Exploring the Relationship Between Article 22 of the General Data Protection Regulation and Article 14 of the Proposed AI Act

Some Preliminary Observations and Critical Reflections

Liane Colonna

Introduction[1]

Human-centered AI is emerging as a central pillar of responsible AI. Instead of narrowly focusing on technical processes like automation and optimization, the field calls for the broader consideration of the ethical, legal, and societal implications of AI systems. The goal is to create AI systems that put humans in control, amplifying and augmenting their capabilities rather than superseding them.[2] A world of human-centered AI envisions an ever-deeper cooperation between humans and machines, allowing humans to not just "increase the accuracy and safety of AI systems" but also "uphold human values in automated decision-making, and build trust in the technology."[3]

[1] This work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program – Humanities and Society (WASP-HS) funded by the Marianne and Marcus Wallenberg Foundation and the Marcus and Amalia Wallenberg Foundation. Additionally, I would like to express my gratitude to Dr. Andreas Kotsios and Dr. Johanna Chamberlain who have provided helpful comments on the manuscript, or parts thereof, at various stages in its development. As far as shortcomings are concerned, they are all attributable to the author.

[2] Ben Shneiderman, Human-Centered AI (Oxford University Press 2022).

[3] Johann Laux, *Institutionalised Distrust and Human Oversight of Artificial Intelligence: Toward a Democratic Design of AI Governance under the European Union AI Act* (March 3, 2023), Available at SSRN: https://ssrn.com/abstract=4377481 or http://dx.doi.org/10.2139/ssrn.4377481, 1–30, abstract; Thomas Herrmann and Sabine Pfeiffer, *Keeping the Organization in the Loop: A Socio-Technical Extension of Human-Centered Artificial Intelligence*, AI and Society (2022)(the "work done by humans and machines will become ever more interactive and integrated").

Combining the use of precise, efficient, objective, and consistent automated decision-making systems with human input, values and judgement is very alluring because it promises to create a win-win scenario, optimizing the strengths of both humans and computers and reducing their weaknesses. However, recent scholarship has highlighted that it may not always be possible or desirable to have human intervention or oversight, giving rise to a concern that policies that demand human-centered AI might have serious drawbacks, potentially promoting the worst of both worlds.[4] For example, Green contends that there is significant "empirical evidence about how people interact with algorithms" to show that they do not reliably perform desired oversight functions.[5] Consequently, policies that require human oversight "provide a false sense of security in adopting algorithms" and allow the use of algorithms by entities without any accountability for the harms they may create.[6] More recently, Crootof et al. identify what they refer to as "the law of the loop" and explain how regulators deploy it in sloppy ways "that set up both the human and the greater human-machine system to fail."[7] In other words, they argue that law is used in a disorganized and haphazard manner which undermines the policy goal to support hybrid decision making.[8]

This paper adds to the critical scholarship around the role of humans in algorithmic decision-making processes and contends that the legal rules that promote human-machine decision making must be more closely scrutinized, synthesized, and potentially revised. More specifically, it contributes to literature by bridging the gap between AI scholarship and data protection scholarship, focusing concretely on the relationship between

[4] Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 467 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781 ("Ideally, a human-in-the-loop system would combine the best of both worlds: human flexibility could cushion algorithmic brittleness, algorithmic speed could swiftly resolve easy issues while leaving space for slower humans to weigh in on the harder ones, and algorithmic consistency and human contextuality would balance each other in appropriate equipoise."); Ben Green, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, 45 Computer Law and Security Review 1–22 (2022); Isaac Ben-Israel, Jorge Cerdio, Arisa Ema et. al., *Towards Regulation of AI Systems: Global Perspectives on the Development of a Legal Framework on Artificial Intelligence (AI) Systems Based on the Council of Europe's Standards on Human Rights, Democracy and the Rule of Law* (Council of Europe, 2020), https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a.

[5] Ben Green, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, 45 Computer Law and Security Review 1–22, 2 (2022).

[6] Ben Green, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, 45 Computer Law and Security Review 1–22, 2 (2022).

[7] Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 434 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781.

[8] Id.

Article 22 of the GDPR and Article 14 of the proposed AI Act.[9] The aim is to make an analytical contribution concerning the connection between these legal provisions which both share the goal of ensuring human-centered AI. It argues that while Article 14 of the AI Act advances the objectives of human-centered AI by extending responsibility for it to technology providers that produce high-risk AI, there nevertheless exist several gaps and ambiguities in the law concerning its relationship to Article 22 of the GDPR that must be resolved to promote the coherency of the legal system.

At the outset, the paper will begin by engaging in some semantic management which is a methodological approach applied in the field of law and informatics that involves structuring relevant legal concepts and explaining the relationships between them.[10] The focus is on understanding the use of the phrase "human oversight" in the AI Act and how it differs from "human intervention", the expression applied in the GDPR. Arguably, understanding the meaning behind these two phrases is a key to unlocking the relationship between Article 14 of the AI Act and Article 22 of the GDPR.

Next, the paper will explore three central issues, exploring inconsistencies, problems, and paradoxes in the laws. First, it examines whether including human oversight under the AI Act will necessarily exclude the application of Article 22 of the GDPR on the basis that there is *a priori* human involvement, meaning the processing is not "solely" by automatic means. Second, the paper assesses the relationship between Article 14 of the AI Act, Article 22 of the GDPR and Article 25 of the GDPR, considering how the different normative phenomena in these provisions relate and possibly conflict with one another. Third, the paper unpacks how different responsibilities for meeting human oversight and human intervention may be shared by various participants in the AI supply chain, highlighting conflicts and practical difficulties that may emerge when legal roles clash or overlap with one another.

[9] For more on the relationship between AI and personal data protection in this book, see Johanna Chamberlain and Andreas Kotsios, Data Protection Beyond Data Protection Regulation, Dataskyddet 50 År (2023).

[10] *See e.g.* Cecilia Magnusson Sjöberg, A *Conceptual Approach to AI and Data Protection*, In: 2020–2021 Nordic Yearbook – Law in the Era of Artificial Intelligence (eds. Liane Colonna and Stanley Greenstein)(Stockholm, The Swedish Law and Informatics Research Institute (IRI)(2022), 47–62, 49–53; Liane Colonna, *Data Mining and the Need for Semantic Management*, in Internationalisation of Law in the Digital Information Society: Nordic Yearbook of Law and Informatics 2010–2012 (Dan Jerker B. Svantesson and Stanley Greenstein (eds.)) (Copenhagen, Ex Tuto Publishing: 2013), 335–344.

Semantic management

Where it concerns human-centered AI, there are many different words and phrases used to describe the relationship between humans and AI, creating confusion about how to distinguish certain terms from one another and potentially resulting in misunderstandings. Particularly relevant for this paper is the fact that the GDPR refers to human intervention[11] whereas the AI Act refers to human oversight[12], raising a question about whether these concepts are synonymous, and if not, what the difference is between them. To enhance comprehension and a more coherent application of the law, a deeper understanding of these expressions is required. Otherwise, the ambiguous use of language may create misinterpretations of the law, possibly allowing for the unintended use of autonomous systems.

When trying to understand the relevance of the language deployed in the GDPR and the AI Act, it is useful to review several of the key legal texts building up to the AI Act, at least insofar as these texts provide an understanding about the legislative intent. In April 2019, the EU Independent High-Level Expert Group on Artificial Intelligence (AI HLEG) released its final "Ethics Guidelines for Trustworthy Artificial Intelligence."[13] In these ethics' guidelines, the expert group proposed seven principles to design trustworthy AI based on fundamental rights. One of these central principles of ethical AI is "human agency and oversight."

According to the AI HLEG, "human agency and oversight" are necessary to ensure human autonomy and decision-making. More specifically, "human agency" is about allowing users to "make informed autonomous decisions regarding AI systems", ensuring they are "given the knowledge and tools to comprehend and interact with AI systems to a satisfactory degree and, where possible, enabling humans "to reasonably self-assess or challenge the system."[14] The AI HELG explicitly connects "human agency" to Article 22 of the GDPR, albeit in a footnote.[15] Human oversight, on the other hand, helps to ensure that an AI system does not undermine human autonomy or causes other adverse effects.[16]

[11] GDPR, Article 22(3).

[12] AI Act, Article 14.

[13] Independent High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI 15 (April 8, 2019), 1–39, 16 https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

[14] Id.

[15] Id. at footnote 36.

[16] Independent High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI 15 (April 8, 2019), 1–39, 16 https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

The AI HELG attaches "human oversight" to the concepts of human-in-the loop (HITL), human-on-the-loop (HOTL), or human-in-command (HIC).[17]

The AI HELG introduces the concept of the HITL as "the capability for human intervention in every decision cycle of the system."[18] HOTL refers to "the capability for human intervention during the design cycle of the system and monitoring the system's operation."[19] HIC refers "to the capability to oversee the overall activity of the AI system … and the ability to decide when and how to use the system in any particular situation."[20]

The Commission White Paper on Artificial Intelligence published in 2020, does not refer to HITL, HOTL or HIC but it does propose "human oversight" as a requirement for the future regulatory framework for AI.[21] The Commission White Paper explains that human oversight might "vary from one case to another" and can have many different manifestations.[22] These manifestations might include, *ex ante* human review and validation of the output of an AI system, *ex post* "human intervention" by a human, real time monitoring of AI systems, including the ability to intervene in real time and deactivate the system as well as design constraints.[23] Importantly, the Commission finds that human oversight should be reasonable and proportionate to the potential risks posed by the AI, indicating that a "one-size fits all" approach will not work in this realm.

Conceptually, it can be challenging to distinguish between these terms, especially because AI systems are complex socio-technical systems involving humans in every step of the way. As Crootof et al succinctly puts it: "Humans are everywhere, whether in the loop, on the loop, off the loop, or hidden from view."[24] To understand if there is a HITL, HOTL, or HIC, it may also be necessary to first predefine the loop,

[17] Id.

[18] Id.

[19] Id.

[20] Id. (continuing to state, "This can include the decision not to use an AI system in a particular situation, to establish levels of human discretion during the use of the system, or to ensure the ability to override a decision made by a system.").

[21] European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust 16 (Feb. 19, 2020), available at https://ec-europa-eu.ezp.sub.su.se/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[22] Id.

[23] For a further discussion *see* Guillermo Lazcoz and Paul de Hert, *Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems: Essential Pre-Requisites Against Abdicating Responsibilities*, 8(32) Brussels Privacy Hub Working Paper 1–31, 11 (2022)(discussing the role of human intervention in the AI Act and how is it related to Article 22 GDPR, focusing on the role of Data Protection Impact Assessments to support accountable and meaningful human intervention).

[24] Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 434 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781; *see also* Meg Leta Jones, *The Ironies of Automation Law: Tying Policy Knots with Fair Automation Practices Principles*, 18

an issue soon to be dealt with by the Court of Justice of the European Union (CJEU) in the SCHUFA case.[25]

It appears that when a human is "on" the loop, the human supervises decision making by the autonomous system whereas when a human is "in" the loop, the human has control over the system and is part of the decision-making process.[26] Crootof et al add that when there is a human in the loop they have "the ability to intervene in an individual decision—to change it, approve it, or immediately implement it."[27] When a human is on the loop, on the other hand, the human "… is less involved, perhaps best described as that of a supervisor, rather than a deciding authority."[28] Here, it is worth mentioning that while humans may have the possibility to intervene *ex post facto* in the design phase of AI development, the evolving nature of AI and its ability to learn new patterns and relationships in data may limit the ability for human intervention to an *ex-ante* nature, depending on the nature of the system.[29]

From a legal perspective, it is unclear what the relationship is between human intervention and human oversight and more specifically, whether a human can be in the loop under the proposed AI Act in a way that does not constitute meaningful intervention under the GDPR. In their work, Crootof et al. define a human in the loop as an "individual who is involved in a single, particular decision made in conjunction with an algorithm."[30] They explicitly note "that nothing in our

Vanderbilt Journal of Entertainment and Technology Law 77, 134 (2015) ("A human will always be in the loop, at a minimum, as interactor or intervener in digital automation.").

[25] European Court of Justice, Request for a Preliminary Ruling (15 October 2021), C-634/21 – SCHUFA Holding and Others, https://curia.europa.eu/juris/documents.jsf?num=C-634/21; Opinion of Advocate General MP Pikamäe, SCHUFA Holding and Others, C-634/21, EU:C:2023:220; see further, Reuben Binns and Michael Veale, *Is That Your Final Decision? Multi-stage Profiling, Selective Effects, and Article 22 of the GDPR*, 11 International Data Privacy Law 319 (2021).

[26] Jesse Hirsh, The Ethical Questions We Need to Ask Before Adopting Automated Weaponry, Centre for International Governance Innovation (3 December 2019). https://www.cigionline.org/articles/ethical-questions-we-need-ask-adopting-automated-weaponry/; Guillermo Lazcoz and Paul de Hert, *Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems: Essential Pre-Requisites Against Abdicating Responsibilities*, 8(32) Brussels Privacy Hub Working Paper 1–31, 11 (2022).

[27] Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 441 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781; Guillermo Lazcoz and Paul de Hert, *Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems: Essential Pre-Requisites Against Abdicating Responsibilities*, 8(32) Brussels Privacy Hub Working Paper 1–31, 11 (2022).

[28] Joel E. Fischer et al., *In-the-Loop or On-the-Loop? Interactional Arrangements to Support Team Coordination with a Planning Agent*, 33 Concurrency and Computation Practice and Experience 1–16 (2021).

[29] The feedback received from Andreas Kotsios inspired this sentence.

[30] Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 440 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781.

definition requires that the human in the loop must be effective."[31] This is a very important distinction, especially when considering the relationship between Article 22 of the GDPR and Article 14 of the Act, as will be explained more below.

Human-centered AI in the law

Article 22 of the GDPR

Article 22 of the GDPR lays the foundation for human control of AI, at least where the technology involves the use of personal data. Article 22(1) of the GDPR states that "(t)he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Three requirements must be satisfied cumulatively for Article 22(1) to be applicable: first, there must be an individual decision; second, the decision must be solely based on automated processing; and third, the decision must have legal or similarly significant effects on the data subject. Fully automated decision-making or profiling is authorized by Article 22 in some situations, such as where it is permitted by Member State law.[32] Where fully automated decision making is permitted under an exception, certain "suitable measures" must be implemented to safeguard the data subject's rights.[33]

The ex-Article 29 Working Party, now replaced by the European Data Protection Board (EDPB), has set forth guidelines about how to interpret Article 22.[34] It first states that Article 22(1) applies only if "there is no human involvement in the decision process."[35] However, it subsequently sets forward two requirements, qualifying the definition of solely.[36] These two requirements are that "meaningful" *ex post* review of an automated decision must be done by a human that has "the authority and competence to change the decision" and the ability to "consider all

[31] Id.

[32] GDPR, Article 22(3).

[33] GDPR, Article 22(2)(b), 22(3).

[34] Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation* 2016/679, 1–37, 21, https://ec.europa.eu/newsroom/article29/items/612053.

[35] Id. at 20–21.

[36] Emily Pehrsson, *The Meaning of the GDPR Article* 22, EU Law Working Papers No. 31, Stanford-Vienna Transatlantic Technology Law Forum 1–31, 17–22 (2018), https://law.stanford.edu/wp-content/uploads/2018/05/pehrsson_eulawwp31.pdf.

the relevant data" in order to remove the processing from the scope of Article 22(1).[37]

Lazcoz and de Hert contend that the right to human intervention is required as "an essential component of decision-making" under Article 22(1) but only as "a safeguard on request" under Article 22(2).[38] That is, under Article 22(1) of the GDPR, a controller can avoid the application of the provision if it introduces a human into the decisional loop. However, if one of the exceptions under Article 22(2) applies then human intervention only enters upon request by the data subject.[39]

The scope of Article 22 has been subject to extensive academic scrutiny. There has been a large debate about whether Article 22 constitutes a right or a qualified prohibition[40], an issue that is likely to be settled soon by the CJEU in the forthcoming SCHUFA case.[41] There has also been significant work around whether there is a right to explanation in the GDPR.[42] Where it concerns the right to human intervention, scholars have highlighted the use of the word "solely" in Article 22 and how this word can cause even "rubber stamping" of automatic decisions by humans to remove the processing from Article 22 scrutiny.[43] As noted at the outset, academic commentators have also challenged whether

[37] Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation* 2016/679, 1–37, https://ec.europa.eu/newsroom/article29/items/612053.

[38] Guillermo Lazcoz and Paul de Hert, *Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems: Essential Pre-Requisites Against Abdicating Responsibilities*, 8(32) Brussels Privacy Hub Working Paper 1–31, 11 (2022).

[39] Guillermo Lazcoz and Paul de Hert, *Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems: Essential Pre-Requisites Against Abdicating Responsibilities*, 8(32) Brussels Privacy Hub Working Paper 1–31, 11 (2022).

[40] *See e.g.* Emily Pehrsson, *The Meaning of the GDPR Article 22*, EU Law Working Papers No. 31, Stanford-Vienna Transatlantic Technology Law Forum 1–31, 17–22 (2018), https://law.stanford.edu/wp-content/uploads/2018/05/pehrsson_eulawwp31.pdf; Margot E. Kaminski and Jennifer M. Urban, *The Right to Contest AI*, 121 Columbia Law Review 1957, 2047 (2021); Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7(2) International Data Privacy Law 76–99, 94–95 (2017); Luca Tosoni, *The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation*, 11(2) International Data Privacy Law (2021); Diana Sanch, *Automated Decision-Making under Article 22 GDPR*, In: Algorithms and Law (eds. Martin Ebers and Susana Navas)(Cambridge University Press, 2020), 136–156, 147–148.

[41] European Court of Justice, Request for a Preliminary Ruling (15 October 2021), C-634/21 – SCHUFA Holding and Others, https://curia.europa.eu/juris/documents.jsf?num=C-634/21; Opinion of Advocate General MP Pikamäe, SCHUFA Holding and Others, C-634/21, EU:C:2023:220.

[42] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7(2) International Data Privacy Law 76–99, 94–95 (2017).

[43] Id.

human intervention is a correct policy decision in the first place, pointing to fundamental issues like automation bias.[44]

Article 14 of the AI Act

Pursuant to the Commission's proposal, Article 14 of the AI Act is entitled "human oversight" and requires that AI systems that are classified as "high-risk" (according to Article 6 and Annex III) must be "designed and developed" in such a way that they can be "effectively overseen by natural persons during the period in which the AI system is in use."[45] There are two ways to ensure human oversight. First, it can be built into the high-risk AI system by the provider.[46] Second, it can be identified by the provider and implemented by the user of the AI system.[47]

Article 14(1) of the Commission's proposal places a special emphasis on implementing appropriate "human-machine interface tools" so that AI systems can be effectively overseen by natural persons during the period in which the AI system is in use. The human or humans that are tasked with oversight must be able to detect anomalies, dysfunctions and unexpected performances[48] as well as be aware of "automation bias."[49] Article 14(4) further specifies that humans must be able to correctly interpret the system's output, be able to disregard, override or reverse the output of the system, and intervene in the operation of the system or interrupt the system through a "stop" button.[50]

Article 14(2) of the Commission's proposal explains that human oversight should prevent or minimize the risks to health, safety or fundamental rights that may emerge with a high-risk AI system.[51] Compared to Article 22 of the GDPR, therefore, human oversight requirements are broader than human intervention requirements in Article 14 of the AI Act, at least insofar as they include not just considering risks to data

[44] Ben Green, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, 45 Computer Law and Security Review 1–22, 1 (2022); Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 500 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781; *see also* Danielle Keats Citron, *Technological Due Process*, 85 Washington University Law Review 1249, 1271–72 (2008); Margot E. Kaminski, *Binary Governance: Lessons from the Gdpr's Approach to Algorithmic Accountability*, 92 Southern California Law Review 1529, 1594 (2019); Riikka Koulu, *Proceduralizing Control and Discretion: Human Oversight in Artificial Intelligence Policy*, 27 Maastricht Journal of European and Comparative Law 720–735, 734 (2020).

[45] AI Act, Article 14(1).

[46] AI Act, Article 14(3)(a).

[47] AI Act, Article 14(3)(b).

[48] AI Act, Article 14(4)(a).

[49] AI Act, Article 14(4)(b).

[50] AI Act, Article 14(4)(c)(d)(e).

[51] AI Act, Article 14(2).

protection but also risks to an individual's health and safety. Importantly, risks under Article 14(2) include those connected to the intended purpose of the system as well as other use cases, at least where they concern "reasonably foreseeable misuse."

Recital 48 of the Commission's proposal specifies that the natural persons to whom human oversight has been assigned under Article 14 should "have the necessary competence, training and authority to carry out that role." This is a valuable step forward since, according to Crootof et al., it is "one of the few times extant law governing human-in-the-loop systems acknowledges this need."[52] However, recitals are non-binding and therefore, do not carry the same force as the text of the AI Act itself.

Furthermore, Article 14(5) of the Commission's proposal sets forward specific measures for AI systems to be used for biometric identification. In addition to the measures referred to in Article 14(3), "no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons."[53] Veale and Borgesius explain that this approach constitutes a "four-eyes' principle" requiring "biometric identification systems to be designed so that two natural persons can sign off on any identification and have their identities logged, and for instructions to specify that they must."[54] Crootof et al. add that the requirement in Article 14(5) "positions the human(s) at the end of the loop, as gatekeepers to prevent action on the basis of an inaccurate algorithmic identification."[55]

The Council's General Approach includes additional language in Recital 48 which emphasizes the need for enhanced human oversight requirements in the context of certain biometric identification systems, although it simultaneously notes that this requirement should "not pose unnecessary burden or delays."[56] It also removes the specific language in Article 14(4)(a) of the Commission's proposal that suggests individuals should be able to detect and address "signs of anomalies, dysfunctions and unexpected performance." It adds language to Article 14(5) which

[52] Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 448 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781.

[53] AI Act, Article 14(5).

[54] Michael Veale and Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act* (July 31, 2021), 22(4) Computer Law Review International 97–112, 103 (2021).

[55] Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 448 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781.

[56] Council of the European Union, Interinstitutional File: 2021/0106(COD), Brussels, 25 November 2022 (OR. en) 14954/22 ("Council General Approach") https://artificialintelligenceact.eu/wp-content/uploads/2022/12/AIA-%E2%80%93-CZ-%E2%80%93-General-Approach-25-Nov-22.pdf.

limits the requirement for separate verification by at least two natural persons for certain high-risk biometric identification systems which are used for the purpose of law enforcement, migration, border control or asylum, at least in cases where Union or national law considers the application of this requirement to be disproportionate.

A notable development is that Article 29(1)(a) of the Council's General Approach suggests that users shall assign human oversight to natural persons who have the necessary competence, training, and authority. While similar language is included in Recital 48 of the Commission's proposal, the inclusion of it into the body of the text is significant considering the non-binding nature of recitals. The Council also includes language in Article 29(4) suggesting that, in addition to monitoring responsibilities, users shall "implement human oversight" based on the instructions of use. In other words, the Council has proposed revisions that would require users of high-risk AI systems to take more responsibility for human oversight.

Article 14(1) of the Parliament's General Approach requires that individuals in charge of human oversight have the AI literacy, the necessary support, and the authority to exercise human oversight. Here, there is a clear link to Article 22, especially the Article 29 guidelines[57] and recent enforcement decisions[58] which emphasize the existence of these criteria to limit the dangers of fully automated profiling. There is another, not explicit, but direct reference to Article 22 in Article 14(2) which states that human oversight shall prevent or minimize risks that arise where decisions are "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." It extends the risks to include not just those posed to health, safety, fundamental rights but also to the environment.[59]

Article 14(3) explains that human oversight "shall take into account the specific risks, the level of automation, and the context of the AI system" meaning that a one-size-fits-all approach is not required under the law. Likewise, it also makes plain that a provider or a user can apply either one or all the suggested measures, applying a "pick and choose" method, depending on the particular circumstances of the AI deploy-

[57] Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation* 2016/679, 1–37, 21, https://ec.europa.eu/newsroom/article29/items/612053.

[58] *For an excellent overview see* Sebastião Barros Vale and Gabriela Zanfir-Fortuna, *Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities*, The Future of Privacy Forum, 1–60, 28 https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf.

[59] Parliament General Approach, Article 14(2).

ment.[60] Article 14(4) again emphasizes that an "appropriate and proportionate" approach should be used when implementing human oversight. Article 14(e) acknowledges that human intervention might increase the risks or negatively impact the performance of AI and therefore, may not always be appropriate.

Finally, the Parliament goes even further than the Commission or the Council regarding the responsibility of "deployers" (their word for "users") of high-risk AI systems.[61] They suggest that deployers shall take appropriate technical and organizational measures to ensure they use high-risk AI systems in accordance with the instructions of use accompanying the systems.[62] The Parliament further explains that deployers of high-risk AI must adhere to the standards for human control outlined in Article 14, at least insofar as they exercise control over the high-risk system.[63] Deployers must also ensure that the natural persons assigned to ensure human oversight of the high-risk AI systems are not just "competent, properly qualified and trained" but also "have the necessary resources" to ensure effective supervision.[64]

Preliminary observations and critical reflections

Conflicting or complementary provisions?

As an initial matter, it is unclear whether compliance with Article 14 will make Article 22 of the GDPR superfluous because the processing may not be considered "solely" by automatic means, at least where high-risk AI is concerned. In other words, it can be argued that if there is "human oversight" under Article 14 then the requirement for *ex ante* human intervention set forward in Article 22 (1) will always be met, making Article 22 immaterial. The consequence of such an interpretation would be that a data subject may lack the right to obtain certain safeguards where it concerns automatic decision making that involves the processing of personal data such as the right to express his or her point of view and to contest the decision.

An alternative and more likely viewpoint is that Article 14 of the AI Act is complementary to Article 22 of the GDPR. That is, by requiring AI providers to develop human oversight mechanisms as soon as technically feasible in the development process, it will be more possible to

[60] Parliament General Approach, Article 14(3).
[61] Parliament General Approach, Article 3(4).
[62] Parliament General Approach, Article 29 (1).
[63] Parliament General Approach, Article 29(1)(a).
[64] Parliament General Approach, Article 29(1)(a).

support human intervention further along the supply chain. For example, without building a well-designed human-computer interface, it may not be possible to later exert sufficient human agency or control over automated decision-making, protecting the individual's qualified right not to be subject to fully automated processing.[65]

Ostensibly, a reason for using the phrase "human oversight" in the AI Act is to demark that it is not synonymous with "human intervention" under the GDPR and that different legal obligations exist under Article 14 of the AI Act and Article 22 of the GDPR. On this point, the Commission White Paper on Artificial Intelligence explicitly notes that the requirement for human oversight should "be without prejudice to the legal rights established by the GDPR when the AI system processes personal data."[66] Likewise, the EDPB and the European Data Protection Supervisor (EDPS), have emphasized that human oversight in the AI Act is critical to ensuring that the right not to be subject to a decision based solely on automated processing under the GDPR is respected, implying that these provisions should work together – not against one another.[67] The fact that Article 14(2) of the Parliament's General Approach makes a direct reference to preventing or minimizing risks that arise in the context of fully automated decision making also suggests that these provisions should support one another.

Barros Vale contends that incorporating human oversight under Article 14 may "not necessarily" rule out the Article 22 GDPR prohibition.[68] He explains that Article 14 of the AI Act "only requires providers to incorporate features that enable human oversight, but not to ensure human oversight as a default."[69] Barros Vale appears to be highlighting

[65] Gloria Andrada, On Human-Centered Artificial Intelligence, Metascience, 1–4, 2–3 (2023) (stating that "designing good interfaces that enhance human control is crucial for extending human agency.").

[66] European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust 16 (Feb. 19, 2020), available at https://ec-europa-eu.ezp.sub.su.se/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[67] EDPB-EDPS, Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) (2021), 1–22, 6 https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en (stating, "The Proposal gives an important place to the notion of human oversight (Article 14) which the EDPB and the EDPS welcome. However, as stated earlier, due to the strong potential impact of certain AI systems for individuals or groups of individuals, real human centrality should leverage on highly qualified human oversight and a lawful processing as far as such systems are based on the processing of personal data or process personal data to fulfil their task so as to ensure that the right not to be subject to a decision based solely on automated processing is respected.").

[68] Sebastião Barros Vale, *GDPR and the AI Act Interplay: Lessons from the FPF's ADM Case-Law Report*, Future of Privacy Forum (FPF), https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/.

[69] Id.

the ambiguous nature of the human oversight obligations under Article 14, which can be achieved by providers who build safeguards into the system before it is placed on the market (e.g. at the design level) or by users who implement appropriate measures after it is has been placed on the market (e.g. at the implementation level).

Arguably, the AI Act requires risk-based, flexible, design-focused requirements for human oversight placed on providers and users which are subsequently bolstered by more rigorous and firm human intervention requirements in the GDPR that are placed on data controllers.[70] If a technology provider implements human oversight measures into a high-risk AI system or if a user implements appropriate measures after it has been placed on the market under Article 14 of the AI Act then it cannot be assumed meaningful human intervention under Article 22 of the GDPR will exist in all situations. To put it differently, Article 14 might require that a user implements measures to support a human to be in the loop, but the oversight provided by this human in the loop may not necessarily rise to the standard of "meaningful" human intervention under Article 22, a matter that will need to be determined on a case-by-case basis.[71]

By way of example, recent enforcement decisions of Article 22 of the GDPR have found that the existence of trainings are an important criterion where it concerns the determination of whether human intervention is meaningful.[72] Afterall, if humans do not have sufficient training or expertise then they may not perform well and be in a position to

[70] Sara Domingo, *Human Intervention and Human Oversight in the GDPR and AI Act*, Trilateral Research (31 May 2022); *see also* Sebastian Bordt, Michèle Finck, Eric Raidl, Ulrike von Luxburg, *Post-Hoc Explanations Fail to Achieve their Purpose in Adversarial Contexts*, FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency 891–905, 895 (2022)(discussing the relationship between Article 13 and 14 of the AI Act to various provisions in the GDPR, including Article 22, with regard to critically analyzing explainability as a legal obligation, especially within adversarial contexts and stating, "In contrast to the draft AIA, which creates vague obligations resting on the user, the GDPR creates specific rights for the individual subjected to such decisions."); Johann Laux, *Institutionalised Distrust and Human Oversight of Artificial Intelligence: Toward a Democratic Design of AI Governance under the European Union AI Act* (March 3, 2023). Available at SSRN: https://ssrn.com/abstract=4377481 or http://dx.doi.org/10.2139/ssrn.4377481 1–30, 7 ("… Article 14 AIA does not provide much information as to what will make human oversight effective or meaningful. Article 14(3) and (4) AIA outline vague systems-design measures aiming to give human overseers the ability to monitor and intervene in the AI's decision-making.").

[71] *See further*, Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 442 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781 ("Note that nothing in our definition requires that the human in the loop must be effective.").

[72] *See e.g.* BVwG – W256 2235360-1, Austrian Federal Administrative Court 12/18/2020, https://rdb.manz.at/document/ris.bvwg.BVWGT_20201218_W256_2235360_1_00?source=726462233230323131323234237269732e6e2e4e4f52343031333935363323525 34c2332333230353132363135.

overcome automation bias.[73] If a user implements trainings to limit or prevent automation bias as recommended by Article 14 of the AI Act, then this may support the removal of the processing from the scope of Article 22 on the basis that there is meaningful human intervention.[74] However, this determination must be made on the facts of each specific case, especially given the rights-based nature of the GDPR.

Finally, it is important to emphasize that the AI Act mainly addresses technology providers and users of AI whereas the GDPR primarily addresses data controllers, data processors and data subjects. Article 14 does not create a relational obligation between providers and individuals at the end of the supply chain who may be harmed by the system created by the provider because of a failure to implement suitable human oversight measures. However, Article 22 partly fills this gap by permitting individuals to bring a claim against a data controller. Here, the goal of Article 14 may be to support the enforcement of existing remedies rather than to create new remedies for individuals.[75] In other words, Article 14 of the AI Act obliges actors that might not qualify as data controllers to support upstream actors who processes personal data to meet their obligations under Article 22 of the GDPR. This issue will be discussed more below.

A connection between human oversight by design and data protection by design?

Article 14(3)(a) of the Commission's proposal requires providers of high-risk AI to include human oversight measures into the architecture of AI systems to prevent harms to health, safety, and fundamental rights, at least where they are "technically feasible." While the obligations set forward in Article 14 are primarily placed on the provider under Article 14(3)(a), users may also be required to implement certain design measures under Article 14(3)(b) as well as under Article 29 of the Parliament's General Approach. Basically, high-risk AI systems must be built so that humans can oversee them and, if the provider cannot accomplish this on its own then it must instruct users as to how it can be done, creating a shared responsibility between the providers and users.[76]

[73] Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 500 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781.

[74] Article 14(3)(b), Article 14(4)(b).

[75] Liane Colonna, "The AI Regulation and Higher Education: Preliminary Observations and Critical Perspectives," In: De Lege 2021: Law, AI and Digitalisation (eds. Katja de Vries and Mattias Dahlberg)(Iustus Förlag AB)(2022), 333–356, 346.

[76] Johann Laux, *Institutionalised Distrust and Human Oversight of Artificial Intelligence: Toward a Democratic Design of AI Governance under the European Union AI Act* (March 3,

Article 14 can be seen as an example of design-based regulation, a term used often interchangeably with code-based or architecture-based regulation and sometimes techno-regulation or ambient law, to indicate the integration of values into technology in a proactive way to prevent harms, before they can occur.[77] Already in the 1990s, Lessig, in his now famous book entitled "Code as Law", arrived at a framework in which he argued that code can do much of the work of law and far more effectively.[78] In his work, he argued that code "can, and increasingly will, displace law", leading to a world in which "effective regulatory power (shifts) from law to code, from severance to software."[79] Decades later, this shift is ever more apparent with "by design" norms "ballooning across a wide range of contexts."[80] Bygrave, echoing Lessig's sentiments, contends that "(c)entral to the rationale" for this push to embed law into technical architectures is the idea that "technology plays a key role in setting the parameters for human conduct" and that it can often shape human behavior in a manner that is more efficient than legal norms.[81]

Reading Article 14 of the Commission's proposal of the AI Act together with Article 22 of the GDPR suggests that there is a direct link between the requirements for "human oversight by design" and "meaningful" human intervention. While Article 22 does not explicitly refer to building technical and organizational measures to ensure human intervention is meaningful, it is implied that such measures are necessary, especially when Article 22 is read in conjunction with the back-bone principle of "data protection by design" found in Article 25. However, as noted above, the GDPR largely only applies to upstream users of AI that operate at the end of the supply chain and qualify as data controllers which is problematic because these actors are not generally able to change the technical design of systems.[82] Here, it is submitted that

2023). Available at SSRN: https://ssrn.com/abstract=4377481 or http://dx.doi.org/10.2139/ssrn.4377481, 1–30, 7.

[77] Lee A Bygrave, *Security by Design: Aspirations and Realities in a Regulatory Context*, 8(3) Oslo Law Review 126–177, 127 (2022); N. van Dijk, A. Tanas, K. Rommetveit and C. Raab, *Right Engineering? The Redesign of Privacy and Personal Data Protection*, 32 International Review of Law, Computers & Technology 230–256, 231 (2018); Mireille Hildebrandt and Bert-Jaap Koops, *The Challenges of Ambient Law and Legal Protection in the Profiling Era*, 73 The Modern Law Review 428–460 (2010).

[78] Lawrence Lessig, Code and Other Laws of Cyberspace, 26 (1999).

[79] Id.

[80] Lee A Bygrave, *Security by Design: Aspirations and Realities in a Regulatory Context*, 8(3) Oslo Law Review 126–177, 153 (2022); *see also* Lawrence Lessig, Code and Other Laws of Cyberspace, 26 (1999).

[81] Id.; *see also* Lawrence Lessig, Code and Other Laws of Cyberspace, 26 (1999).

[82] *For more, see* Liane Colonna, *Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-oriented, Relational, and Distributed Approach*, 27(1) Tilburg Law Review 1–21 (2022).

an added value of Article 14 is that it imposes a legal responsibility on downstream actors to implement technical strategies to safeguard the fundamental right of data protection into their systems from the outset of the system's development, even if this obligation is limited to only providers of high-risk AI and therefore, still has a major limitation.[83]

While "by design" approaches to law are highly attractive from a policy perspective since they offer an immediate and effective way to enforce public policies, the growing shift towards techno regulation poses challenges that require critical assessment. For example, the requirement under the AI Act to embed multiple and broad values like "health", "safety" and "fundamental rights" into technical systems can no doubt be difficult to achieve since technology providers may lack methods to appropriately handle tradeoffs or direct conflicts between the different values that should be embedded into the system's design.[84] Here, it is important to add that these methods must now take into account the onslaught of "by design" requirements such as "human oversight by design", "privacy by design", "data protection by design", "security by design" etc. that must be implemented under various statutes and consider how all these different legal requirements can be effectively and simultaneously implemented across system development and throughout its deployment. For example, Article 14 might incentivize including a human in the loop, even when it is not appropriate or potentially dangerous, although the Parliament's General Approach does attempt to address this issue by explicitly recognizing that human oversight may not always be required under the AI Act.[85]

There may also be conflicts between the goals of "data protection by design" and "human oversight by design", particularly because Article 14 refers not to just data protection but also other interests including health, safety, and the environment, making its requirements broader. For instance, it may be that enabling human surveillance of high-risk AI systems to spot signs of dysfunctions conflicts with certain data protection values like data minimization, requiring a provider to make difficult tradeoffs at the design level that will subsequently have legal implications for technology providers, users, data controllers and data subjects. In short, technical experts may lack expertise and methodolo-

[83] Id.

[84] *See more generally* Mary Flanagan, Daniel C. Howe, Helen Nissenbaum, *Values at Play: Design Tradeoffs in Socially-Oriented Game Design*, CHI '05: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems April 2005, 751–760 (2005).

[85] Parliament General Approach, Article 14(4)(e); *see also* Lorrie Faith Cranor, 'A Framework for Reasoning about the Human in the Loop', Proceedings of the 1 st Conference on Usability, Psychology, and Security (UPSEC'08), 2008, 1 (arguing that in many cases, it is more secure for systems to avoid relying on a "human in the loop" to perform security-critical functions).

gies to balance fundamental rights, consider core legal principles like proportionality and to take into account the broader socio-technical context where the technology is deployed.

The development and deployment of technical standards may support technology providers and users to comply with the broad requirements of Article 14 of the AI Act as well as Article 22 and Article 25 of the GDPR. Indeed, the EU Commission has already issued a standardization request which tasks European Standards Organizations such as the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) with developing harmonized standards to support the implementation of the AI Act.[86] It has specifically requested European standard(s) and/or European standardization deliverable(s) on human oversight of AI systems.[87] These standards will be very influential and even act as a basis for conformity with the law.[88]

While the reliance on standards may provide a mechanism for technology providers and users to overcome some of the methodological challenges and meet their human oversight and human intervention obligations, it is necessary to recognize that reliance on standards may deepen the well-known opacity concerns around techno regulation.[89] While standards should theoretically be built with insight gathered from all relevant stakeholders, there are some practical issues to achieving

[86] Another European Standards Organizations is the European Telecommunications Standards Institute (ETSI) that may also be tasked with creating AI standards; *for more see* Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council OJ L 316/ 12, Annex I; *see also* Michael Veale and Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act* (July 31, 2021), 22(4) Computer Law Review International 97–112, 104 (2021); Martin Ebers, *Standardizing AI The Case of the European Commission's Proposal for an 'Artificial Intelligence Act'*, The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, Available at SSRN: https://ssrn.com/abstract=3900378 or http://dx.doi.org/10.2139/ssrn.3900378.

[87] European Comission, Draft Standardisation Request to the European Standardisation Organisations in Support of Safe and Trustworthy Artificial Intelligence, https://ec.europa.eu/docsroom/documents/52376.

[88] AI Act, Article 40.

[89] Bert-Jaap Koops, "Criteria for Normative Technology: The Acceptability of "'Code as Law'" in Light of Democratic and Constitutional Values", In: Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes 157–174 (Roger Brownsword and Karen Yeung eds.)(Hart Publishing 2008); Ronald E. Leenes, *Framing Techno-Regulation: An Exploration of State and Non-state Regulation by Technology*, 5 Legisprudence 143–169 (2011); Mireille Hildebrandt, "Technology and the End of Law" in: Facing the Limits of the Law (Bert Keirsbilck, Wouter Devroe & Erik Claes eds)(Springer 2009), 1–22; *see further* Liane Colonna, "Reconciling Privacy by Design with the Principle of Transparency", in: General Principles of EU Law and the EU Digital Order (eds. Prof. S. de Vries and Prof. U.Bernitz)(Kluwer Law International 2020).

an inclusive approach to standardization: standardization bodies are privately operated organizations that are influenced heavily by industry actors which limits the opportunities for fundamental rights experts and representatives of civil society like consumer protection groups to get involved, especially since they may not have the time or funding to participate.[90] Here, there is a concern that global companies and technical experts will shape European standards, excluding those representatives with more knowledge about fundamental rights from the process.

Which humans, what responsibilities and how to balance many caps?

While the flexibility provided for in Article 14(3) of the Commission's proposal for the AI Act creates different opportunities for regulated entities to meet their human oversight obligations depending on the context, it also leads to confusion about how responsibility for human oversight should be practically divided and shared between various actors in the supply chain. The different possibilities for human oversight provided for in Article 14 means that there may not just be a single human in the loop but, more likely, there will be many humans in the loop(s) that have co-existing responsibilities, some operating at the design level and others operating at the implementation level. Moreover, these humans may have overlapping obligations since they may not just qualify as a provider or a user under the AI Act but also as a data controller or processor under the GDPR.

It is interesting to consider the different roles and responsibilities regarding human oversight and human intervention under the AI Act and the GDPR and how they are divided between various humans involved in the supply chain. Under the GDPR, the controller bears the bulk of responsibilities whereas under the AI Act, the weight of the obligations of the law rest with the technology provider, although it must be noted that the Parliament is pushing for users to bear more responsibility for human oversight.[91] To highlight the difficulty of understanding

[90] Clément Perarnaud, "With the AI Act, We Need to Mind the Standards Gap," (25 April 2023), https://www.ceps.eu/with-the-ai-act-we-need-to-mind-the-standards-gap/; *see also*, Presentation by Sebastian Hallensleben, AI Standards Hub, European AI Standardisation in the context of the EU AI Act: The work of CEN-CENELEC JTC 21 (17 February 2023), European AI Standardisation in the context of the EU AI Act: The work of CEN-CENELEC JTC 21 (17 February 2023); European Digitial Rights, The Role of Standards and Standardisation Processes in the EU's Artificial Intelligence (AI) Act, https://aistandardshub.org/events/european-ai-standardisation/; https://edri.org/wp-content/uploads/2022/05/The-role-of-standards-and-standardisation-processes-in-the-EUs-Artificial-Intelligence-AI-Act.pdf.

[91] Parliament General Approach, Article 29.

which humans have what responsibilities and when these responsibilities arise, a practical example is provided.

Imagine a university would like to deploy an automatic grading system to score student performance which would constitute high-risk AI under the AI Act since it involves the assessment of students under Annex III(3)(b) of the Commission's proposal. In the context of an automatic grading system, it may be that the university has procured the technology from an Ed Tech provider, or it may be that it has developed the system in house. If the university has procured the system from an Ed Tech provider, it is likely that the university is the controller under the GDPR as well as the user under the AI Act and that the Ed Tech company is the provider under the AI Act. That said, the Ed Tech company may be classified as a controller, joint controller, or data processor under the GDPR, depending on the nature of the service. Here, it is interesting to consider whether under some circumstances the Ed Tech Company will automatically become a joint controller with the university under the theory that it defines the AI system's intended purpose and has control over the technical infrastructure, even if they do not process any personal data of the students.[92]

If the automatic grading technology is operated by a university that has developed the system in house, then it might find itself in the situation of being the provider, the user, and the controller.[93] The specific role (and attendant responsibility) of institutional employees within this context gets even more blurred since the concept of user seems to include both the university as well as natural persons within the university such as instructors who deploy the technology.[94] It is interesting to more broadly consider all of the humans that may be involved in an automatic assessment system at the university and their role for human oversight and intervention. Of course, the teacher and the students will directly interact with such a system, but various IT Departments may also be involved in ensuring its security and well-functioning. Perhaps an AI researcher at the university was the one to develop the tool. In

[92] Sebastião Barros Vale, *GDPR and the AI Act Interplay: Lessons from the FPF's ADM Case-Law Report*, Future of Privacy Forum (FPF), https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/.

[93] Liane Colonna, *The AI Regulation and Higher Education: Preliminary Observations and Critical Perspectives*, In: De Lege 2021: Law, AI and Digitalisation (eds. Katja de Vries and Mattias Dahlberg)(Iustus Förlag AB)(2022), 333–356.

[94] Anastasiya Kiseleva, Comments on the EU Proposal for the Artificial Intelligence Act (August 05, 2021). Available at SSRN: https://ssrn.com/abstract=3949585 or http://dx.doi.org/10.2139/ssrn.3949585 "(stating, 'It seems that the concept of the 'user' suggested in the proposed regulation has a dual character and applies both to organizations applying AI systems and natural persons doing so inside the organization. In this case, the roles and obligations of these subjects have to be clearly distinguished. Otherwise, their proper accountability can be difficult to ensure.' (internal citation omitted)"

their recent work, Herrmann and Sabine Pfeiffer emphasize that the binary of "human and technology" fails to consider "the use of technology and the decisions generated in this interplay of humans and technology are embedded in human organizations."[95]

Previous research has argued that a more distributed form of responsibility for AI is emerging in EU law, particularly where it concerns sharing responsibility to design technical systems in a way which respects fundamental rights.[96] The AI Act attempts to place more responsibility on individuals and entities who have hitherto been "off the hook" for building their systems in a way that respects fundamental rights. While requiring that responsibility is borne by more actors in the supply chain than just the data controller is a positive legal development since it acknowledges that design requirements are more effectively implemented at an early stage of technological development, an issue with this approach is that it can practically be very difficult to squarely pinpoint and apportion legal responsibility when it is shared. After all, distributed responsibility does not necessarily mean that all agents that contribute to an outcome, should bear equal responsibility for it.[97] Guidance will be required to clarify how an individual or entity who is classified as a provider, a user and/or a data controller can practically meet their human oversight and human intervention obligations under the law as well how liability can be apportioned.

Conclusion

There are many humans involved in the AI supply chain and it is relevant to consider how they might share responsibility for human oversight and intervention.[98] For example, there are programmers, engineers,

[95] Thomas Herrmann and Sabine Pfeiffer, *Keeping the Organization in the Loop: A Socio-Technical Extension of Human-Centered Artificial Intelligence*, AI and Society (2022)(continuing to explain, "Organizations—be they commercial enterprises or public institutions—are subject to their own logic, integrated into complex external environments, and divided internally by competition among departments with divergent interests. No matter whether decisions are technically or humanly generated, they must be negotiated and processed within the organization.").

[96] Liane Colonna, *Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-oriented, Relational, and Distributed Approach*, 27(1) Tilburg Law Review 1–21 (2022).

[97] Laura Cabrera and Jennifer Carter-Johnson, *Emergent Neurotechnologies and Challenges to Responsibility Frameworks*, 54 Akron Law Review 1, 16 (2020); Mark Coeckelbergh, *Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability*, 26 Science and Engineering Ethics 2051, 2056 (2020).

[98] Liane Colonna, *Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-oriented, Relational, and Distributed Approach*, 27(1) Tilburg Law Review 1–21 (2022).

designers, software vendors and other humans that are involved with designing, developing and operating automated decision-making systems.[99] It is also important to remember that the interactions that take place between humans and technology, especially where it concerns automated decision making systems, are often embedded in organizations which have their own distinct practices that shape the use of the technology.[100] Furthermore, there are many different loops and stages where human oversight and intervention may take place, depending on how a loop is defined or framed.[101] There may be humans involved but their oversight or intervention may not be meaningful, at least not from an empirical perspective.[102]

The proposed AI Act attempts to distribute responsibility for building human-centered AI to actors operating at the beginning of the supply chain, especially technology providers who have hither hereto generally been absolved of responsibility where it concerns building their systems in a way that respects fundamental rights. While requiring providers and users of AI systems to design and use their systems in a manner that minimizes risks to health, safety, fundamental rights and the environment is a positive development since design requirements are more easily met at the outset of a system's development rather than being bolted on later in the developmental process, it is unclear how legal obligations under Article 14 of the AI Act will co-exist with those under Article 22 of the GPDR.

One issue is that compliance with Article 14 may render Article 22 superfluous since there will almost always be some kind of *a priori* human involvement, although this is unlikely. A more probable interpretation is that Article 14 provides for a flexible and risk-based approach to human oversight and Article 22 provides for a more precise standard of meaningful human intervention, at least where personal data is involved in the processing. Another issue concerns the connection between "human oversight by design" and "data protection by design," and more specifically, around how technology providers should operationalize these requirements as well as manage tradeoffs and conflicts

[99] Zachari Swiecki, Hassan Khosravi, Guanliang Chen, Roberto Martinez-Maldonado, Jason M.Lodge, Sandra Milligan, Neil Selwyn, Dragan Gašević, *Assessment in the Age of Artificial Intelligence*, 3 Computers and Education: Artificial Intelligence 1–10, 6 (2022).

[100] Thomas Herrmann and Sabine Pfeiffer, *Keeping the Organization in the Loop: A Socio-Technical Extension of Human-Centered Artificial Intelligence*, AI and Society (2022).

[101] Rebecca Crootof et al., *Humans in the Loop*, 76 Vanderbilt Law Review 429–510, 444 (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4066781; Reuben Binns and Michael Veale, *Is That Your Final Decision? Multi-stage Profiling, Selective Effects, and Article 22 of the GDPR*, 11 International Data Privacy Law 319 (2021).

[102] Ben Green, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, 45 Computer Law and Security Review 1–22 (2022).

between legal norms. Although the creation and application of technical standards may assist technology providers to meet the ambiguous requirements of Article 14 of the AI Act as well as Articles 22 and 25 of the GDPR, it is important to note that this may create concerns about the legitimacy of technological regulation. A final issue is that there is considerable confusion over how an entity who is classified as a provider, a user and a data controller can practically meet its human oversight and human intervention obligations under the law. Guidance is necessary to help those subject to the GDPR and the AI Act to understand what human oversight and intervention means in practice and how to handle situations where their roles under each of the respective law may conflict.