the decision-making processes of algorithm-based services and individual privacy. Algorithms learn from historical data, which more often than not contain the inherent biases present in society. When these biased datasets are used to train new AI models, they can perpetuate and even amplify societal prejudices. Added to the lack of adequate

[1] High-Level Expert Group on AI (AI HLEG), "Ethics Guidelines for Trustworthy AI" <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (last accessed 15 September 2023).

[2] ibid; "Pause Giant AI Experiments: An Open Letter" (*Future of Life Institute*, 2023) <https://futureoflife.org/open-letter/pause-giant-ai-experiments/> (last accessed 9 October 2023).

[3] A Rabitsch, R Wazir and T Treml, "Policy Paper on Artificial Intelligence's (AI) Impact on Freedom of Expression in Political Campaign and Elections" (2021) OSCE.

[4] AS Gillis, "The Impact of AI on Social Media" (*Techtarget*, 8 June 2023) <https://www.techtarget.com/whatis/feature/The-impact-of-AI-on-social-media> (last accessed 17 August 2023).

[5] H Srinivasan, "Helping Recruiters Save Time and Increase Candidate Engagement with AI" (*LinkedIn*, 17 May 2023) <https://www.linkedin.com/business/talent/blog/talent-acquisition/helping-recruiters-save-time-increase-candidate-engagement-with-ai?lipi=urn%3Ali%3Apage%3Ad_flagship3_pulse_read%3BfBxA%2BQ1fSe%2BImSYVqegvmA%3D%3D> (last accessed 17 August 2023).

[6] H Farah, "Tinder Tests AI Tool to Help Users Select Best-Looking Photos" (*The Guardian*, 3 August 2023) <https://www.theguardian.com/technology/2023/aug/03/heres-a-thought-tinder-tests-ai-tool-to-help-users-select-best-looking-photos> (last accessed 17 August 2023).

[7] B Marr, "The 10 Best Examples of How Companies Use Artificial Intelligence in Practice" (*Forbes*, 9 December 2019) <https://www.forbes.com/sites/bernardmarr/2019/12/09/the-10-best-examples-of-how-companies-use-artificial-intelligence-in-practice/> (last accessed 17 August 2023).

due-diligence mechanisms ensuring transparency and accountability in an AI's output,[8] this can lead to discriminatory outcomes in areas such as recruitment, money lending and law enforcement. Privacy is yet another significant ethical concern.[9] AI systems often require access to vast amounts of personal data to function effectively. The collection, storage and use of these data raise questions as to the effectiveness of the current understanding of privacy. AI's inference capabilities defy the individual-centred approach of data protection and, therefore, the very founding of current legislation.[10]

In this context of economic, social and ethical uncertainty, the proposal for a Regulation on Artificial Intelligence[11] (AI Act) is the European legislative response thereof.

III. The AI Act: context, novelties and purpose

1. Political context

Not many jurisdictions have taken actions in order to regulate algorithm-powered technologies and the risks thereof.[12] Some of the reasons for this lagging behind of the legislators is probably the backlash from investors, the novelty and the uncertainty around the scope of the implications of AI as well as its consequences for governments.[13]

The political commitment that brought up the current proposal for the Regulation dates back to 2017 with the explanatory memorandum of the proposal states,[14] when the European Council issued its Conclusions,[15] which were followed by a series of statement documents in 2019 and 2020.[16] The European Parliament (EP) engaged in this process and supported the adoption of a number of resolutions outlining what would take shape as the

[8] C Cath, "Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges" (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20180080 <https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0080> (last accessed 19 August 2023).

[9] AA Khan et al, "Ethics of AI: A Systematic Literature Review of Principles and Challenges", *The International Conference on Evaluation and Assessment in Software Engineering 2022* (ACM 2022) <https://dl.acm.org/doi/10.1145/3530019.3531329> (last accessed 9 January 2024); BC Stahl and D Wright, "Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation" (2018) 16 IEEE Security & Privacy 26 <https://ieeexplore.ieee.org/document/8395078/> (last accessed 9 January 2024); M Milossi, E Alexandropoulou-Egyptiadou and KE Psannis, "AI Ethics: Algorithmic Determinism or Self-Determination? The GPDR Approach" (2021) 9 IEEE Access 58455 <https://ieeexplore.ieee.org/document/9400809/> (last accessed 9 January 2024).

[10] JJ Suh et al, "Distinguishing Group Privacy from Personal Privacy: The Effect of Group Inference Technologies on Privacy Perceptions and Behaviors" (2018) 2 Proceedings of the ACM on Human–Computer Interaction 1 <https://dl.acm.org/doi/10.1145/3274437#sec-ref> (last accessed 18 September 2023); A Puri, "A Theory of Group Privacy" (2021) 30 Cornell Journal of Law and Public Policy 477 <https://community.lawschool.cornell.edu/wp-content/uploads/2021/11/Puji-final.pdf> (last accessed 1 September 2023).

[11] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final) 2021.

[12] J Shapiro and J Cota, "An Overview of Global AI Regulation and What's Next" (8 March 2023) <https://www.progressivepolicy.org/blogs/an-overview-and-of-global-ai-regulation-and-whats-next/> (last accessed 9 October 2023).

[13] ME Kaminski, "Regulating the Risks of AI" (2023) 103 Boston University Law Review 65; ITU, "Transformative Technologies (AI) Challenges and Principles of Regulation" (9 August 2023) <https://digitalregulation.org/3004297-2/> (last accessed 9 October 2023).

[14] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final), supra, note 11, p 2.

[15] Council of the European Union, "European Council Meeting (19 October 2017) – Conclusion, EUCO 14/17, 2017" <https://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf> (last accessed 15 September 2023).

[16] Council of the European Union, "Conclusions on the Coordinated Plan on Artificial Intelligence-Adoption 6177/19" <https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf> (last accessed 19 September 2023); Council of the European Union, "Special Meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020" <https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf> (last accessed 18 September 2023).

future AI Regulation framework. While those documents pledge for a comprehensive approach based on ethical principles and fundamental rights protection, addressing the risks of AI systems, it is the 2020 EP Resolution on a Framework of Ethical Aspects of Artificial Intelligence Robotics and Related Technologies that consolidates the principles guiding the European approach in a specific proposal for regulation.[17]

The European Commission made public on 21 April 2021 the proposal for a Regulation on Artificial Intelligence,[18] known as the AI Act. This piece of legislation is part of the larger EU strategy in the digital domain.[19] It builds on the documents adopted by the European Council and EP and is embedded into a series of revisions and adaptations of legislation in order to respond to the challenges posed by AI development and use.[20]

The ambition of the draft Regulation as stated by its explanatory memorandum is three-fold: first, to create a framework for a trustworthy, human-centric, secure and ethical AI; second, to prevent fragmentation of the European market by harmonising the requirements for "AI products and services, their marketing, their use, the liability and the supervision by public authorities"[21]; and third, to ensure legal certainty and to facilitate investment and innovation.[22]

Thus, the present AI Act proposal is the legal tool that the European legislator chose to set forth in order to address the risks emerging from the disparate national legislation and enforcement laws as well as from the production and commercial use of AI tools.

2. Novelties

With this intention in mind, the text of the proposed Regulation establishes a harmonised set of rules, limitations and requirements for AI creation, placement on the market and use.[23] The Regulation applies to providers placing on the market or putting into service AI systems or the use thereof, regardless of whether they are established in the Union market. It applies to all users located in the EU as well as in all those cases where, if located elsewhere, providers or users apply the output of an AI system within the Union. Thus, the wording of Articles 1 and 2 of the Regulation leave no doubt as to the universal scope of

[17] European Parliament, "European Parliament Resolution of 20 October 2020 on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies, 2020/2012(INL)" <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html> (last accessed 15 September 2023).

[18] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final), supra, note 11.

[19] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Shaping Europe's Digital Future. Com(2020)67 Final" <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020DC0067> (last accessed 10 September 2023); European Commission, "White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, COM(2020) 65 Final" <https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf> (last accessed 15 September 2023); European Commission, "Inception Impact Assessment for a Proposal for a Legal Act of the European Parliament and the Council Laying down Requirements for Artificial Intelligence" <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:Ares(2020)3896535&rid=3> (last accessed 15 September 2023).

[20] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Shaping Europe's Digital Future. Com(2020)67 Final", supra, note 19.

[21] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final), supra, note 11; European Commission, "Inception Impact Assessment for a Proposal for a Legal Act of the European Parliament and the Council Laying down Requirements for Artificial Intelligence", supra, note 19.

[22] ibid.

[23] Art 1, AI Act proposal.

application of the proposed document, as well as the ambition of its drafters to set and lead the global standard in the field of AI regulation.[24]

The proposed AI Act follows a risk-based approach based on three levels of AI impacts on individuals, namely unacceptable risk, high risk and low risk. First, the Regulation prohibits AI practices that are considered to be particularly harmful and posing unacceptable risk with regard to human dignity, freedom, equality, democracy and the rule of law as well as fundamental rights (Recital 15). Specifically, AI systems intended to distort human behaviour (Recital 16) and to provide social scoring of individuals (Recital 17) as well as systems enabling "real-time" remote biometric identification (Recital 18) are forbidden expressly in Article 5.

Second, particular requirements are laid down for high-risk AI systems, which have the potential to impact significantly fundamental rights and decrease safety. The Regulation mandates the establishment of a risk management system (Article 9), which should make sure that the minimum but compulsory requirements concerning training data quality (Article 10), documentation (Article 11), recordkeeping (Article 12), transparency (Article 13), human oversight (Article 14) and accuracy and robustness (Article 15) are respected. In addition, a conformity assessment mechanism (Article 43) is foreseen as well. The Regulation lays down obligations for providers and deployers of high-risk AI systems as well as other involved parties (Articles 26–29).

Finally, other low-risk algorithms are bound by less strict rules but still have to comply with transparency obligations. In addition, the AI Act sets forth an institutionalised governance system at the Member State level and creates a European Artificial Intelligence Board.

3. Purpose

The yet-to-be-enacted AI Act is one of the major legislative undertakings of the current EU executive government. The AI Act strikes a balance between, from one side, the yet-to-be-explored AI technology promises and, from the other, the issues it poses to fundamental rights. Precisely there resides the core of the debate around the Regulation on AI.

The criticism around the AI Act points out that the approach adopted seems overly paternalistic.[25] In this vein, some EU governments considered that raising the compliance costs for an emerging industry whose full potential is yet to be explored may hinder European competitiveness in a global market driven by powerful big tech companies established outside of Europe.[26]

However, it seems that the AI Act's critics do not give an account of EU competition policy. The European approach boils down to one main objective, and that is to achieve market integration by reducing barriers to private initiatives[27] and by protecting "competitors rather than competition".[28] This understanding of the EU's economy substantiates the prohibition

[24] "The proposal also strengthens significantly the Union's role to help shape global norms and standards and promote trustworthy AI that is consistent with Union values and interests. It provides the Union with a powerful basis to engage further with its external partners, including third countries, and at international fora on issues relating to AI." AI Act proposal, p 5.

[25] M Wörsdörfer, "The E.U.'s Artificial Intelligence Act: An Ordoliberal Assessment" (2023) AI and Ethics <https://link.springer.com/10.1007/s43681-023-00337-x> (last accessed 5 January 2024).

[26] The Joint Non-Paper by Italy, France and Germany exemplifies this stance. See L Nikiforov, "Joint Non-Paper on the AI Act. France, Germany and Italy Reach Consensus" (*Brussels Privacy Hub*, 2023) <https://brusselsprivacyhub.com/wp-content/uploads/2023/12/Joint-Non-Paper-on-the-AI-Act.-France-Germany-and-Italy-reach-consensus.-November-2023-LN-FINAL.pdf> (last accessed 7 January 2024).

[27] R Van den Bergh, *Comparative Competition Law and Economics* (Cheltenham, Edward Elgar Publishing 2017).

[28] GJ Werden and LM Froeb, "Antitrust and Tech: Europe and the United States Differ, and It Matters" (2019) SSRN Electronic Journal <https://www.ssrn.com/abstract=3442798> (last accessed 5 January 2024); M Iacovides and K Stylianou, "The Goals of EU Competition Law: A Comprehensive Empirical Investigation" (2022) 42 Legal Studies 620 <https://www.cambridge.org/core/journals/legal-studies/article/goals-of-eu-competition-law-a-comprehensive-empirical-investigation/4D18A299D5CC9B005F8DFD8F7489047C#article> (last accessed 5 January 2024).

that "the competition may not be eliminated for a substantial part of the relevant market as one of the four cumulative conditions to grant an exemption from the cartel prohibition".[29] This is why EU competition policies are based on the idea of a market of small and medium-sized companies that should be protected and whose initiative should be unhindered.[30] Therefore, EU competition regulations are not intended to favour big conglomerates, as is the case for other players such as the USA and China, where, for different reasons, companies are able to amass huge market power. The European approach to the AI industry aligns with its own competition doctrine. It is not intended to create companies able to capture a whole market in order to exert influence on the other market players. Furthermore, the framework of the AI Act aims to provide a common level playing field for those who use AI or would like to enter the market, following the EU's competition policy. The Regulation aims to provide clarity and certainty for companies operating in the industry and, through this, to encourage innovation and investment in the development of new AI technologies that comply with the General Data Protection Regulation (GDPR) and other data protection regulations. In that sense, the AI Act aims to establish accountability and transparency rules that could eventually translate into increased trust in AI systems and, consequently, greater adoption of the technology.[31]

While some express uncertainty about the Regulation's success,[32] its drafters are confident that the AI Act will become a beacon for other jurisdictions in matters of regulating AI and repeat the game-changing impact of the GDPR. Doubts persist, however, over the end result, as some challenge the potential of the AI Act to reaffirm the power of the *Brussels effect*.[33]

While the previous paragraphs aimed to provide a picture of the context, novelties and envisaged general purpose of the AI Act, in the following I focus particularly on the EP's proposed amendments of the Regulation,[34] especially concerning the notion of "groups of persons" and its challenges.

IV. The amendments: groups of persons

The proposed amendments introduce the notion of group or "groups of persons" next to the notion of an individual as potentially adversely affected parties by an AI-powered system. This is a major novelty that has the potential to shift the current data protection

[29] Van den Bergh, supra, note 27.

[30] European Commission, "Inception Impact Assessment for a Proposal for a Legal Act of the European Parliament and the Council Laying down Requirements for Artificial Intelligence", supra, note 19; European Union, "Consolidated Version of the Treaty on the Functioning of the European Union, C 326/49"; Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final), supra, note 11.

[31] The objective to raise trust and hence increase the adoption rates of this technology is a subject of a debate. See J Laux, S Wachter and B Mittelstadt, "Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk" (2023) 18 Regulation & Governance 3.

[32] A Calderaro and S Blumfelde, "Artificial Intelligence and EU Security: The False Promise of Digital Sovereignty" (2022) 31 European Security 415 <https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2101885> (last accessed 19 September 2023); OJ Gstein, "European AI Regulation: Brussels Effect versus Human Dignity?" (2022) 25 Zeitschrift für Europarechtliche Studien (ZEuS) 755.

[33] Gstein, supra, note 32; S Feldstein, "Evaluating Europe's Push to Enact AI Regulations: How Will This Influence Global Norms?" (2023) Democratization 1 <https://www.tandfonline.com/doi/full/10.1080/13510347.2023.2196068> (last accessed 5 February 2024).

[34] European Parliament, "Amendments Adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))" <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html> (last accessed 8 September 2023).

approach in a new direction. The current approach is entirely centred on the role and place of the individual user in relation to the processing party. This individual-based approach owes its central place to the technological and legislative reality that data protection law evolved in over recent decades.[35]

1. Historical background

In the following paragraphs, I revise briefly the origins and conceptualisation of the current approach with regard to the technological reality back then as well as the legal understanding of the matter.

First,[36] individual data were collected directly from single users, often mainly relying on consent. Consent has a long history, dating back to antiquity,[37] as a tool expressing someone's will and knowledge,[38] which reflects an individual's autonomy to decide. The core idea behind consent is for it to be a tool empowering individuals in a power-asymmetrical relationship – for example, between a patient and a physician or a data subject and a data controller. Putting it into perspective, consent as a lawful basis for data processing should be regarded as a component of the development of data protection and privacy policies.[39] Although the notion of privacy as a separate right was already being discussed in the nineteenth century,[40] it was not until the late 1970s–1980s that privacy and data protection acts were first adopted in some European countries.[41] In 1983, the German Constitutional Court adopted a landmark decision[42] establishing a right to "informational self-determination".[43] This decision is based on the idea that dignity, privacy and freedom to decide for oneself should be legally guaranteed in the digital environment as well.[44] This case

[35] F Bieker, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law*, vol 34 (1st editiong, The Hague, TMC Asser Press 2022) <https://link.springer.com/10.1007/978-94-6265-503-4> (last accessed 5 January 2024).

[36] This paragraph is inspired by L Nikiforov, "Informed Consent: Mission (Im)Possible, and Other Risk Remedies in Data Processing" (2022) Institute of European Democrats 1 <https://www.iedonline.eu/publications/2022/democracy-versus-autocracy/informed-consent-mission-impossible-and-other-risk-remedies-in-data-processing-liubomir> (last accessed 15 September 2023).

[37] P Dalla-Vorgia et al, "Is Consent in Medicine a Concept Only of Modern Times?" (2001) 27 Journal of Medical Ethics 59.

[38] TL Beauchamp and JF Childress, *Principles of Biomedical Ethics* (8th edition, Oxford, Oxford University Press 2019).

[39] PLM de la Cueva and JLP Mañas, *El derecho a la autodeterminación informativa* (Madrid, Fundación Coloquio Hurídico Europeo 2009) <https://www.fcjuridicoeuropeo.org/wp-content/uploads/file/Libros_Publicados/Cuadernos_Fundacion/EL%20DERECHO%20A%20LA%20AUTODETERMINACION%20INFORMATIVA.pdf> (last accessed 15 September 2023).

[40] SD Warren and LD Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193 <https://www.jstor.org/stable/1321160> (last accessed 15 September 2023).

[41] The Hessian Data Protection Act adopted in 1970 is Europe's and the world's oldest data protection law (Datenschutzgesetz, Gesetz- und Verordnungsblatt für das Land Hessen (GVB1) Teil I, Seite 625). Subsequent examples (as well as of the role of consent as a lawful ground for data processing) are: the 1973 Swedish Data Act, Datalag (1973:289), and the 1978 French Data Protection Act, Loi N° 78-17, the 1978 Danish Private Registers Act (LBK nr 622 af 02/10/1987) and the Public Authorities' Registers Act (LOV nr 294 af 08/06/1978), the 1978 Norwegian Personal Data Registers Act and the 1979 Austrian data protection act (BGBl I Nr. 565/1978). B van der Sloot, "Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation" (2014) 4 International Data Privacy Law 307.

[42] The famous German Constitutional Court case: Bundesverfassungsgericht (BVerfG). Urteil des Ersten Senats vom 15. Dezember 1983 (Judgement of the first senate of 15 December 1983) – 1 BvR 209/83, Rn. 1-215 – ECLI:DE:BVerfG:1983:rs19831215.1bvr020983.

[43] OJ Gstrein and A Beaulieu, "How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches" (2022) 35 Philosophy & Technology 3 <https://link.springer.com/10.1007/s13347-022-00497-4> (last accessed 5 February 2024).

[44] EJ Eberle, "Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview" (2012) 33 Liverpool Law Review 201.

plays a fundamental role in understanding the present-day data protection landscape and its focus on the individual as a holder, manager and controller of their data.

Second, since the census case, technology has evolved exponentially, and with it the amount of data collected and stored. In the early 2000s, the development of Big Data technologies made it possible to collect, process and store larger volumes of data in a faster and more efficient way. This led to the emergence of predictive analytics and machine learning, which shifted the value of the data, which "no longer resides solely in its primary purpose for which it was collected, but in its secondary uses".[45] Datasets are now interactive repositories that have the potential to allow AI systems to infer information regarding the subjects included in the dataset as well as those outside of it, build upon this information and take a decision or predict human behaviour through the combination of various sources of data. This unchains Big Data, or any other AI tool, from the necessity to collect data on all of the members of a given target group in order to achieve successful results. Furthermore, AI systems can affect individuals whose data are not present in the dataset that is used for the performance of the output of the AI system.[46] Thus, individuals' *voluntary* participation (eg through consent) is no longer crucial or necessary for the performance of an algorithm. This in turn translates into a lack of legal protection of those individuals who never consented to their data being collected or processed, and therefore they cannot rely on the rights enshrined in the GDPR. Hence, they are left with little to no legal protection or possibility to search for redress.

In sum, this dramatic change in the volume, velocity and variety[47] of the data collected and processed over recent years challenges the current data protection and privacy legislation state of affairs.[48] In particular, when it comes to individual control over personal data, the existing model of collection on the basis of consent seems inadequate, as do the mechanisms to prevent identification, such as anonymisation or differential privacy.[49]

In this context, the notion of groups of persons as employed in the EP's amendments to the proposed AI Regulation seem promising, and they are explored further in this article.

2. The AI Act's amendments on groups of persons: categories and challenges

The EP amends the AI Act proposal in such a way that it introduces "groups of persons" as potentially affected entities of high-risk AI systems. The new Amendment 167 to Article 3, paragraph 1, point 1b defines "significant risk" as the ability to "affect an individual, a plurality of persons or to affect a particular group of persons". Furthermore, Amendment 174 to Article 3, paragraph 1, point 8a (new) establishes that the "affected person" may include "any natural person or group of persons", and Amendment 191 to Article 3, paragraph 1, point 34 adds groups of persons to those possibly affected by an "emotion recognition system". These amendments testify to the purposeful and coherent intention to extend the AI Act's protected parties further, to those who may be affected adversely by an algorithm-based decision on the grounds of their belonging to a particular group. In order to understand how these changes fit within the AI Act, the remainder of this subsection is divided into two parts: categories of amendments and the challenges they pose.

[45] Puri, supra, note 10.

[46] L Taylor, L Floridi and B Van Der Sloot (eds), *Group Privacy: New Challenges of Data Technologies*, vol 126 (1st edition, Berlin, Springer 2017) <http://link.springer.com/10.1007/978-3-319-46608-8> (last accessed 10 September 2023).

[47] Often cited as the 3 Vs – volume, velocity and variety – these are the core properties defining Big Data.

[48] Taylor et al, supra, note 46.

[49] Puri, supra, note 10.

a. Categories

In this respect, the changes related to groups that the European legislator introduces could be clustered into three main categories, namely adverse effects, public trust and redress. In the following, this article explores those categories.

i. Adverse effects. Discrimination based on groups' characteristics can ensue from several technical and social contexts related to the development of an AI and its uses.[50] Its development and learning models, based predominantly on past historical data and records, play a crucial role.[51]

First, Amendment 50 to Recital 26a (new) highlights the particular risk of discrimination against individuals and groups of people. AI used by law enforcement authorities to make predictions, profiles or risk assessments based on "personality traits and characteristics, including the person's location, or past criminal behaviour of natural persons or groups of persons for the purpose of predicting the occurrence or reoccurrence of an actual or potential criminal offence(s)" may lead to a violation of human dignity and of the presumption of innocence.[52] Moreover, the use of AI systems involves a specific power imbalance between the respective authority and the suspect(s), who may face insurmountable obstacles in order to obtain meaningful information and challenge the results.[53] Therefore, those systems should be prohibited, pursuant to Amendment 224, Article 5, paragraph 1, point da (new).

Second, AI systems that influence decisions in the domain of education are considered high-risk "since they may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood".[54] The EP underlines the potential consequences of these systems for specific groups within society, such as "women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation".[55]

Third, the same reasoning applies in the professional domain as well as in the process of recruitment according to Amendment 66, Recital 36, "since those systems may appreciably impact future career prospects, livelihoods of these persons and workers' rights".

Fourth, AI may adversely influence and perpetuate historical discriminatory patterns and biases[56] as well as create new ones affecting persons or groups when it comes to their access to healthcare or other public and private services or benefits, following Amendment 67 to Recital 37.

ii. Public trust. Confidence in the decision-making process of an AI system and therefore in the results ensuing thereof is of prime importance for the deployment and use of algorithm-based systems. The principles of lawful, fair, transparent and accurate and accountable data collection and processing are some of the cornerstones of data protection.[57] They contribute to greater confidence in this technology, which collects and processes huge amounts of personal data. This is why they find their place in the proposed AI Act (Articles 13, 15, 52) as well. The amendments introduce a collective perspective to several of those principles, particularly in terms of accuracy, risk assessment and transparency.

First, when it comes to the accuracy of the information represented in the dataset used by the AI, the right balance between technical excellence in terms of operations'

[50] High-Level Expert Group on AI (AI HLEG), supra, note 1; Suh et al, supra, note 10.
[51] High-Level Expert Group on AI (AI HLEG), supra, note 1.
[52] Amendment 50, Recital 26a (new).
[53] Amendment 69, Recital 38.
[54] Amendment 65, Recital 35.
[55] Amendment 65, Recital 35.
[56] Amendment 78, Recital 44.
[57] Art 5 1(a), (d), 2 GDPR.

effectiveness and accuracy is indispensable in order to prevent any adverse impacts on individuals.[58] It is important to highlight the difference in the meaning of "accuracy" used in this context compared to the meaning of "accuracy" used in the GDPR. While in the latter accurate data in Article 5(d) designates data that are up to date and correctly reflect users' characteristics, in the AI Act "accuracy" signifies the correct output of the system. Updated personal data play a role in the correctness of AI predictions but are not the only factor that would influence the result. In this sense, technical resilience and the security of the system from external attacks should not be to the detriment of the quality of the data used to inform the predictions of the system.

Second, the role of developers and deployers of AI systems is essential to the risk assessment of the algorithm. A new Article 29a, under Amendment 413, is proposed in which a description of the fundamental rights impact assessment for high-risk AI systems is established. Points c) and f) specifically mention harm likely to impact groups. Moreover, in paragraph 4, Article 29a (new) mandates that representatives of the affected groups should be involved in the impact assessment procedure. Amendment 92, Recital 58a (new) establishes that the deployers of high-risk AI systems should create such governance mechanisms so that the potential adverse effects on "the people or groups of people likely to be affected, including marginalised and vulnerable groups" can be adequately foreseen. When it comes to assessing the harm posed by a high-risk AI system, a series of amendments[59] instruct that the impact on a "particular group of persons" should be taken into account as well.

The national supervisory authority on the matters contained in this Regulation should intervene whenever there is a suspicion that an "AI system exploits the vulnerabilities of vulnerable groups or violates their rights intentionally or unintentionally".[60]

Third, the group aspect has been embedded in the transparency mechanism foreseen in the AI Act. For example, Amendment 315, Article 10, paragraph 3 mandates that human oversight should be ensured "where decisions based solely on automated processing by AI systems produce legal or otherwise significant effects on the persons or groups of persons on which the system is to be used".

Furthermore, the technical information required for the placement on the market of an AI should include "the categories of natural persons and groups likely or intended to be affected"[61] and "the overall processing or logic of the AI system … with regard to persons or groups of persons",[62] as well as detailed information about "the degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected level of accuracy".[63]

iii. Redress. Importantly for the effectiveness of those changes, amendments envisaging redress mechanisms are foreseen. First, the proposed Recital 84a (new)[64] urges deployers to "provide internal complaints mechanisms to be used by natural and legal persons or groups of natural persons". Second, a new Article 68a is introduced aiming to empower users and "groups of natural persons" by providing them with a right to lodge a complaint before the respective national authority.[65]

[58] Amendment 86, Recital 50; Amendment 288, Art 10, para 3.

[59] Amendment 247, Art 7, para 2, point d; Amendment 253, Art 7, para 2, point g b (new); Amendment 256, Art 7, para 2a (new); Amendment 276, Art 9, para 8; Amendment 634, Art 69, para 2.

[60] Amendment 597, Art 65, para 2.

[61] Amendment 742, Annex IV, para 1, point 1, point a (new).

[62] Amendment 752, Annex IV, para 1, point 2, point b.

[63] Amendment 757, Annex IV, para 1, point 3.

[64] Amendment 133, Recital 84a (new).

[65] Amendment 628, Art 68a (new).

b. Challenges

The proposal to introduce groups as protected parties in the AI Act is a major innovation in the data protection landscape, whose main objective is to prevent negative effects of algorithmic decision-making that could have an impact on parties whose data have not been collected but whose processing thereof has an impact on. The potential of the collective dimension to fill this gap is not negligible. However, the place and role of groups within the larger data protection landscape, and particularly in the context of the AI Act, do not seem to be without pitfalls. In the following paragraphs, I explore the potential challenges that the notion of "group" would entail.

i. Challenge 1: definition of "group". The proposed AI Act as well as its amendments do not include a definition of "group" or "group of persons", unlike the detailed and layered description of individuals,[66] their role and their place within the architecture of the Regulation. This lack of legal definition is not isolated to this Regulation, because nowhere in the data protection legislation could be found any definition of collective entities or groups as protected data subjects. With no legal reference from the domain of data protection, it seems challenging to determine the applications and implications of the proposed provisions.

ii. Challenge 2: "plurality of notions". The wording of the text and its interpretation further increase this uncertainty. From one side, in three instances the text of the proposed amendments mentions the effect of AI on "a plurality of persons".[67] The lack of clarity on the definition of plurality of persons, however, seems surmountable when applying a textual analysis of the Articles in question. While groups of persons are separated by "or", individual and pluralities of persons are clustered together. Thus, it could be concluded that the legislator envisaged that harm could be inflicted on an individual or more than one person. This raises the question about the threshold at which a number of individuals becomes a group and, subsequently, the distinction between a "group of persons" and a "plurality of persons", given that both consist of more than one person. Therefore, a plausible interpretation is that the legislator refers to two separate groups. While groups of persons designates a concrete entity *identified* in the AI Act's vulnerable groups, "plurality of persons" is the term used for the individuals collectively affected by an AI's predictions.

Furthermore, this lack of clarity feeds on the apparent dichotomy between vulnerable groups of people and other groups. First, in multiple instances the text defines certain groups as "vulnerable". In particular, this reference can be found in provisions referring to prohibited AI techniques that could distort human behaviour,[68] the training models used,[69] the implementation of a risk management system,[70] the role of the supervisory body in this context[71] and the elaboration of codes of conduct.[72] Second, groups of persons could be harmed in the context of education and work as well as in the provision of public and private services. Although the amendments seem to avoid defining them as "vulnerable" and delimit their belonging to particular "minority subgroups"[73] in society usually associated with higher rates of discrimination, such as "persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation",[74] those subgroups happen

[66] AI Act, Art 3 (4), Amendments 172 to Art 3, para 1, point 4 and 174 to Art 3, para 1, point 8a (new).

[67] Amendment 60, Recital 32; Amendment 167, Art 3, para 1, point 1b (new); Amendment 247, Art 7, para 2, point d.

[68] Amendment 38, Recital 16.

[69] Amendment 78, Recital 44.

[70] Amendment 276, Art 9, para 8; Amendment 413, Art 29a (new).

[71] Amendment 597, Art 65, para 2.

[72] Amendment 634, Art 69, para 2.

[73] Amendment 86, Recital 50.

[74] Amendment 65, Recital 35; Amendment 66, Recital 36; Amendment 67, Recital 37.

to overlap with the groups who present the highest degree of vulnerability. Therefore, the meaning of these amendments should be interpreted as an attempt to establish the features that certain groups should comply with in order to be characterised as such. Third, the wording of Amendment 256, Article 7, paragraph 2a (new) and Amendment 413, Article 29a (new) supports this conclusion, which mandates that the AI impact assessment should include representatives of "people or groups of people likely to be affected, including marginalised and vulnerable groups".[75] Nevertheless, it remains uncertain as to how these groups' representatives would be identified and on what grounds they would be entitled to represent diverse and unrelated members of a group. In addition, it poses doubts as to the provisions' real effects unless those groups are institutionalised under some form of a union or association. Workers' unions are example thereof.

Other parts of the text suggest that vulnerable groups or marginalised minorities are not the only ones who could potentially be adversely affected by AI systems. The best example of this can be found in Amendment 413, Article 29a (new). While Article 29a (new) f) mandates that the fundamental rights impact assessment for high-risk AI systems shall include "specific risks of harm likely to impact marginalised persons or vulnerable groups", point c) establishes that the assessment shall include "categories of natural persons and groups likely to be affected by the use of the system". Therefore, the proposed amendments set forth a distinction between vulnerable groups and groups impacted by AI in general. This approach is similar to the one adopted by the GDPR concerning vulnerable data subjects.[76]

A possible critique to the conclusion drawn in the previous paragraph could stem from the fact that the proposed Article 29a (new) mandates that the impact assessment should establish categories of groups and, after that, delimit the specific risks of harm likely to affect vulnerable groups. Hence, the only groups envisaged by the legislator are those that bring together vulnerable and marginalised communities. While this might be the actual intention of the drafters of the text, it is plausible to expect that an impact assessment involving the identification of the affected groups would witness a surge of other *unexpected* groups of persons equally affected, although not "vulnerable", pursuant to the indications of the Regulation. It is uncertain, however, what action should be taken in such cases. Although these critiques might be grounded in the particular wording of the amendments, groups falling outside of the definitions of "vulnerable" or "marginalised" exist and could be equally influenced by an AI system's decisions. This is so because of the particular ways in which algorithms perform tasks. They could categorise and cluster users' data based on multiple indicators, which could give rise to the creation of random groups that would be unaware of their existence as such. The difference between stable (eg marginalised communities) and unstable groups stems from the level of awareness, institutionalisation and stability of the group. Stable groups,[77] also called active groups,[78], usually are aware of their belonging to the group, either because they are auto-proclaimed as such or because they are externally designated as such – take, for example, linguistic, cultural, professional or urban subgroups and minorities. The most important characteristic is that they are static and do not endure easy, rapid and random shifts in their morphology. Unstable groups, on the other hand, are usually externally

[75] Amendment 92, Recital 58a (new).

[76] G Malgieri and J Niklas, "Vulnerable Data Subjects" (2020) 37 Computer Law & Security Review <https://linkinghub.elsevier.com/retrieve/pii/S0267364920300200> (last accessed 20 September 2023).

[77] L Taylor, B Van Der Sloot and L Floridi, "Conclusion: What Do We Know About Group Privacy?" in L Taylor, L Floridi and B Van Der Sloot (eds), *Group Privacy: New Challenges of Data technologies*, vol 126 (1st edition, Berlin, Springer 2017) <https://link.springer.com/book/10.1007/978-3-319-46608-8> (last accessed 10 September 2023).

[78] L Kammourieh et al, "Group Privacy in the Age of Big Data" in L Taylor, L Floridi and B Van Der Sloot (eds), *Group Privacy: New Challenges of Data Technologies*, vol 126 (1st edition, Berlin, Springer 2017) <https://doi.org/10.1007/978-3-319-46608-8_3> (last accessed 10 September 2023).

proclaimed and unaware of their existence and relatedness. They are also highly malleable and thus could be created and dissolved rapidly. In addition, their structure and membership could evolve quickly. For example, while the students of a university may regard themselves as members of one community (therefore, a stable group), an algorithm could cluster some of them based on their postcode, gender or transportation used in order to infer correlations about the safety of the campus.

Therefore, while the Regulation envisages some protection for particular groups based on specific or general vulnerabilities, there could be groups issuing from an AI system's analytical capacities that would fall outside of the intended protected groups. Hence, individuals whose data do not participate in the dataset of the algorithm or are not identified in the Regulation would not be able to rely on effective protection against the adverse effects of a particular automated decision.

iii. Challenge 3: explainability 2.0. In this relation, a third challenge stems from the technical information required pursuant to Article 11(a) in Annex IV of the Regulation. Amendment 742 stipulates that before the deployment of an AI, a general description of the AI system has to include the categories of "natural persons and groups likely to be affected" by the algorithm. While for some groups, such as the previously mentioned stable ones, this is possible, AI's capacities allow the grouping of people based on many different, often unrelated indicators in order to reach a decision or to provide a particular output. Therefore, this Amendment raises doubts as to the effectiveness of providing a clear-cut general projection of the groups possibly affected by an AI system's output and consequently on the compliance of AI developers and deployers with the Regulation itself.

Moreover, Amendment 752 to Annex IV, paragraph 1, point 2, point b mandates that a description of the architecture, including the logic of the AI system, its rationale and its assumptions, has to be provided "also with regard to persons or groups of persons on which the system is intended to be used". This means that an ex-ante description of the architecture of the algorithm is needed. A developer may be able to design, create and successfully launch an AI, but this does not imply an understanding of what data determined its results, nor the specific process behind its determination. Hence, this text poses a challenging task to developers due to the nature of AI systems, which are intended to harness huge amounts of data and infer correlations that humans are otherwise unable to do. Providing understandable information regarding the purposes, functioning and outcomes expected of algorithmic data processing is often a fiction. This is so because in some cases it is very difficult to describe the purposes of this data collection. Data might be collected for one reason but later may prove useful for different, previously unspecified purposes.

iv. Challenge 4: redress mechanism. Finally, the fourth challenge posed by the wording of the amendments concerns the redress mechanism proposed in the amendments to the Regulation. A new Article 68a stipulates that "every natural persons or groups of natural persons shall have the right to lodge a complaint with a national supervisory authority". Furthermore, another amendment recommends that "it is essential that natural and legal persons or groups of natural persons have meaningful access to reporting and redress mechanisms and to be entitled to access proportionate and effective remedies". In the previous paragraphs, I have sustained that the lack of clarity on the definition of the notion of groups of persons as well as on the scope of the term prevents its effective application and performance as a separate subject of data protection. Those same pitfalls also determine the uncertainty around the mechanism for redress when groups of persons claim to have been harmed by an AI system's decision. The proposed new Articles do not clarify the requirements that groups should comply with in order to be able to lodge a complaint in procedural or substantial terms. It is not clear what types of groups could claim tort. Should only vulnerable or marginalised groups be able to do this, or should any other group that has been targeted and treated as group and suffered a tort thereof be able to lodge a complaint? In addition, who should prove that a passive group[79] (created externally; eg by an algorithm) is actually a group? Furthermore, it is unclear whether there should be a mechanism to represent the group as such or whether it would be represented be an appointee.

V. Recommendations

With regard to the discussion above concrete recommendations can be made that could serve as inspirations for the legislator as well as for further discussion and analysis of this matter.

1. Clarify the definition of the terms "plurality of persons" and "group of persons"

If the AI Act is enacted with the current amendments, the Regulation should include definitions of those terms in order to clarify their scope and their intended addressees, if they are two separate entities. Data protection law has not developed a notion of "vulnerability"[80] or of the groups affected by algorithm-based decision-making. Therefore, the dichotomy between particularly affected and generally affected groups because of their specific social status or because of the logic of the algorithm reinforces the uncertainty around the introduction of the notion of groups. In addition to the clarification of these terms, the AI Act should foresee the implications thereof when it comes to the representation of those groups in the impact assessment mechanism.

2. Clarify how AI developers and deployers can provide general and detailed descriptions of the AI architecture concerning groups of persons

Further improvement of the Regulation proposal should envisage the need to provide a more detailed description of the information that those groups should expect. EU legislators should take a stance on the question as to which groups are entitled to an explanation of the functioning of the algorithm as a system and how this description of the logic of the algorithm would be reasonably achieved.

3. Provide guidelines on the redress mechanism for groups of persons

Provisions on the mechanism for redress for groups of persons would empower not only vulnerable groups but also those individuals whose data were not collected but who are affected by the AI system's inference capabilities. A common framework for lodging collective complaints, including the requirement to prove harm based on defined requirements, would provide legal certainty for users and AI providers and ultimately extend the legal coverage of data protection.

VI. Conclusion

The proposed amendments introducing the notion of "groups of persons" into the AI Act are a significant step forward in addressing the challenges posed by AI systems that influence individuals whose data have not been directly collected. These changes have the potential to broaden the data protection framework and adapt it to the evolving

[79] Following the distinction between active and passive groups in ibid.
[80] Malgieri and Niklas, supra, note 76.

technological landscape. By recognising and providing protection for groups of persons, the amendments attempt to bridge the gaps in current data protection approaches and ensure that the rights of individuals affected by AI are upheld. Therefore, the notion of "groups of persons" is relevant and necessary. However, these amendments are not without their challenges. The lack of a clear legal definition of "groups" raises uncertainty regarding the scope and application of the proposed changes. Additionally, understanding and providing a detailed description of the involved AI system's logic concerning groups of persons can be technically challenging. It is necessary to carefully consider how to effectively explain AI systems in a meaningful and understandable way. Moreover, establishing a comprehensive and fair redress mechanism for groups of persons is a complex task that requires further clarification and guidelines to ensure its effectiveness and accessibility. Not addressing these challenges risks undermining the AI Act's intended purpose of protecting users, reducing it simply to a group of words.

VII. Limitations

This analysis is not without its limitations, which stem from the evolving nature of the legislation in question. The provisions discussed above are part of the proposed amendments to the AI Act's text by the EP, which entails some uncertainty as to the final text of the Regulation. This is the first ever piece of legislation on the matter of AI. Hence, there is no reference jurisprudence that this analysis could rely on. In addition, the notions of group or group privacy represent underexplored terrain when it comes to their application to data protection or AI as well as their practical consequences. This is the reason as to why this article envisages a further revision that would take into account the final and definite text of the AI Act once enacted. Despite these limitations, my hope is that this article inspires further investigations into the matter because I believe it opens new horizons in data protection and privacy scholarship.

Competing interests. The author declares none.

Cite this article: L Nikiforov (2024). "Groups of Persons in the Proposed AI Act Amendments". *European Journal of Risk Regulation* **15**, 757–771. https://doi.org/10.1017/err.2024.13