ERA Forum
https://doi.org/10.1007/s12027-023-00777-2

ARTICLE

Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: shaping the digital legal order while upholding Rule of Law principles and European values

Stéphanie Laulhé Shaelou[1] · Yulia Razmetaeva[2,3]

Accepted: 13 December 2023

Abstract

Recently, the concept of the 'European digital legal order' seems to have gained more importance than the overarching concept of European legal order, of which the former is arguably a modern manifestation. The European legal order traditionally entails a set of fundamental human rights, Rule of Law principles and Democratic values as enshrined in the multinational legal order. From maintaining the Rule of Law derive the sustainability of Democratic values, and freedoms under the law enshrined

The first author is Professor of European Law and Reform, Head of School of Law, Director of the Jean Monnet Centre of Excellence for the Rule of Law and European Values (CRoLEV), University of Central Lancashire, Cyprus. The first author thanks the Academy of European Law (ERA) for their invitation to write this article following the invitation to their Annual Conference on 'AI Systems and Fundamental Rights', to chair the Roundtable Discussion on 'Clarifying expectations for conducting risk assessments' on 7-8.4.2022 in Brussels and online, as well as for their invitation to participate to the Roundtable discussion on 'Liability for fundamental rights violations arising from AI systems' on 30.3.2021 online. Many thanks also go to all peers involved in the discussion and/or the review of this paper throughout the years, including Dr. Klearchos Kyriakides who provided valuable comments before publication. All errors remain our own. This research is affiliated with the Jean Monnet Centre of Excellence CRoLEV (2022-25) Grant Agreement Grant decision no 101047752, co-funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The second author is the head of the Jean Monnet Centre of Excellence European Fundamental Values in Digital Era (EFVDE). This research is also affiliated with the Jean Monnet Centre of Excellence EFVDE (2022-25) Grant Agreement decision no 101085385, co-funded by the European Union. Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Extended author information available on the last page of the article

Published online: 10 January 2024

in fundamental human rights. To the extent that the European digital legal order is the manifestation of the European legal order in the modern digital world, the fundamental question of the nature, scope and upholding of fundamental human rights, Rule of Law principles and Democratic values remains. Without disputing the need for digital transformation and its proper regulation, this paper will turn its attention to the current status of fundamental principles in the modern setting of democratic societies.

Artificial Intelligence or Artificial Intelligence Systems are technologies that have and will have a serious impact on the European legal order at large. Without dismissing the value of a human-centered regulatory approach in the field of AI, in this paper we discuss why this may be difficult as digitisation and algorithmisation deepen. This paper reviews the regulatory framework of AI and proposes potential new/renewed/modernised rights that should enhance and/or supplement the current catalogue of fundamental human rights, as contained inter alia in the EU Charter and the ECHR. This paper also argues that regulatory standards regarding AI should be clearer and stronger as well as suggests a new wording of some standards. The particular new rights and/or their new wording will be suggested in the paper.

Keywords Artificial Intelligence (AI) · Artificial Intelligence systems (AIS) · Rule of Law · Democratic values · Fundamental human rights · European public legal order · European digital legal order

1 Introduction

In March 2023, the Italian Data Protection Authority (*Garante per la protezione dei dati personali*) suspended the

'triumphal procession' of ChatGPT, the first such attempt among the EU countries, on the ground that this OpenAI tool did not meet the requirements for lawful personal data collection and that there was no proper age verification system in place for children.[1] Less than a month later, ChatGPT was unblocked in Italy, but this episode once again stirred up the debate about the proportionality of bans and potentially disruptive innovations, as well as the effectiveness and possible mis- or over-regulation of AI.

Recently, the concept of the 'European digital legal order' seems to have gained more importance than the overarching concept of European legal order, of which the former is arguably a modern manifestation. The European legal order traditionally entails a set of fundamental human rights, Rule of Law principles and Democratic values as enshrined in the UN Charter,[2] the Council of Europe Statute,[3] the Euro-

[1] *Intelligenza artificiale* [27]*: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori*. 31.3.2023. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847.

[2] Articles 1 and 2, the Charter of the United Nations (1945) https://www.un.org/en/about-us/un-charter; see also Declaration of the HighLevel Meeting of the General Assembly on the Rule of Law at the National and International Levels: resolution A-RES-67-EN https://digitallibrary.un.org/record/738646.

[3] Article 3, Statute of the Council of Europe (1949) https://rm.coe.int/1680935bd0; see also European democracies and democratic societies in Resolution Res(2002)12 establishing the European Commission for the Efficiency of Justice (CEPEJ).

pean Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR),[4] as well as the EU Treaties[5] and the Charter of Fundamental Rights of the European Union (EU Charter).[6] From maintaining the Rule of Law derive the sustainability of Democratic values, and freedoms under the law enshrined in fundamental human rights.[7] To the extent that the European digital legal order is the manifestation of the European legal order in the modern digital world, the fundamental question of the nature, scope and upholding of fundamental human rights, Rule of Law principles and Democratic values remains. Without disputing the need for digital transformation and its proper regulation, this paper will turn its attention to the current status of fundamental principles in the modern setting of democratic societies. This will include a review in the digital legal order of fundamental human rights as enshrined in the ECHR and interpreted by the European Court of Human Rights (ECtHR) and, at the same time, as may be developed in the EU Treaties, the EU Charter and the Court of Justice of the European Union's case law, in the framework of Rule of Law principles and the values of European democracy as enshrined in Article 2 TEU.[8] It is important to emphasise the convergence of the two European fundamental human rights instruments that represent the ECHR and the EU Charter as, jointly and severally, they constitute the foundations of the European legal order as far as fundamental human rights are concerned. Across their jurisprudence, both European courts interpreting and preserving fundamental human rights in Europe have used similar and/or complementary mechanisms upholding fundamental human rights in Europe, providing prima facie equivalent protection to rights,[9] whereas these very same rights are most likely to be affected by AI in a modern setting.[10] The strengthening of the mutual cooperation of the Court of Justice of the European Union (CJEU) and of the Euro-

[4]European Convention on Human Rights https://www.echr.coe.int/documents/d/echr/Convention_ENG [16].

[5]Articles 2, 6 and 7 Treaty on the European Union (TEU) [11].

[6]Charter of Fundamental Rights of the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT. For a detailed account of the European public legal order, see S. Laulhé Shaelou [43], 'Market Freedoms, EU fundamental rights and public order: views from Cyprus', (2011) 30(1) Yearbook of European Law 298, fn 4.

[7]See e.g. Sir Alfred Denning [14] (later known as Lord Denning MR, Master of the Rolls from 1964 until 1982), Freedom under the law (Stevens & Sons Ltd: London, 1949), 3 & 96) https://socialsciences.exeter.ac.uk/media/universityofexeter/schoolofhumanitiesandsocialsciences/law/pdfs/Freedom_Under_the_Law_1; see also Democracy, the 'constant relationship between the rulers and people' (Winston Churchill MP, Leader of the Opposition, Hansard, House of Commons Debates, 11.11.1947, Column 205, https://api.parliament.uk/historic-hansard/commons/1947/nov/11/parliament-bill.

[8]See Consolidated Version of the Treaty on European Union [2008] OJ C115/13 [11], art 2: "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are3 common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail".

[9]For a discussion of the principle of equivalent protection under the ECHR and EU law including the EU Charter, see Laulhé Shaelou S. [41], The EU and Cyprus: principles and strategies of full integration, Studies in EU External Relations (SEUR 3, Brill/Martinus Nijhoff Publishers, 2010) 201-208.

[10]See on algorithmic scoring Opinion, SCHUFA Holding and Others (Scoring) [47], Case C-634/21, ECLI:EU:C:2023:220.

pean Court of Human Rights (ECtHR) could only reinforce the protection afforded to fundamental human rights in AI cases.

While there is no uniform definition of Artificial Intelligence (AI) or Artificial Intelligence Systems (AIS) in the European legal order at large – several attempts have been made to provide 'all-encompassing but changeresistant' definitions[11] – AIS's serious impact on fundamental human rights is not doubtful anymore. For this reason, the European Declaration on Digital Rights and Principles for the Digital Decade[12] proposes an anthropocentric interaction with such systems. As will be discussed in this paper, being human-centred in the field of AI and AIS can become more and more difficult, as we move along the path of digitalisation and algorithmisation.

Taking this into account, this paper reviews the regulatory framework of AI and proposes potential new/renewed/modernised rights that should enhance and/or supplement the current catalogue of fundamental human rights, as contained *inter alia* in the EU Charter and the ECHR. This paper also argues that regulatory standards, especially in relation to AI, should be clearer and not be based on a half-hearted approach or on a "muddling through".[13] Some wordings of rights and standards will be suggested in this paper.

2 Technological determinism and the legal order

In the EU, incredibly detailed, cumbersome and extraterritorial regulations in the last decade are designed to strengthen the foundation of the European legal order so that it can withstand the challenges of the digital age. The core framework of this approach is already formed by the General Data Protection Regulation (GDPR)[14] and, more recently, by the Digital Markets Act (DMA)[15] and the Digital Services Act (DSA).[16] It remains to be seen whether and, if so, how this framework will be supplemented by

[11] See Report from the Commission to the European Parliament [60], the Council and the European Economic and Social Committee [59] (Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics) (COM/2020/64 final); 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 [51] (COM/2021/206 final); Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence [50] (AI Liability Directive) (COM/2022/496 final).

[12] See European Declaration on Digital Rights and Principles for the Digital Decade [21] (2023/C 23/01).

[13] See e.g. Peter Hennessy [26], Muddling Through: Power, Politics and the Quality of Government in Postwar Britain (London: Victor Gollancz, 1996).

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.4.2016 [56] 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).

[15] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14.9.2022 [57] on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[16] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19.10.2022 [58] on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

the widely discussed proposal for an Artificial Intelligence Act (AIA).[17] With these regulatory tools, the EU and its Member States are trying to achieve the goal of developing and implementing legislation that is thoughtful, effective and progressive, while respecting fundamental human rights and the well-being of societies. These acts represent an overall compromise. First of all, it is a compromise between the requirements of legal principles and norms and the freedom to innovate. On the one hand any proper regulation should be aimed at protecting fundamental human rights and consistent with legal certainty. On the other hand, it should not multiply gaps and contradictions in which technologies are allowed to proliferate uncontrolled and could significantly impinge on human rights, fundamental freedoms and legitimate interests. In addition, the final versions of these acts seem to be a compromise not only between the European Parliament, the Council and the European Commission, but also between legislators representing the interests of states and their citizens vis-à-vis businesses representing the industry. Technologies pushed by business with the help inter alia of lobbying[18] and innovation may be an almost invisible component in this trade-off, spurring action and contributing to some of the regulation becoming obsolete before it even goes out to print. This is especially indicative of the legal framework regarding AI. While fierce discussions have been going on about whether a model based on assigning various levels of risk to AIS is good enough and whether it is right to have technological details in annexes to the act, fresh problems surface, including technologies based on large linguistic models, bringing us closer to generative AI. The development of AI systems probably also brings us closer to turning to technological determinism in its, if not hard, then at least soft version.

Technological determinism claims that technology determines the development of society, and in some extreme manifestations, this concept considers technology as an independent agent. In general, this term refers to the belief that technology is 'a key governing force in society'.[19] This kind of determinism includes, among other things, the notion that people can – only – adapt to the development of technology,

[17] Proposal for a regulation of the European Parliament and of the Council [3] laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final).

[18] See Atikcan, E. Ö., Chalmers, A. W. [5], 'Choosing lobbying sides: the General Data Protection Regulation of the European Union' (2019) Journal of Public Policy 39 (4), 543–564. https://doi.org/10.1017/S0143814X18000223; Christou, G., Rashid, I. [10], 'Interest group lobbying in the European Union: privacy, data protection and the right to be forgotten' (2021) Comparative European Politics 19, 380–400. https://doi.org/10.1057/s41295-021-00238-5; The lobby network: Big Tech's web of influence in the EU. Report. Corporate Europe Observatory and LobbyControl e.V. Brussels and Cologne, August 2021 [68]. https://www.politico.eu/wp-content/uploads/2021/08/30/BigTech-Firepower-study-Final.pdf; The lobbying Ghost in the Machine. Big Tech's covert defanging of Europe's AI Act. Report. Corporate Europe Observatory. February 2023, Brussels [69]. https://corporateeurope.org/sites/default/files/2023-03/The%20Lobbying%20Ghost%20in%20the%20Machine.pdf.

[19] Smith, M. [64], Technological Determinism in American Culture. In Smith, M., Marx, L. (eds.), Does Technology Drive History? The Dilemma Of Technological Determinism (MIT Press. Cambridge, Mass, 1994) 2.

which has its own internal logic.[20] This is also a view that can be valuable when we consider social-shaping tendencies of technology.[21]

Besides, technological determinism draws attention to the impact of technology at both the macro and micro levels and suggests that cautions about over-determination be taken seriously. One of the reasons for this is 'the fact that many modern technological artefacts and systems are so complicated that no single person, or group of persons, has an overall grasp of them or knows the design in full, which means that the risk of unforeseen consequences of technology increases'.[22] In the light of the addition of a digital dimension to almost all human activity, and as a result arguably also to human rights, and of the widespread deployment of increasingly sophisticated algorithms, this may be an especially useful approach.

For the purposes of this paper, we propose to consider technological determinism as a trend in which technology largely determines modern society in general and the European legal order in particular. We argue that technologies have already begun to shape the European legal order at large, towards a renewed digital legal order.[23] As such, breakthrough technologies of AIS may shift the fundamental pillars of this order, if not alienate them altogether, unless these technologies are integrated 'by design', i.e. at the conception phase and in their subsequent use/refinement/upgrades. Targeted yet all-encompassing influence, profiling and manipulation with the assistance of AI can undermine democracy. Decision-making, when based on algorithmic recommendations, on lack of clarity and on the erosion of the public debate can be detrimental to the Rule of Law and democratic values. But perhaps the most immediate and visibly devastating effect of AI is for fundamental human rights.[24]

[20] Jandric, P. [28], 'Postdigital human capital. International Journal of Educational Research' (2023) 119 https://doi.org/10.1016/j.ijer.2023.102182.

[21] Dafoe, A. [12], 'On Technological Determinism: A Typology, Scope Conditions, and a Mechanism. Science, Technology, & Human Values (2015) 40(6), 1047–1076. https://doi.org/10.1177/0162243915579283. See also Stahl B. [65], Artificial Intelligence for a better future: An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies (2021, Springer); Stahl B. et. al. [66], 'Artificial intelligence for human flourishing – Beyond principles for machine learning, Journal of Business Research 124, 374-388 (2021). https://doi.org/10.1016/j.jbusres.2020.11.030.

[22] Hallström, J. [25], 'Embodying the past, designing the future: technological determinism reconsidered in technology education' (2022) International Journal of Technology and Design Education 32, 17–31, 22.

[23] The lead author in this paper has co-argued this in public consultations/Feedback to the European Commission on AI – ethical and legal requirements [22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legalrequirements/F2665299_en (August 2021); in Questionnaire and Position Paper for the European Commission, Declaration of Digital Principles – the 'European way' for the digital society https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13017Declaration-of-Digital-Principles-the-%E2%80%98European-way%E2%80%99-for-the-digital-society_en (August 2021); and in Questionnaire, feedback and position paper for the European Commission, Civil liability – adapting liability rules to the digital age and artificial intelligence https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rulesto-the-digital-age-and-artificial-intelligence/public-consultation_en (January 2022).

[24] See Andreou A., Laulhé Shaelou S., Schroeder D. [4], Current Human Rights Frameworks (Sherpa project of Smart Information Systems, Horizon 2020, 2019) https://doi.org/10.21253/DMU.8181827. See also Rodriges R., Panagiotopoulos A., Lundgren B., Laulhé Shaelou S. [61, 62], Grant A., Regulatory options for AI and big data (Sherpa project of Smart Information Systems, Horizon 2020, 2020) https://doi.org/10.21253/DMU.11618211.

3 AI impact on fundamental human rights

The impact AI has on fundamental human rights can be seen primarily along two lines. Firstly, how AI affects fundamental human rights may affect the ideal of human rights in general through the erosion of value bases and the recourse to technological determinism and a more utilitarian approach to regulation and practice. Secondly, AIS can attack individual rights in overt and covert manners as will be shown in this paper. Such attacks may affect primarily, but not only, rights enshrined in the EU Charter and the ECHR, such as the rights to respect for private and family life,[25] to protection of personal data,[26] to freedom of expression and information,[27] to freedom of thought, to conscience and religion,[28] to rights of liberty and security,[29] to the right to a fair

[25]Charter of Fundamental Rights of the European Union [9] (18.12.2000), 2010 O.J. C 83/02, entered into force 1.12.2009, Article 7; European Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 4.11.1950), 312 E.T.S. 5, as amended by Protocol No. 3, E.T.S. 45; Protocol No. 5, E.T.S. 55; Protocol No. 8, E.T.S. 118; and Protocol No. 11, E.T.S. 155; entered into force 3.9.1953 (Protocol No. 3 on 21.9.1970, Protocol No. 5 on 20.12.1971, Protocol No. 8 on 1.1.1990, Protocol 11 on 11 Jan 1998)., Article 8. In the case of Privacy International CJEU decided that national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society (See Judgment of the Court (Grand Chamber) [35] of 6.10.2020, Privacy International, Case C-623/17, ECLI:EU:C:2020:790). AIS make it possible to be more intrusive in privacy formally not crossing the line of legal prohibihion. It stems from the AIS abilities to connect and puzzle a peices of data.

[26]EU Charter, Article 8. In the case of Meta Platforms and Others on 4.7.2023 CJEU considered the issue of the business model of the platform, which provides for the collection of data from other services of the group and third-party websites and applications through integrated interfaces, as well as the conditions under which this contradicts the requirements of the GDPR (See Judgment of the Court (Grand Chamber) [32] on 4.7.2023, Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social), Case C-252/21, ECLI:EU:C:2023:537). With AI tools both collecting and processing personal data has already gone far beyond concrete platform as well as applications and websites affiliated with this platform.

[27]EU Charter, Article 11; ECHR, Article 10. In the case of Høiness v. Norway ECtHR [19] balanced privacy with freedom of expression in online context. The Court did not find the violation of Ms Mona Høiness right to privacy and reputation despite the fact that some anonymous comments about her were inappropriate. In regard to fair balance the ECtHR also referred to the measures adopted by Internet portal which had an established system of removal of the offensive comments and moderators who monitored content (See Høiness v. Norway, 43624/14, [2019] ECHR 221). With AIS the systems of content moderation are going to be fully or almost fully-automated. Not having human in the loop may change the balance between rights.

[28]EU Charter, Article 10; ECHR, Article 9. For example, in the case of Taganrog LRO and Others v. Russia [20] on 7.6.2022, the Russian Federation had taken various actions against Jehovah's Witnesses religious organisations including banning of their religious literature and international website and misusing "extremism" for prosecution (See Taganrog LRO and Others v. Russia, 32401/10, [2022] ECHR 419). With AIS instruments it is much easier to prosecute believers in their online activity and wide spreading information by them.

[29]EU Charter, Article 6; ECHR, Article 5. In the case of La Quadrature du Net and Others [34] CJEU outlined some limits of the right of liberty and security (See Judgment of the Court (Grand Chamber) of 6.10.2020, La Quadrature du Net and Others, Joined Cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791). AIS could rise a question of these limits again including about a balance between privacy and security.

trial,[30] to the right to non-discrimination,[31] to equality of men and women,[32] to rights of the child[33] and/or to the principle of no punishment without law.[34] These must also be seen in the global socio-political context of external factors, crisis situations and shocks involving the use of AI.[35] A particular feature of the impact of AIS on human rights is what could be referred to as cross-cutting impact where not one, but a number of rights can be affected by the deployment of a particular technology. For example, content moderation algorithms may affect not only freedom of expression, but also freedom of thought, conscience and religion, the right to non-discrimination, equality of men and women, and the rights of the child, since these algorithms in

[30]EU Charter, Article 47; ECHR, Article 6. The right to a fair trial includes to guarantee access to courts that are able to verify all grounds and evidence on the basis of which decisions are made. Besides, in the case of ZZ v Secretary of State for the Home Department CJEU reminded that the parties to a case must have the right to examine all the documents or observations submitted to the court for the purpose of influencing its decision, and to comment on them. The Court also ruled that, in case of state security resons, a competent national authority must be entrusted to verify and be able to carry out an independent examination whether those reasons stand in the way of precise and full disclosure of the grounds on which the decision in question is based and of the related evidence (See Judgment of the Court (Grand Chamber) [33] of 4.6.2013, ZZ v Secretary of State for the Home Department, ECLI:EU:C:2013:363). Using AIS in courts for supporting decisionmaking may lead to erosion of fair trial as it could be impossible to examine AI decisions.

[31]EU Charter, Article 21; ECHR, Article 14. In the case of Ligue des droits humains [30] CJEU agreed with Advocate General in point that, given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a program arrived at a positive match using some 'pre-determined' criteria (Judgment of the Court (Grand Chamber) of 21.6.2022, Ligue des droits humains v Conseil des ministres, Case C-817/19, ECLI:EU:C:2022:491). It may also lead to problem to challenge the nondiscriminatory nature of the results obtained by AI.

[32]EU Charter, Article 23. In the case of K and Others v Tesco Stores Ltd [36] the CJEU confirmed the inadmissibility of violating the principle of equal pay for male and female workers for 'work of equal value', as well the fact that Tesco Stores appears to constitute, in its capacity as employer, a single source to which the pay conditions of the workers performing their work in its stores and distribution centres may be attributed and which could be responsible for any discrimination (Judgment of the Court (Second Chamber) of 3 June 2021, K and Others v Tesco Stores Ltd, ECLI:EU:C:2021:429). AI instruments make it possible to create such settings under which it is possible to filter out women when hiring or to create such a system under which discrimination will be more difficult to prove than in the given case. Moreover, AIS could repeat creator's prejudices and teach themselves not to hire women based on past discriminatory practice.

[33]EU Charter, Article 24. In the case of Belgian State (Retour du parent d'un mineur) [37] CJEU emphasized the duty to consider the best interests of the child, which covers all decisions and actions that directly or indirectly affect children as well as all actions relating to children, whether taken by public authorities or private institutions (See Judgment of the Court (Tenth Chamber) of 11.3.2021, M. A. v État belge, Case C-112/20, ECLI:EU:C:2021:197). AI-based learning apps which could directly affect children and form addictions may not meet the requirement to have the child's best interests as a primary consideration.

[34]ECHR, Article 7. The to the principle of no punishment without law includes the principle that only the law can define a crime and prescribe a penalty (See Kokkinakis v. Greece [17], [1993] ECHR 20). Here we need to stress that predictive AIS and those which make an assessment of people to define what preventive measure should the court assign to them, what degree of public danger do those charged with criminal responsibility have, etc., shold not be legitimate parts of criminal justice.

[35]See Andreou A., S. Laulhé Shaelou S., D. Schroeder D. [4], Current Human Rights Frameworks (Sherpa project of Smart Information Systems, Horizon 2020, 2019) 41-42 https://figshare.dmu.ac.uk/articles/online_resource/D1_5_Current_Human_Rights_Frameworks/8181827; see also https://www.projectsherpa.eu/smart-information-systems-and-democracy-freedom-of-thought-control-and-manipulation-2/ on the pros and cons of smart information systems on Democracy.

their design and/or use may be invasive, selective, promote polarisation of opinions and dilute discussions, as well as generally contribute to the formation of a certain picture of the world among users of digital content. Therefore, when describing the impact of AIS on fundamental human rights, it is not always possible to single out specific rights that are affected by these technologies. Thus, the question arises as to how to best prepare and protect them.

The ability of AIS to track users both in the public and the private sphere of life is outstanding. That is so particularly because it is not necessary to use technological artefacts directly to be the object of certain tracking actions. Bits of information put into the digital space by others can make it easier for non-users to track them because AI can search, process, combine and analyse those bits with astonishing accuracy, as well as keep track of what people have been interested in and weave it into their online searches, intrusively or more subtly.[36] For example, algorithms can establish a match on a photo with a person who did not take or post this photo on the network and may even not have known that it was taken, then determine the location of this person at a certain time.

AI technologies used in public spaces by public authorities can go far beyond what is considered acceptable in a democratic society upholding Rule of Law principles and European values as well as fundamental human rights.[37] Given the 'progressive datafication of reality', the introduction of AI-based surveillance systems puts the public at an increased risk of power imbalances, whereby public authorities have excessive access to privileged information on individuals' private lives.[38] When it comes to biometric data the intrusion into one's private life could be even more seriously invasive. AI may track or process personal biometric data including micro expressions, tone of voice, heart rate or temperature data. This opens the field not only for an overly accurate picture of how a particular person breathes, moves and lives, but also for planning a very targeted impact on this person if this data is used beyond the goals declared by public authorities.

By the same token private actors can impact people extremely successfully. For example, fitness bracelets or rings that track heart rate and body temperature advertised by companies provide them with extremely sensitive and intimate information. Such information then processed by AI can serve to influence or impose something on specific people using their personal vulnerabilities. Children may be particularly at risk because their cognitive and socio-emotional skills manifest rapid growth and they lack fully mature abilities.[39] AIS makes it possible to get close to children and influence them even if they do not use social networks but only educational applications.

[36] Razmetaeva, Y. [53], 'Opinions and Algorithms: Trust, Neutrality and Legitimacy' (2022) Filosofiya prava i zahal′na teoriya prava, 1, 86. See also https://www.project-sherpa.eu/sis-and-privacy-and-data-protection/ and https://www.project-sherpa.eu/how-social-media-data-isused-to-predict-risk/.

[37] For example, using AIS for automatic decision-making which do not sufficiently take into account individual circumstances and rare cases may be incompatible with the rights of persons belonging to minorities.

[38] Fontes, C. et al. [23], 'AI-powered public surveillance systems: why we (might) need them and how we want them' (2022) Technology in Society 71. https://doi.org/10.1016/j.techsoc.2022.102137.

[39] Charisi, V. et al. [8], 'Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy' EUR 31048 EN, Publications Office of the European Union (2022), 24.

AIS can easily rank information by choosing what people should see when using search or turning to daily news in the media, visiting websites or simply scrolling through social media feeds. Given that a giant number of people today are looking for information provided in digital form and not in print, this opens the door for manipulation by those players who dominate the digital space, especially big tech companies. At the same time, companies do not miss opportunities to present themselves as a neutral side and as those who only provide access to content – as facilitators. For example, Google presented itself as a mere 'transmitter of popular preference', as processed through its algorithms with no obligation to adhere to social values when a Holocaust denial site appeared on the top ten of search results for the query 'Jew'. Then Google claimed that an anti-Semitic site could rise to the top search results based on certain algorithms.[40]

Big tech companies claim a degree of power that approaches the public one and actually become actors in the public sector. At the same time, they try to avoid/minimise public responsibility – the kind of responsibility that high courts or government agencies bear as actors in the public sector and public power bearers – and even that kind of responsibility that traditional media bear, named editorial responsibility. Such a lack of responsibility as well as accountability coupled with serious powers is one point of concern especially when things are moving slowly in terms of regulation. The potential intrusion AIS, with the help of companies that develop and maintain them, may be even more threatening than power over data which was discussed in early GDPR times. The reasons for this concern may be the ability of algorithms to manipulate public opinion relatively easily, their predictive power and seemingly depersonalised character which influence the responsibility issues.[41]

Undoubtedly, there is some positive movement in matters of responsibility and accountability of AI owners and/or developers. On 24 May 2023, the General Court of the EU issued a judgment in which it dismissed the appeals of Meta Platforms in cases T- 451/20 *Meta Platforms Ireland v. Commission* and T- 452/20 *Meta Platforms Ireland v. Commission* establishing that the contested decision did meet objectives of general interest recognised by the European Union.[42] Meta Platforms Ireland Ltd tried to challenge the request to provide documents to be identified by search terms because the European Commission sent a request for information to Meta Platforms Ireland Ltd based on suspicions of anticompetitive behaviour in its use of data and in the management of its social network platform. However, the Court did not find that the disputed request went beyond what was necessary. Also, the Court did not find that establishing a virtual data room failed to ensure that sensitive personal data was sufficiently protected. On the other hand, the European Commission had found Google in abuse of dominant position in national markets and imposed a penalty of

[40] Pasquale, F. [49], 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power' (2016) Theoretical Inquiries in Law 17, 487–513, 495.

[41] See Razmetaeva, Yu. [52], 'Algorithms in The Courts: Is There any Room For a Rule of Law' (2022) Access to Justice in Eastern Europe 4 (16) https://doi.org/10.33327/AJEE-18-5.4-a000429.

[42] See Judgment [38] of 24.5.2023, Meta Platforms Ireland v Commission, Case T-451/20, ECLI:EU:T:2023:276, Case T-452/20, ECLI:EU:T:2023:277.

€2.42 billion on Google for its use of algorithms reducing the ranking of competing services in search results, while Google's own services had a prominent position.[43]

As such, the regulation of companies that use AI to manipulate information widely requires strategic decisions like those made for 'very large' digital platforms. In fact, there should be clear and even strict standards that apply both to any company that owns AI (since AI tools can elevate even the smallest and most inconspicuous company to the top of power) and to those companies that, owning platforms and search engines, have a significant impact on societies. At the moment, the standards that apply to very large digital platforms are formulated as half-hearted or muddled through. In particular, the DSA imposes additional obligations on providers of very large online platforms and search engines, applying the logic that these platforms and search engines must bear obligations that are proportionate to their societal impact. Yet, the concept of active recipients of the service as 'all the recipients actually engaging with the service at least once in a given period of time' – that does not necessarily coincide with those of a registered user of a service [44] – is rather weak to assess the power and influence of such platforms. Besides, the question arises as to how the unique recipients of the service will be determined when the DSA does not require providers to perform specific tracking of individuals online but does not prohibit it simultaneously.

On the other hand, big tech companies on their online platforms are utilising AI to identify and remove content that breaches their terms of service. However, that means that legitimate content may be flagged or removed.[45] Cases where legitimate content has been removed include examples of well-known paintings that contain nudity, photographs, and other significant evidence of historical events. These cases also illustrate a deeper problem than the AI bug and the subsequent bug of human content moderators controlling takedowns. It seems that the deeper problem here is the governance of human rights issues by companies through corporate policies rather than based on rights-based provisions enshrined in European and national laws.

The increasing interaction with AIS may aggravate the lack of control which should remain in the hands of people over their lives. However, the more data about people it becomes possible to receive and process, the less this control remains. As a result, and as rightly noted: 'The vast amounts of sensitive data required in algorithmic profiling and predictions, central to recommender systems, pose multiple issues regarding individuals' informational privacy'.[46] Algorithmic predictions not only narrow the scope of some human rights, but also undermine justice when they become part of a judicial process, or democracy and openness when they seem to make public discussion about public decisions unnecessary. Pre-emptive power of AIS makes possible both: narrowly targeted and very precise intrusions into the sphere of life of a specific person protected by human rights, as well as the governing

[43] Judgment of the General Court [39] of 10.11.2021, Google and Alphabet v Commission, Case T-612/17, ECLI:EU:T:2021:763.

[44] Regulation (EU) 2022/2065 of the European Parliament and of the Council [58] of 19.10.2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), para 77.

[45] Ad hoc Committee [2] on Artificial Intelligence (CAHAI), Feasibility Study (2020), 9.

[46] Tsamados, A., Aggarwal, N., Cowls, J. et al. [71], 'The ethics of algorithms: key problems and solutions' (2022) AI & Society: Knowledge, Culture and Communication 37, 215–230, 223.

of people who were algorithmically sorted into groups based on certain characteristics of these people. Profiling, for instance, sorts of people in the way 'in which mechanisms that generate demarcations become increasingly opaque and incomprehensible for those who are objects of profiling'.[47] AIS consider characteristics people have or probably have and use them for imposing goods, services or opinions, as well as for nudging humans to certain actions or decisions. For example, during the COVID 19 pandemic, both digital and analogue nudges were actively used by many governments to effectively influence people's behaviour, especially regarding maintaining physical distance, wearing medical masks, and performing certain hygiene procedures. This stimulated a discussion about the necessity and ethics of nudging in times of crisis.[48]

The ways AI developers use data or particular datasets themselves can lead to unequal treatment of the human being. If 'structural differences' exist for protected attributes such as gender, ethnic origin or political opinion, the AI through its output can discriminate against certain groups or individuals. Examples include a hiring algorithm favouring men over women, an online chatbot becoming racist after a few hours of use, and face recognition systems working better for white people in comparison to people of colour.[49] When it comes to machine learning, 'performance criteria such as reliability, efficiency, and accuracy, addressing bias should be an integral part of any machine learning application'.[50] However, eliminating bias is not as easy as technical experts and managers at AI development companies often declare it to be. There is 'an implicit assumption that once we collect enough data, bias will no longer be a problem—an assumption that in general is not justified'.[51] Biases might be a deep problem because they can reflect not only poor approach to data used for AI but also entrenched social practices or reproduce practices that societies tend to move away from.

[47] Weiskopf, R. [75], 'Algorithmic Decision-Making, Spectrogenic Profiling, and Hyper-Facticity in the Age of Post-Truth' (2020) Le foucaldien 6 (1), 1–37, 23.

[48] See Krawiec, J.M., Piaskowska, O.M., Piesiewicz, P.F. et al. [40], 'Tools for public health policy: nudges and boosts as active support of the law in special situations such as the COVID-19 pandemic' (2021) Global Health 17, 132. https://doi.org/10.1186/s12992-021-00782-5; Vilhelmsson, A., Sant'Anna, A., Wolf, A. [74], 'Nudging healthcare professionals to improve treatment of COVID-19: a narrative review' (2021) BMJ Open Quality, 10:e001522 https://doi.org/10.1136/bmjoq-2021-001522; Sasaki, S., Saito, T., Ohtake, F. [63], 'Nudges for COVID-19 voluntary vaccination: How to explain peer information?' (2022) Social Science & Medicine, 292 https://doi.org/10.1016/j.socscimed.2021.114561), as well as direct criticism in Dodsworth, L. [15], A State of Fear: How the UK Government Weaponised Fear During the Covid-19 Pandemic (London: Pinter & Martin, 2021).

[49] 'Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights' [13] (EU Agency for Fundamental Rights (FRA). Luxembourg: Publications Office of the European Union, 2019) 8, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-dataquality-and-ai_en.pdf.

[50] van Giffen, B. et al. [73], 'Overcoming the pitfalls and perils of algorithms: A classification of machine learning biases and mitigation methods'(2022) Journal of Business Research 144, 93–106, 105.

[51] Olhede, S.C., Wolfe, P.J. [46], 'The growing ubiquity of algorithms in society: implications, impacts and innovations' (2018) Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences A376: 20170364. https://doi.org/10.1098/rsta.2017.0364. Biased data (when biased datasets are results of historical discrimination in some domains or lack of diversity) as well as biased people (when algorithms have been designed specifically to create discriminatory outcomes).

Biased data (when biased datasets are results of historical discrimination in some domains or lack of diversity) as well as biased people (when algorithms have been designed specifically to create discriminatory outcomes)[52] lead to massive violations of the right to non-discrimination. It may include differential treatment based on protected characteristics, such as discrimination and bias-motivated crimes, differentiation, statistical bias and offset from origin. [53] As AI is deployed in all areas and increasingly used to automate decision-making processes, inequality

– as the contrary of 'equality before the law'[54] – could affect large numbers, and disproportionately affect vulnerable groups and marginalised communities, etched into a more technologically advanced future society.

The European Union has stressed the importance for 'European AI [to be] grounded in our values and fundamental rights such as human dignity and privacy protection'.[55] To achieve this goal, it is necessary to have a vision of the future with AIS that is inclusive of all stakeholders and scenarios, but clearly adheres to the European values of fundamental human rights and democracy at the core of Rule of Law principles.[56]

4 Vision of the future with AI

The threats posed by AIS to human rights do not – and cannot – mean we need to abandon AI altogether.[57] Overall, it can create efficiency benefits that businesses can use to optimise their production, increase production quality, minimise production stoppages, optimise transportation logistics and reduce maintenance, provide a safer and more effective training and guidance through the use of augmented reality, reduce human error,[58] etc. At the same time, it is necessary to consider that we are not discussing some hypothetical distant future, but we consider the future knowing that AI already occupies a significant part of the current life of people and societies.

4.1 The dependence on AIS

The dependence of the public sector on private actors who create, modify, adjust and maintain algorithms could be one of the scenarios that may have adverse conse-

[52] Stinson, C. [67], 'Algorithms are not neutral' (2022) AI Ethics 2, 763–770, 764.

[53] 'Bias in algorithms - Artificial intelligence and discrimination. Report' [6] (EU Agency for Fundamental Rights (FRA). Luxembourg: Publications Office of the European Union, 2022), 23.

[54] See The Venice Commission. Report [70] on the rule of law. CDL-AD(2011)003rev-e. Adopted by the Venice Commission at its 86th plenary session (Venice, 25-26.3.2011). https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2011)003rev-e; see also Bingham, T. [7] The Rule of Law (Penguin Books, 2011).

[55] 'White Paper on Artificial Intelligence – A European Approach to Excellence and Trust' [76] COM(2020) 65 final, 2.

[56] Laulhe Shaelou, S., Alexandrou, C. [42], An overview of the EU's Artificial Intelligence Regulation https://www.project-sherpa.eu/anoverview-of-the-eus-artificial-intelligence-regulation/; see also https://www.project-sherpa.eu/european-agency-for-ai/.

[57] See contra https://futureoflife.org/open-letter/pause-giant-ai-experiments/.

[58] Opportunities of Artificial Intelligence (European Parliament, 2020), 36., [48] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf.

quences for the Pillars of democratic societies, fundamental human rights, the Rule of Law and democratic values in Europe. For example, AI owners may legally refuse to disclose source codes, thereby depriving users, including government organisations and institutions that may face emergency situations, from the opportunity to check potential discriminative vulnerabilities of the algorithmic tool, investigate security threats as well as technical errors.

Such dependence may be exacerbated by the monopoly position of some AI developers. This monopoly includes large online platforms which 'operate at an unprecedented scale', and 'have a[n ever growing] market value of over $400 billion'.[59] Additionally, these giant companies often acquire smaller companies or startups, effectively eliminating competition and cementing their monopoly. The monopoly position of big tech companies allows them to dictate terms to both governments and users, which means more and more people, since AI affects not only direct users, but also people whose information enter the digital space without their direct participation (indirect users). Moreover, in the future, the impact of AI will affect those whose information do not enter the digital space, making these people or groups invisible and contributing to their digital exclusion from society.

4.2 The effective regulation of AIS

Any vision for AI must include proper and effective regulation, which is an extremely difficult task given the rapidity and unpredictability of the development of these technologies. On the one hand, overdetailed regulation may lead to the limitation of innovation by the technology companies, while making it even more difficult for lawmakers to update a certain set of regulations, following technological advancement. On the other hand, broader regulation might create loopholes that companies will use to act for profit rather than human rights-based approaches where possible. Whether we accept or reject technological determinism, it is clear that AI is an area where legislators, especially in democratic societies, inevitably lag behind.

Many hopes are placed on the transparency of AIS, a requirement well documented at the regional and national level, urging for the explain ability of decisions made by AI.[60] Beyond the Rule of Law principle of transparency and in more practical terms, transparency has been described in many ways. Some claim AI should be open to inspection and evaluation; others that the core idea is reliability; while others that transparency means to report unexpected behaviour. However, most frequently, transparency is about making the 'decision-making processes accessible to users, so that they can understand and judge how an autonomous system has reached a certain decision.'[61] The principle of transparency seems to be too fundamental to be applicable without the interpretation and guidance from courts, International Organisations and civil society rather than in the hands of companies and other AI developers.

[59] 'Regulating in a Digital World' [55] (House of Lords, Selection Committee on Communications 2019), Para 121.

[60] Ad hoc Committee on Artificial Intelligence (CAHAI). [2] Feasibility Study (2020), 33, 34.

[61] Trust and Transparency in Artificial Intelligence [1] (Human Brains Project, 2021), 17 http://doi.org/10.5281/zenodo.4588648. 64 Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries. [54] https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14.

Further deployment and use of AI will exacerbate the issue of responsibility for its actions and decisions, or – since AI has not yet reached such a level of development to be completely independent and self-governing – for those types of actions and decisions in taking and implementing which people significantly rely on AIS. The responsibility and role of internet intermediaries has been highlighted in various documents. In particular, the Committee of Ministers of the Council of Europe has observed that states should ensure that fundamental human rights are upheld through the use of such intermediaries. At the EU level, AI deemed as 'high risk' under the proposed AIA, may be held at a higher standard of liability. Conversely, AI not labelled as high risk, should follow suit with 'consumer AI', and be governed by the existing legal framework. Current EU legislation moves along the path to be adequate to accommodate modern challenges. In particular, a new version of the Product Liability Directive should contain clear liability rules for certain products such as software including AIS and digital services.[62]

In this sense, it is encouraging that on 14 June 2023 the European Parliament voted to adopt its position for the upcoming AIA proposing stricter rules following a risk-based approach.[63] Amendment 27 deserves special attention because it clearly states that AIS 'should make best efforts to respect general principles establishing a high-level framework that promotes a coherent human-centric approach to ethical and trustworthy AI in line with the EU Charter and the values on which the Union is founded'.[64]

4.3 The 'new' fundamental rights

A vision of the future with AIS could open the possibility to create new rights and/or (significantly) change/upgrade the essence and scope of already existing rights. Introducing new rights may also mean changing their status from rights that apply to certain categories of persons (such as user rights or data subject rights) to fundamental human rights that are of utmost importance to all human beings.

Among such (re-)new(ed) rights could be the 'right not to be subjected to automatic decision-making and automatic processing' in the broadest sense. The beginning of this right is laid down by the GDPR in Article 22 (Automated individual decision-making, including profiling).[65] This appears to only have effect on 'serious impactful events', without further explanation of what this could entail.[66] While not

[62] New Product Liability Directive. Overview. [45] Briefing EU Legislation in Progress (May 2023) https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf.

[63] MEPs ready to negotiate first-ever rules for safe and transparent AI [44] (Press Releases, 14.6.2023) https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparentai.

[64] Amendments adopted by the European Parliament on 14.6.2023 [3] 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.

[65] GDPR, Article 22.

[66] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 [24] (Data Protection Working Party, Adopted 3.10.2017). https://ec.europa.eu/newsroom/article29/redirection/document/49826.

disputing that some elements in the decision-making chain should be automated for speed, better analysis and cost-effectiveness, we argue that human withdrawal from semi or fully automated decision-making is one of the red lines of the European digital public legal order. The new dimension or broader sense of the right must include the requirement to have humancentered decision-making process controlling the AI decision and being ultimately responsible for it.

Another right that should gain wider meaning is the 'right to influence one's digital footprint'. Its forerunner is the right to be forgotten, developed in the decisions of the CJEU[67] and enshrined in the GDPR in Article 17 (Right to erasure or 'right to be forgotten').[68] In terms of influencing the digital footprint, individuals should have the right to participate in their digital lives in such a way that information is reviewed in accordance with time passed and its significance to the individual and not to society. One red line is that this should not provide loopholes for those who seek amnesty from their crimes against humanity or otherwise, to be erased from history. But it should give the proper tools to control one's image over time to avoid or put an end to the indelible past endlessly stalking people. This is all the more important as these people and/or their representatives at the time could not even imagine that AI tools are able to find and associate rare and extremely outdated data with them.[69]

In addition, the European Commission should consider introducing new rights in the AIA, with the rights enshrined in the EU Charter as a basis, similar to the right to be forgotten in the GDPR. For instance, the Regulation does refer to transparency obligations by AI systems, whereas the magnitude of certain situations merits genuine human contact, such as medical decisions. The rights proposed elsewhere by the authors of this piece and others are the 'right not to be manipulated', the 'right to be neutrally informed online'[70] and the 'right to meaningful human contact'.[71] The latter is especially important when considering which human activities can be fully automated and which cannot, and moreover, which human activities can, but should not be fully automated. Such a right should include the obligation to state to natural persons when they are interacting with an AIS system.

[67] See Judgment of the Court (Grand Chamber) [29]of 13.5.2014 (request for a preliminary ruling from the Audiencia Nacional — Spain) — Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317; Judgment of the Court (Grand Chamber) [31] of 24.9.2019, Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772.

[68] GDPR, Article 17.

[69] This right raises difficult questions as to where the balance should be drawn between, on the one hand, freedom of expression (including the right to receive information) and, on the other hand, for example, the rehabilitation of offenders. These two fundamental principles may collide in this subject area, which is a topic beyond the reach of this particular paper and to which the authors will return.

[70] Feedback to the European Commission on AI – ethical and legal requirements. Prof. Stéphanie Laulhé Shaelou and Konstantinos Alexandrou, University of Central Lancashire Cyprus campus (2021). https://ec.europa.eu/info/law/better-regulation/have-yoursay/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665299_en.

[71] van Est, R., Gerritsen, J. [72], 'Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality' (2017) Rathenau Instituut, 44. See also Laulhé Shaelou S. and Alexandrou K. https://www.project-sherpa.eu/anoverview-of-the-eus-artificial-intelligence-regulation/.

Besides, these new rights may include the 'right not to be measured, analysed or coached',[72] since both states and companies are increasingly resorting to mass surveillance and collecting the smallest detailed information about people. Such a right could include obligations not to resort to mass surveillance, at least in some places that should remain private, and not to resort to 24/7 surveillance. In addition, the very legality of mass surveillance must be questioned. The legality of such excessive surveillance was questioned by the ECtHR,[73] but the Court preferred to focus on the details of the surveillance, in particular what conditions should be met by proper surveillance.

5 Conclusion

Interaction with artificial intelligence systems requires some courage and cautions at the same time and in the right doses. It may appear that there are at least three characteristics we would need to live with AIS in social harmony, namely potentially (re-)new(ed) fundamental rights, core values as part of AI design, and a noncompromised regulatory framework on issues of principal importance for fundamental human rights, Rule of Law and democratic values protection. To meet these goals we suggest to enhance, supplement and/or expand the catalogue of (digital) fundamental human rights in the European Legal Order with such rights as described in this paper and by others as the 'right not to be subjected to automatic decision-making and automatic processing' (in the broadest sense), the 'right to influence one's digital footprint', the 'right not to be manipulated', the 'right to be neutrally informed online', the 'right to meaningful human contact', and the 'right not to be measured, analysed or coached'.

This paper shows the extent to which fundamental human rights, the Rule of Law and European values based on democracy must be embedded in all areas of the digital legal order, aiming at their effective and meaningful rather than formal inclusion. This paper calls on all proposed regulatory standards regarding AIS to be clear and strict in the sense that they do not allow putting human rights at risk and of driving people and societies away from the fundamental benefits of digitalisation at a higher cost vis-a-vis the benefits of technological developments and innovation. Achievements in the development of AI should not be evaluated from the standpoint that it is a race between democratic societies and future technologies. Ultimately, we want to have both: democratic societies based on the Rule of Law and fundamental human rights in which everyone benefits equally from technologies

Declarations

Competing Interests The authors declare no competing interests.

[72] van Est, R., Gerritsen, J. [72], 'Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality, 43.

[73] See ECtHR (Grand Chamber) Judgment [18], Big Brother Watch and Others v. the United Kingdom, App. Nos. 58170/13, 62322/14, 24960/15 (2021).

References

1. Trust and Transparency in Artificial Intelligence (Human Brains Project, 2021). https://doi.org/10.5281/zenodo.4588648
2. Ad hoc Committee on Artificial Intelligence (CAHAI), Feasibility Study (2020). https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da
3. 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 – C90146/2021 – 2021/0106(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html0236_EN.html
4. Andreou, A., Laulhé Shaelou, S., Schroeder, D.: Current Human Rights Frameworks (Sherpa project of Smart Information Systems, Horizon 2020, 2019). https://doi.org/10.21253/DMU.8181827
5. Atikcan, E.Ö., Chalmers, A.W.: Choosing lobbying sides: the general data protection regulation of the European Union. J. Public Policy **39**(4), 543–564 (2019). https://doi.org/10.1017/S0143814X18000223
6. 'Bias in algorithms – Artificial intelligence and discrimination. Report' (EU Agency for Fundamental Rights (FRA). Luxembourg: Publications Office of the European Union, 2022). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf
7. Bingham, T.: The Rule of Law. Penguin Books, Baltimore (2011)
8. Charisi, V., et al.: 'Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy' EUR 31048 EN, Publications Office of the European Union (2022). https://doi.org/10.2760/012329
9. Charter of Fundamental Rights of the European Union (18 Dec. 2000), 2010 O.J. C 83/02, entered into force 01 Dec. 2009
10. Christou, G., Rashid, I.: Interest group lobbying in the European Union: privacy, data protection and the right to be forgotten. Comp. Eur. Polit. **19**, 380–400 (2021). https://doi.org/10.1057/s41295-021-00238-5
11. Consolidated Version of the Treaty on European Union [2008] OJ C115/13
12. Dafoe, A.: On technological determinism: a typology, scope conditions, and a mechanism. Sci. Technol. Human Values **40**(6), 1047–1076 (2015). https://doi.org/10.1177/0162243915579283
13. 'Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights' (EU Agency for Fundamental Rights (FRA). Luxembourg: Publications Office of the European Union, 2019). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf
14. Denning, A.: Freedom Under the Law. Stevens & Sons Ltd, London (1949)
15. Dodsworth, L.: A State of Fear: How the UK Government Weaponised Fear During the Covid-19 Pandemic. Pinter & Martin, London (2021)
16. European Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 04 Nov. 1950), 312 E.T.S. 5, as amended by Protocol No. 3, E.T.S. 45; Protocol No. 5, E.T.S. 55; Protocol No. 8, E.T.S. 118; and Protocol No. 11, E.T.S. 155; entered into force 03 Sept. 1953 (Protocol No. 3 on 21 Sept. 1970, Protocol No. 5 on 20 Dec. 1971, Protocol No. 8 on 1 Jan 1990, Protocol 11 on 11 Jan 1998)
17. European Court of Human Rights (Chamber) Judgment. Kokkinakis v. Greece. App. Nos. 14307/88, A/260-A (1993)
18. European Court of Human Rights (Grand Chamber) Judgment. Big Brother Watch and Others v. the United Kingdom. App. Nos. 58170/13, 62322/14, 24960/15 (2021)

19. European Court of Human Rights (Second Section) Judgment. Høiness v. Norway. App. Nos. 43624/14 (2019)
20. European Court of Human Rights (Third Section) Judgment. Taganrog LRO and Others v. Russia. App. Nos. 32401/10 and 19 others (2022)
21. European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01)
22. Feedback to the European Commission on AI – ethical and legal requirements. Prof. Stéphanie Laulhé Shaelou and Konstantinos Alexandrou, University of Central Lancashire Cyprus campus (2021). https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665299_enethical-and-legal-requirements/F2665299_en
23. Fontes, C., et al.: AI-powered public surveillance systems: why we (might) need them and how we want them. Technol. Soc. **71**, 102137 (2022). https://doi.org/10.1016/j.techsoc.2022.102137
24. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (Data Protection Working Party, Adopted 3 October 2017). https://ec.europa.eu/newsroom/article29/redirection/document/49826
25. Hallström, J.: Embodying the past, designing the future: technological determinism reconsidered in technology education. Int. J. Technol. Des. Educ. **32**, 17–31 (2022)
26. Hennessy, P., Through, M.: Power, Politics and the Quality of Government in Postwar Britain. Victor Gollancz, London (1996)
27. Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori. 31 March 2023. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847
28. Jandric, P.: Postdigital human capital. Int. J. Educ. Res. **119**, Article ID 102182 (2023). https://doi.org/10.1016/j.ijer.2023.102182
29. Judgment of the Court (Grand Chamber) of 13 May 2014, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317
30. Judgment of the Court (Grand Chamber) of 21 June 2022, Ligue des droits humains v Conseil des ministres, Case C-817/19, ECLI:EU:C:2022:491
31. Judgment of the Court (Grand Chamber) of 24 September 2019, Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772
32. Judgment of the Court (Grand Chamber) of 4 July 2023, Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social), Case C-252/21, ECLI:EU:C:2023:537
33. Judgment of the Court (Grand Chamber) of 4 June 2013, ZZ v Secretary of State for the Home Department, ECLI:EU:C:2013:363
34. Judgment of the Court (Grand Chamber) of 6 October 2020, La Quadrature du Net and Others, Joined Cases C511/18, C512/18 and C520/18, ECLI:EU:C:2020:791
35. Judgment of the Court (Grand Chamber) of 6 October 2020, Privacy International, Case C-623/17, ECLI:EU:C:2020:790
36. Judgment of the Court (Second Chamber) of 3 June 2021, K and Others v Tesco Stores Ltd, ECLI:EU:C:2021:429
37. Judgment of the Court (Tenth Chamber) of 11 March 2021, A. A. v État belge, Case C-112/20, ECLI:EU:C:2021:197
38. Judgment of the Court of 24 May 2023, Meta Platforms Ireland v Commission, Case T-451/20, ECLI:EU: T:2023:276, Case T-452/20, ECLI:EU: T:2023:277
39. Judgment of the General Court of 10 November 2021, Google and Alphabet v Commission, Case T612/17, ECLI:EU: T:2021:763
40. Krawiec, J.M., Piaskowska, O.M., Piesiewicz, P.F., et al.: Tools for public health policy: nudges and boosts as active support of the law in special situations such as the Covid-19 pandemic. Glob. Health **17**, 132 (2021). https://doi.org/10.1186/s12992-021-00782-5
41. Laulhé Shaelou, S.: The EU and Cyprus: principles and strategies of full integration, Studies in EU External Relations (SEUR 3, Brill/Martinus Nijhoff Publishers, 2010), 201-208
42. Laulhé Shaelou, S., Alexandrou, C.: An overview of the EU's Artificial Intelligence Regulation. https://www.project-sherpa.eu/an-overview-of-the-eus-artificial-intelligence-regulation/
43. Laulhé Shaelou, S.: Market freedoms, EU fundamental rights and public order: views from Cyprus. Yearb. Eur. Law **30**(1), 298 (2011)
44. MEPs ready to negotiate first-ever rules for safe and transparent AI (Press Releases, 14 June 2023). https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-aifirst-ever-rules-for-safe-and-transparent-ai

45. New Product Liability Directive. Overview. Briefing EU Legislation in Progress (May 2023). https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf
46. Olhede, S.C., Wolfe, P.J.: The growing ubiquity of algorithms in society: implications, impacts and innovations. Philos. Trans. R. Soc. A, Math. Phys. Eng. Sci. **376**, 20170364 (2018). https://doi.org/10.1098/rsta.2017.0364
47. Opinion, SCHUFA Holding and Others (Scoring), Case C-634/21, ECLI:EU:C:2023:220
48. Opportunities of Artificial Intelligence (European Parliament, 2020). https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf
49. Pasquale, F.: Platform neutrality: enhancing freedom of expression in spheres of private power. Theor. Inq. Law **17**, 487–513 (2016)
50. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) (COM/2022/496 final)
51. 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)
52. Razmetaeva, Yu.: Algorithms in the courts: is there any room for a rule of law. Justice East. Eur. **4**(16), 87–100 (2022). https://doi.org/10.33327/AJEE-18-5.4-a000429
53. Razmetaeva, Y.: Opinions and algorithms: trust, neutrality and legitimacy. Filos. Prava i Zahal'na Teor Prava **1**, 80–94 (2022). https://doi.org/10.21564/2707-7039.1.275638
54. Recommendation CM/Rec (2018)2 of the Committee of Ministers to member States on the roles and responsibilities of Internet intermediaries. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14
55. 'Regulating in a Digital World' (House of Lords, Selection Committee on Communications 2019)
56. 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)
57. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)
58. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)
59. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee (Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics) (COM/2020/64 final)
60. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee (Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics) (COM/2020/64 final)
61. Rodriges, R., Panagiotopoulos, A., Lundgren, B., Laulhé Shaelou, S., Grant, A.: Regulatory options for AI and big data (Sherpa project of Smart Information Systems, Horizon 2020, 2020). https://doi.org/10.21253/DMU.11618211
62. Rodriges, R., Panagiotopoulos, A., Lundgren, B., Laulhé Shaelou, S., Grant, A.: Regulatory options for AI and big data (Sherpa project of Smart Information Systems, Horizon 2020, 2020). https://doi.org/10.21253/DMU.11618211
63. Sasaki, S., Saito, T., Ohtake, F.: Nudges for Covid-19 voluntary vaccination: how to explain peer information? Soc. Sci. Med. **292**, 114561 (2022). https://doi.org/10.1016/j.socscimed.2021.114561
64. Smith, M.: Technological determinism in American culture. In: Smith, M., Marx, L. (eds.) Does Technology Drive History? The Dilemma of Technological Determinism. MIT Press, Cambridge (1994)
65. Stahl, B.: Artificial Intelligence for a Better Future: An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies. Springer, Berlin (2021)
66. Stahl, B., et al.: Artificial intelligence for human flourishing – beyond principles for machine learning. J. Bus. Res. **124**, 374–388 (2021). https://doi.org/10.1016/j.jbusres.2020.11.030
67. Stinson, C.: Algorithms are not neutral. AI Ethics **2**, 763–770 (2022). https://doi.org/10.1007/s43681https://doi.org/10.1007/s43681-022-00136-w022-00136-w
68. 'The lobby network: Big Tech's web of influence in the EU'. Report. Corporate Europe Observatory and LobbyControl e.V. Brussels and Cologne, August 2021. https://www.politico.eu/wp-content/uploads/2021/08/30/BigTech-Firepower-study-Final.pdf
69. 'The lobbying Ghost in the Machine. Big Tech's covert defanging of Europe's AI Act'. Report. Corporate Europe Observatory. Brussels, February 2023. https://corporateeurope.org/sites/default/files/2023-03/The%20Lobbying%20Ghost%20in%20the%20Machine.pdf

70. The Venice Commission. Report on the rule of law. CDL-AD (2011)003rev-e. Adopted by the Venice Commission at its 86th plenary session (Venice, 25-26 March 2011). https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2011)003rev-e
71. Tsamados, A., Aggarwal, N., Cowls, J., et al.: The ethics of algorithms: key problems and solutions. AI Soc.: Knowl, Cult. Commun. **37**, 215–230 (2022). https://doi.org/10.1007/s00146-021-01154-8
72. van Est, R., Gerritsen, J.: Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality. Rathenau Instituut. (2017). https://www.rathenau.nl/sites/default/files/2018-02/Human%20Rights%20in%20the%20Robot%20Age-Rathenau%20Instituut-2017.pdf
73. van Giffen, B., et al.: Overcoming the pitfalls and perils of algorithms: a classification of machine learning biases and mitigation methods. J. Bus. Res. **144**, 93–106 (2022). https://doi.org/10.1016/j.jbusres.2022.01.076
74. Vilhelmsson, A., Sant'Anna, A., Wolf, A.: Nudging healthcare professionals to improve treatment of Covid-19: a narrative review. BMJ Open Qual. **10**, e001522 (2021). https://doi.org/10.1136/bmjoqhttps://doi.org/10.1136/bmjoq-2021-0015222021-001522
75. Weiskopf, R.: Algorithmic decision-making, spectrogenic profiling, and hyper-facticity in the age of post-truth. Le foucaldien **6**(1), 1–37 (2020). https://doi.org/10.16995/lefou.62
76. 'White Paper on Artificial Intelligence – a European Approach to Excellence and Trust' COM (2020) 65 final. https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_enapproach-excellence-and-trust_en

Authors and Affiliations

Stéphanie Laulhé Shaelou[1] · Yulia Razmetaeva[2,3]

✉ S.L. Shaelou
SLaulhe-Shaelou@uclan.ac.uk

1 Professor of European Law and Reform, Head of School of Law, Director of the Jean Monnet Centre of Excellence for the Rule of Law and European Values (CRoLEV), University of Central Lancashire, 12-14 University Avenue, 7080, Larnaca, Cyprus

2 Associate Professor, Department of Human Rights and Legal Methodology, Yaroslav Mudryi National Law University, 77 Pushkinska street, 61024, Kharkiv, Ukraine

3 Visiting Researcher, Department of Law, Uppsala University, 20 Trädgårdsgatan, 753 09, Uppsala, Sweden