TILBURG LAW REVIEW
Journal of International and European Law

Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-oriented, Relational, and Distributed Approach

RESEARCH ARTICLE

LIANE COLONNA

]u[ubiquity press

ABSTRACT

This paper explores the extent to which technology providers are responsible to end users for embedding data protection rules in the AI systems they design and develop, so as to safeguard the fundamental rights to privacy and data protection. The main argument set forth is that a relational rationale, requiring a broader range of actors in the supply chain to share legal responsibility for Data Protection by Design (DPbD) is better suited to address infringements to these fundamental rights than the current model that assigns responsibility mainly to the data controller or data processor. Reconceptualizing the law in a more future-oriented, relational, and distributed way would make it possible to adapt legal rules – including those within the GDPR and the continuously evolving EU acquis – to the complex reality of technology development, at least partly addressing the responsibility gap in DPbD.

A future-oriented conception of responsibility would require technology providers to adopt more proactive approaches to DPbD, even where they are unlikely to qualify as a controller. A relational approach to DPbD would require technology providers to bear greater responsibilities to those individuals or groups that are affected by their design choices. A distributed approach to DPbD would allow for downstream actors in the supply chain to bear part of the legal responsibility for DPbD by relying on legal requirements that are applicable to various actors in the supply chain supporting DPbD such as those found in contract law, liability law, and the emerging EU acquis governing AI, data, and information security.

CORRESPONDING AUTHOR:

Liane Colonna

Associate Professor, The Swedish Law and Informatics Research Institute (IRI), Stockholm University, Stockholm, Sweden

liane.colonna@juridicum.su.se

KEYWORDS:
Data Protection by Design; technology providers; GDPR; AI Act; responsibility

TO CITE THIS ARTICLE:
Liane Colonna, 'Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-oriented, Relational, and Distributed Approach' (2022) 27(1) *Tilburg Law Review* pp. 1–21. DOI: https://doi.org/10.5334/tilr.274

1 INTRODUCTION

Imagine the situation where Artificial Intelligence (AI) is deployed to ensure academic integrity in the context of an online exam at a major university in Sweden. In other words: AI – more specifically, facial recognition technology (FRT) – is used to automatically recognize behavior in students that indicates cheating or other academic misconduct. Unfortunately, at the beginning of an exam, the facial recognition software fails to recognize a dark-skinned student, even after several attempts by the student to make herself visible, including opening a window, turning on the lights, and shining a flashlight over her head.[1] As a result, the student is automatically prevented from taking the exam. This causes her severe anxiety and stress, both at the time of flagging and later, due to concerns regarding her ability to clear herself from being branded a "cheater" and performing at a high level on subsequent online exams.[2]

This paper will explore the relationship between the AI technology providers and the AI end users from a relational perspective. Taking the above scenario as a starting point, it will consider what obligations, if any, the provider of an Ed Tech system has to the student affected by the AI. It will focus on the obligation to embed data protection rules into the system to avoid negative outcomes from happening in the first place, pursuant to Article 25 of the General Data Protection Regulation (GDPR). The main argument set forth is that a relational rationale, requiring a broader range of actors[3] in the supply chain to share legal responsibility for Data Protection by Design (DPbD), is better suited to address infringements to the fundamental rights to privacy and data protection than the current model that assigns responsibility mainly to the data controller or data processor.[4]

While this paper is critical of the "data controller – data subject" dichotomy presented in the GDPR, it does not make the radical argument that the entire GDPR should be revised to include a broader set of actors that can be held responsible for DPbD. Rather, the argument set forth herein is that technology providers must bear greater responsibility for ensuring that the requirements of DPbD are met, even if they do not process personal data themselves or determine the purpose of the personal data processing. Reconceptualizing the law in a more future-oriented, relational, and distributed way would make it possible to adapt legal rules – including those within the GDPR and the continuously evolving EU *acquis* – to the complex reality of technology development. Technology providers could be required to build their systems with the fundamental rights to privacy and data protection front and center, even where the providers are not considered data controllers.

At the outset, it must be made clear that this paper is concerned with legal responsibility (liability), as opposed to moral responsibility (blame), although there is naturally some overlap. In other words, the focus of this paper is on responsibility attributed on the basis of law.[5] Furthermore, though the design and deployment of AI is conceptualized as a complex technological social assemblage, this paper is focused on the legal responsibility for human actors to design privacy-aware AI.[6] To

[1] Janice Wyatt-Ross, EdD, Twitter (23 February 2021), https://twitter.com/JaniceWyattRoss/status/1364032597484056577 (stating, "Daughter 1 was taking an exam today being proctored by some type of software that apparently was not tested on dark skin. She had to open her window, turn on the lights, and then shine a flashlight over her head to be detectable.").

[2] For more on exam anxiety in the context of online proctoring, *see* Daniel Woldeab and Thomas Brothen, *Video Surveillance of Online Exam Proctoring: Exam Anxiety and Student Performance*, 36 International Journal of E-Learning & Distance Education / Revue Internationale Du E-Learning Et La Formation à Distance 1 (2021), http://www.ijede.ca/index.php/jde/article/view/1204/1857.

[3] *See* Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford University Press 2005), 71 (defining an actor as "anything that does modify a state of affairs by making a difference is an actor – or if it has no figuration yet, an actant.").

[4] N. van Dijk, A. Tanas, K. Rommetveit and C. Raab, 'Right Engineering? The Redesign of Privacy and Personal Data Protection' (2018) 32 International Review of Law, Computers & Technology 230, 237 (stating that "The notion of personal data protection by design predominantly centers on the role of the controller as the responsible entity for the protection of individuals.").

[5] For more on the difference between legal and moral responsibility, *see* Aimee van Wynsberghe, 'Responsible Robotics and Responsibility Attribution' in Joachim von Braun, Margaret S. Archer, Gregory M. Reichberg, Marcelo Sánchez Sorondo (eds), *Robotics, AI, and Humanity* (Springer Cham 2021), 239–249, 243.

[6] For a similar approach, *see* Madalina Busuioc, 'Accountable Artificial Intelligence: Holding Algorithms to Account' (2021) 81 Public Administration Review 825, 826 (stating, "When we speak of actors in an accountability sense therefore, we still in this context, as in traditional contexts, speak of human actors. As algorithms have not achieved sentience or consciousness—despite widely hyped media stories, there has been little discernible progress towards so-called 'artificial general intelligence' (AGI) or 'human-level AI' (Ng 2018)—the responsibility for algorithmic use and operation in the public sector necessarily lies with human actors: AI system providers and public sector adopters and users for the operation and the implications of the algorithmic systems they create and respectively purchase and deploy.").

put it differently, this article is *not* focused on the issue of assigning responsibility to AI itself, even to highly autonomous AI that has achieved some level of sentience or consciousness, although important work is being done on that subject.[7]

2 METHOD

This paper seeks to explore the extent to which technology providers are responsible to end users for embedding data protection rules in the AI systems they design and develop, so as to safeguard human rights. To answer this research question and provide a comprehensive understanding of the complex legal issue and the body of law that surrounds it, a doctrinal research method is applied.[8] This method involves an in-depth interpretation and systematization of the law, with application of the established hierarchy of legal sources.[9] The purpose of this method is to identify gaps, ambiguities, contradictions, and other inconsistencies in the law in an effort to promote consistency and coherence in the legal system.[10]

The positive law relied upon in this work is principally expressed in regulations and case law concerning data protection at the EU level, but other sources include "literature expounding the rules."[11] Here, the distinct character of EU law has been considered by, for example, recognizing the plurality of legal sources and the phenomenon of shared sovereignty.[12] While acknowledging that national and EU law make up a multi-level system, which creates some methodological challenges, the main focus of this paper is the EU level, since the GDPR is implemented directly into national law.[13] In other words, the substantial degree of harmonization of data protection law at the EU level motivates a focus on EU sources of law.

In addition to the traditional, doctrinal analysis of the law as it is (*de lege lata*), the work will suggest what the law should be (*de lege ferenda*). Suggestions are made about how the law *ought* to address the responsibility of technology providers, at least as regards DPbD. In particular, suggestions are made on how the current legal framework could reflect a more just and fair approach to managing the responsibility for DPbD by revising existing laws and on how new laws could be developed to eliminate problems or defects in the law.

3 PREVIOUS RESEARCH

3.1 DPBD AND THE ROLE OF THE "CONTROLLER"

DPbD is an approach to system design that involves embedding privacy and data protection measures into a technology at the very outset of its development and throughout the entire design and deployment process. It is a dynamic and constantly evolving concept, as methods

[7] *See, e.g.,* Aimee van Wynsberghe, 'Responsible Robotics and Responsibility Attribution' in Joachim von Braun, Margaret S. Archer, Gregory M. Reichberg, Marcelo Sánchez Sorondo (eds) *Robotics, AI, and Humanity* (Springer Cham 2021), 239–249.

[8] For an overview of the doctrinal research method, *see* Benedict Sheehy and John Dumay, 'Examining Legal Scholarship in Australia: A Case Study' (2021) 49 International Journal of Legal Information 32–51, 38–39; *see also* Alexander Peczenik, 'A Theory of Legal Doctrine' (2001) 14:1 Ratio Juris 75–107, 79 (explaining that the doctrinal research method aims at acquiring a "coherent picture of the law … presenting the law as a network of principles, rules, metarules, and exceptions, at different levels of abstraction, connected by support relations.").

[9] Mark Van Hoecke, *Methodologies of Legal Research* (Oxford University Press 2011), preface, vi (stating that "Doctrinal legal research ranges between straightforward descriptions of (new) laws, with some incidental interpretative comments, on the one hand, and innovative theory building (systematization), on the other."); *see also* Christopher McCrudden, 'Legal Research and the Social Sciences' (2006) 122 Law Quarterly Review 632, 634.

[10] Álvaro Núñez Vaquero, 'Five Models of Legal Science' (2013) 19 Revus: Journal of Constitutional Theory and Philosophy of Law 53–81, 79; *see also* Suzanne Egan, 'The Doctrinal Approach in International Human Rights Scholarship' (November 29, 2017). UCD Working Papers in Law, Criminology & Socio-Legal Studies Research Paper No. 19/17, <https://ssrn.com/abstract=3082194 or http://dx.doi.org/10.2139/ssrn.308219417> page 17.

[11] David Ibbetson, 'Historical Research in Law' in Mark Tushnet and Peter Cane (eds), *The Oxford Handbook of Legal Studies* (Oxford University Press 2003), 864.

[12] Ruth Nielsen, 'New European Legal Realism: New Problems, New Solutions?' In Ulla Neergaard and Ruth Nielsen (eds) *European Legal Method: Towards a New Legal Realism?* (DJØF Publishing 2013).

[13] Martijn W. Hesselink, 'The Common Frame of Reference As A Source of European Private Law' (2009) 83 Tulane Law Review 919, 932 (discussing the "dynamic multi-level system" that exists between German and European law and the methodological approaches available in the context of private law); Johan Axhamn, 'Striving for Coherence in EU Intellectual Property Law: A Question of Methodology' in Jan Rosén, Gunnar Karnell, Annette Kur, Per Jonas Nordell, Daniel Westman, Stephan Carlsson, Johan Axhamn (eds) *Liber Amicorum* (Eddy 2016), 35–60.

and approaches to operationalizing DPbD are continuously expanding.[14] In many ways, DPbD has become the "holy grail" of data protection to the extent that it offers a governance strategy to prevent privacy and data protection problems *before* they happen, by seamlessly integrating the requirements of the law into system design.[15]

DPbD is derived from the closely related concepts of Privacy-Enhancing Technologies (PETs) and Privacy by Design (PbD).[16] Broadly, PETs are technical measures deployed in information and communication technology (ICT) to eliminate or minimize the "unnecessary or unwanted processing of personal data without the loss of the functionality of the information system."[17] Encryption is a textbook example of a PET. While PETs are entirely technology-driven solutions, PbD also includes organizational measures designed to respond to legal requirements, such as Data Protection Impact Assessments.[18]

The GDPR includes the principles of PbD in two requirements included in Article 25: DPbD and Data Protection by Default (DPbDF). Given the interrelationship between DPbD and DPbDF, this work refers only to DPbD. That said, it is important to understand that there is a conceptual difference between DPbD and DPbDF. Jasmontaite *et al.* state that DPbD refers to "the existence of embedded safeguards and mechanisms throughout the lifecycle of the application, service or product that protect the right to data protection, whereas (DPbDF) refers to the activation and application of such safeguards as default setting."[19] In other words, DPbDF is a subset of DPbD that is focused on the implementation of data protection safeguards in default settings.

Article 25 of the GDPR requires that organizations must "implement appropriate technical and organizational measures … which are designed to implement data protection principles … , in an effective manner and to integrate the necessary safeguards into [data] processing."[20] The provision further clarifies that controllers may take several factors into account when implementing DPbD, including the state of the art, the cost of implementation, the nature, scope, context and purposes of processing, and the risks (of varying likelihood and severity) to the rights and freedoms of natural persons posed by the processing.[21] Recital 78 includes a list of potential measures that may assist a data controller with its compliance burden such as minimizing the processing of personal data, pseudonymizing personal data as soon as possible, and providing transparency with regard to the functions and processing of personal data.[22] Stalla-Bourdillo *et al.* explain that "DPbD is the backbone of the GDPR, as complying with Article 25 should lead to complying with the data protection principles, as detailed by Article 5, and to enable all data subject rights, as listed in Articles 12–22."[23]

[14] *See, e.g.,* Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24 International Journal of Law and Information Technology 151; Alex Mihaildis, Liane Colonna, 'A Methodological Approach to Privacy by Design Within the Context of Lifelogging Technologies' (2020) 46 Rutgers Computer and Technology Law Journal 1–52.

[15] Liane Colonna, 'In Search of Data Protection's Holy Grail Applying Privacy by Design to Lifelogging Technologies' in Ronald Leenes, Dara Hallinan, Serge Gutwirth and Paul De Hert (eds.) *Data Protection and Privacy: Data Protection and Democracy* (Hart Publishing 2019), 176.

[16] EU Agency for Cybersecurity, Privacy by Design,<https://www.enisa.europa.eu/topics/data-protection/privacy-by-design>; Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24 International Journal of Law and Information Technology 151; Alex Mihaildis, Liane Colonna, 'A Methodological Approach to Privacy by Design Within the Context of Lifelogging Technologies' (2020) 46 Rutgers Computer and Technology Law Journal 1–52.

[17] G.W. van Blarkom, J.J. Borking, J.G.E. Olk, *Handbook of Privacy and Privacy-Enhancing Technologies; The case of Intelligent Software Agents* (College bescherming persoonsgegevens, Hague 2003), 33 available online https://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf; Commission of the European Communities. Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs). COM 2007 228 Final 2007. Available online: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX%3A52007DC0228.

[18] Ann Cavoukian, *Privacy by Design: The Seven Foundational Principles*, Information and Privacy Commissioner of Ontario, Canada (2010), available at: www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[19] Lina Jasmontaite *et al.*, 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' (2018) 4 European Data Protection Law Review 168, 169, available https://par.nsf.gov/servlets/purl/10081980.

[20] European Union, Council Regulation 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, OJ 2016 L 119/1 ("GDPR") Article 25.

[21] GDPR, Article 25.

[22] GDPR, Recital 78; Ari Ezra Waldman, 'Privacy's Law of Design' (2019) 9 UC Irvine Law Review 1239.

[23] Sophie Stalla-Bourdillon, Alfred Rossi, Gabriela Zanfir-Fortuna, *Data Protection by Process How to Operationalize Data Protection by Design for Machine Learning*, Future of Privacy Forum, 1–21, 4 https://fpf.org/wp-content/uploads/2019/12/WhitePaper_DataProtectionByProcess.pdf.

In theory, DPbD calls for a "holistic and rigorous" approach to data protection,[24] involving coordination of multiple parties in its deployment to ensure its effectiveness. These parties would include engineers, interaction designers, managers, lawyers, and policymakers, working not only within a given establishment, but also across the technology supply chain.[25] While DPbD is a regulative technique that embraces a "participatory and collaborative" model of governance,[26] it is generally only the controller who is responsible for compliance with the legal requirement.[27] A data controller is an entity that "determines the purposes and means of the processing of personal data."[28] According to the ex-Article 29 Working Party, the data controller is responsible for determining respectively "the why" and "the how" of particular processing activities.[29] Blume puts it simply: "[D]ata protection stands and falls with the controller."[30]

Previous research has demonstrated that the law is focused on the data controller as the main party responsible for DPbD. This is problematic because that approach fails to consider the important roles that other parties in the supply chain, such as manufacturers, engineers and system developers, play in the design process of data protection-aware systems.[31] These entities, collectively referred to as "technology providers," are unlikely to be classified as "data controllers" as they merely provide a product or service rather than receive, process, store, or access personal data.[32] While these parties are incentivized to adhere to the requirements of DPbD set forth in Article 25,[33] the data controller remains the main entity responsible for integrating data protection safeguards into technology.[34] Dijk *et al.* describe the dilemma: "Strong emphasis is put on data-controlling organizations for ensuring DPbD, but they must rely on solutions developed by technology producers who, in turn, are only 'encouraged' to take personal data protection into account."[35] To put it differently, data controllers are placed in the precarious position where they must take full legal responsibility for meeting the requirements of Article 25, but may themselves have only limited ability to implement data protection strategies into the system design.

[24] Urs Gasser, 'Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy' (2016) 130 Harvard Law Review Forum 61 available at https://harvardlawreview.org/2016/12/recoding-privacy-law-reflections-on-the-future-relationship-among-law-technology-and-privacy/.

[25] Woodrow Hartzog and Frederic Stutzman, 'Obscurity by Design' (2013) 88 Washington Law Review 385, 392.

[26] *See* Orly Lobel, 'The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought' (2004) 89 Minnesota Law Review 342, 344.

[27] *For more, see* Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81.

[28] GDPR, Article 4(7) (defining a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.").

[29] Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor," 1–31, 13, (Sept 16, 2010), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[30] Peter Blume, An Alternative Model for Data Protection Law: Changing the Roles of Controller and Processor, 5 International Data Privacy Law 292–297, 292 (2015).

[31] Ari Ezra Waldman, 'Privacy's Law of Design' (2019) 9 UC Irvine Law Review 1239, 1246 (stating, "It seems obvious to almost everyone that technology companies should be responsible for implementing privacy by design."); Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81.

[32] Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81, 84–85 *citing* Center for Information Policy Leadership [CIPL], Comments by the Centre for Information Policy Leadership on the European Data Protection Board's "Guidelines 4/2019 on Article 25 Data Protection by Design and By Default" Adopted on 13 November 2019 1, 6 (Jan 16, 2020), https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/cipl_response_to_edpb_privacy_by_design_guidelines.pdf.

[33] European Data Protection Board, Guidelines of the European Data Protection Board on Data Protection and Design, 1–31, 4 (Oct 20, 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (stressing the competitive advantage that technology providers and processors can gain by ensuring they both implement DPbD themselves and advise controllers on how best to do this).

[34] *See* Jiménez-Gómez, Briseida Sofía, 'Risks of Blockchain for Data Protection: A European Approach' (2020) 36 Santa Clara High Technology Law Review 281, 311 (explaining "The importance of identifying a data controller is two-fold. First, it defines the degree of responsibility for participants, consequently, the scope of accountability and the degree of eventual liability. Second, it enables communications from data subjects and data protection authorities to data controllers.").

[35] N. van Dijk, A. Tanas, K. Rommetveit and C. Raab, 'Right Engineering? The Redesign of Privacy and Personal Data Protection' (2018) 32 International Review of Law, Computers & Technology 230, 237.

3.2 DPBD AND THE ISSUE OF "MANY HANDS"

The issue of "many hands" refers to the challenge of identifying a single actor as responsible for a particular outcome when in fact multiple actors, both human and technical, have come together to contribute to it.[36] It refers to the difficulty that actors have in retaining individual agency in a hyperconnected, networked world where people, information, and technology work together to produce outcomes such as the one described at the outset of this article.[37] Van de Poel *et al.* define the problem of "many hands" as "undesirable outcomes in collective setting for which it is hard or even impossible to hold an individual or organization… responsible."[38] Essentially, the concept helps to describe "a problematic gap the distribution of responsibilities" in a collective setting where it is hard to squarely identify what act or omission led to a certain result or decision.[39]

The issue of "many hands" has been addressed by contemporary philosophers and ethicists, who highlight that in modern sociotechnical systems, where many different agents may contribute to a particular outcome, it becomes increasingly difficult to precisely determine "the who" or "the what" responsible for the outcome.[40] Ultimately, the concept of "many hands" underlines the interconnectedness and interdependencies of modern software and hardware supply chains, the cascading effects of design decisions made in this context, and the challenges of holding any single actor solely responsible for harms caused by a technology. Up until now, there has been limited research exploring the "many hands" problem from a strictly legal perspective.[41]

4 DPBD: TOWARDS A MORE FUTURE-ORIENTED, RELATIONAL, DISTRIBUTED CONCEPT

In the scenario at the outset of this article, it is likely that many different factors led to the unfavorable outcome where a dark-skinned student was left panic-stricken, flashing a light above her head to take an exam, and then unjustly prevented from doing so. The algorithm underlying the FRT might have had errors. For example, the FRT might have failed to recognize the student's face because the software developer relied on open-source software which had a history of racial bias issues. Perhaps the provider of the online proctoring tool bought an object recognition AI product or service from some other supplier and then "fine-tuned" the model with its own data, but incorrectly labelled the images, so the model was faulty. Alternatively, the hardware on the student's desktop might have been faulty. Maybe the camera malfunctioned because a sensor was damaged or incorrectly installed. There could have also been a problem with the underlying architecture used to support the AI system, such as a server, database, network, or cloud platform.[42] It might even be the case that a deep learning algorithm was applied, making it impossible for anyone to ever discover what precisely went wrong, even after having total access to the system designs and implementations.[43]

[36] Luciano Floridi, 'Distributed Morality in an Information Society' (2012) 19 Science and Engineering Ethics 727, 728 (discussing the problem of the "invisible hand"); M. Davis, 'Ain't No One Here But Us Social Forces: Constructing the Professional Responsibility of Engineers' (2012) 13 Science Engineering Ethics 13, 22–26 (distinguishing the between the problem of many hands and the problem of many causes); Laura Cabrera and Jennifer Carter-Johnson, 'Emergent Neurotechnologies and Challenges to Responsibility Frameworks' (2020) 54 Akron Law Review 1, 12.

[37] Andrej Zwitter, 'Big Data Ethics' (2014) Big Data and Society 1; Laura Cabrera and Jennifer Carter-Johnson, 'Emergent Neurotechnologies and Challenges to Responsibility Frameworks' (2020) 54 Akron Law Review 1, 12.

[38] Ibo van de Poel, Lamber Royakkers, and Sjoerd D. Zwart, *Moral Responsibility and the Problem of Many Hands* (Routledge 2015), 4.

[39] Neelke Doorn and Ibo van de Poel, 'Editors' Overview: Moral Responsibility in Technology and Engineering' (2012) 18 Science and Engineering Ethics 1, 6.

[40] Laura Cabrera and Jennifer Carter-Johnson, 'Emergent Neurotechnologies and Challenges to Responsibility Frameworks' (2020) 54 Akron Law Review 1, 12.

[41] *But see* Laura Cabrera and Jennifer Carter-Johnson, 'Emergent Neurotechnologies and Challenges to Responsibility Frameworks' (2020) 54 Akron Law Review 1; *see also* Silvia De Conca, 'Bridging the Liability Gaps: Why AI Challenges the Existing Rules on Liability and How to Design Human-empowering Solutions' in Bart Custers and Eduard Fosch-Villaronga (eds.), *Law and Artificial Intelligence* 239–258 (T.M.C. Asser Press 2022) (discussing the disrupting effects of AI on traditional notions of liability and proposing legal solutions to liability gaps).

[42] Charlotte A. Tschider, 'Beyond the Black Box' (2021) 98 Denver Law Review 683, 693.

[43] Mike Ananny, Kate Crawford, 'Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability' (2016) 20 New Media & Society 973–989, 981.

The point is that there were possibly several actors – human and computer – that contributed to the regretful outcome. There are likely an equal number of actors who could have prevented the outcome through designing the system in a more privacy-aware manner. In short, because the development of AI-based Ed Tech software involves many technical resources and stakeholders like data suppliers, front-end developers, back-end developers, database managers, cloud vendors, etc., any one of these agents acting alone or jointly could have contributed to the unjust outcome.[44]

This section will explore how the law should respond to the issue of many hands in the context of DPbD. It explores whether the current model of holding the data controller as the party mainly responsible for DPbD sufficiently acknowledges the assemblage of human actors and technologies working together in a complex system of systems where responsibility is inherently distributed among many different agents. It contends that DPbD must be conceived of as a more future-oriented, relational, and distributed concept, to address the complex human-technological interactions that are involved in the process of designing data protection into systems.

4.1 A FUTURE-ORIENTED CONCEPT

Previous research on the concept of responsibility shows that scholars distinguish between backward-looking responsibility and forward-looking responsibility.[45] DPbD has a backward-looking nature in that a court or judge can review an AI malfunction like the one described at the outset of this article and find that blame should be attributed based on the failure to prevent such a malfunction by embedding safeguards into the system. In the case at hand, it might be that the university that deployed the technology would be liable under the GDPR for a violation of Article 25 (DPbD). The university should embed technical and organizational measures to avoid the negative consequences to data protection rights where it relies on AI that has a significant impact on the life of any individual, such as in the grading context.

DPbD can also be conceived as a forward-looking responsibility in that it involves a prospective responsibility to prevent harm to the fundamental rights of privacy and data protection from the outset of system development through both organizational and technical strategies in a "constructive and mutually supporting way."[46] Indeed, DPbD, from the outset of its conceptualization, has been explicitly described as a "proactive not reactive" approach to safeguarding fundamental rights.[47] It is a concept that has a conscious orientation towards the future insofar as it seeks to "anticipate and address privacy problems *before* they can occur."[48] The concept is fundamentally about warding off data protection harms in an *ex ante*, preventative fashion, rather than in a remedial and reactive way.[49] Here, it is very important to highlight that the obligation exists regardless of whether there was any resulting data protection harm, an issue discussed in greater detail below.

Given the proactive nature of DPbD, it is strange that policymakers have decided to hold data controllers responsible for it, essentially limiting the legal obligation for proactivity to a single actor in the supply chain. Tsormpatzoudi *et al.* explain that data controllers often operate "at the very end of the supply chain" and this may be too late for the obligations of DPbD to be

[44] Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81, 91.

[45] Iris Marion Young, 'Responsibility and Global Justice: A Social Connection Model' (2006) 23 Soc Phil. & Pol'y 102, 121–122.

[46] Peter Seipel, 'Nordic School of Proactive Law Conference, Closing Comments' (2006) 49 Scandinavian Studies in Law 362, 360.

[47] Ann Cavoukian, *Privacy by Design*, available at https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf, 2 (declaring that Privacy by Design is based on seven foundational principles, including "proactive not reactive").

[48] Liane Colonna, 'Reconciling Privacy by Design with the Principle of Transparency' in S. de Vries and U. Bernitz (eds.), *General Principles of EU Law and the EU Digital Order* (Kluwer Law International 2020), 405–422, 407.

[49] Ann Cavoukian, *Privacy by Design*, https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf, page 2; Dag Wiese Schartum, '*Making Privacy by Design Operative*' (2016) 24 International Journal of Law and Information Technology 151, 155 (2016) (explaining that "An important point to underline is that proactivity is not only about preventing bad solutions from the perspective of privacy, but also about expressing the aim of ensuring beforehand that potential opportunities for privacy and effects thereof are considered."); *for more, see* Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework* (Springer Cham 2018).

effective.[50] Yet, as mentioned above, technology providers are unlikely to qualify as controllers "because they only make available the software to the user."[51]

It is understood that technology providers are in an excellent position to translate knowledge and values into technological artefacts.[52] Not only do they have the capacity to build technological systems that can completely prevent certain actions, they can also design systems to benefit certain individuals, groups, and values at the expense of others, placing them in a unique position to enable DPbD.[53] Ethicists claim that technology providers are in fact responsible for the tools they create because developers are not only the ones who create the actual technological architecture of the system, but also the ones who have the capacity to change the ways in which AI functions.[54] Martin explains that by "willingly creating an algorithm that works in a value-laden and particular manner," technology providers "voluntarily become a party to the decision system and take on the responsibility of the decision to include the harms created, principles violated, and rights diminished by the decision system."[55] However, the law holds data controllers as the main party responsible for DPbD, leaving technology providers largely free from legal responsibility on the basis that they do not determine how the software is used or exert control over the data processed.[56] Here, it can be observed that there is a gap in ethics and law.

While it may not be easy to entirely separate backward- and forward-looking responsibility in the case of DPbD, it is argued that responsibility for DPbD must be conceived as having a forward-looking nature, so that liability and risk can be managed better throughout the supply chain by *all* the actors that have a role in its implementation. In other words, all agents, even those far removed down the supply chain, should have a proactive obligation to implement data protection measures to prevent fundamental rights infringements to end users. This approach is in line with current research where scholars have increasingly confronted the need to consider responsibility in the context of both harms that have happened and harms that might happen in the future.[57] For example, Adam and Groves contend that current legal conceptualization of responsibility fails to consider responsibilities towards those in the future, and that it is key for legal scholars to engage with "phenomenological and feminist concepts of care" to remedy this situation.[58]

There is no doubt a need for methodological approaches to address what proactivity for DPbD means in practice and to better understand how proactivity can be translated into explicit legal requirements. Building on previous research by Mittelstadt *et al.*, Felzmann *et al.* suggest

[50] Pagona Tsormpatzoudi, Bettina Berendt and Fanny Coudert, 'Privacy by Design: From Research and Policy to Practice – The Challenge of Multi-Disciplinary, APF 2015: Privacy Technologies and Policy,' Bettina Berendt, Thomas Engel, Demosthenes Ikonomou, Daniel Le Métayer, Stefan Schiffner (eds.), in Lecture Notes in Computer Science (LNCS, volume 9484)(Springer 2016) 199–212, 207 (2016).

[51] Briseida Sofia Jiménez-Gómez, 'Risks of Blockchain for Data Protection: A European Approach' (2020) 36 Santa Clara High Technology Law Journal 281, 313.

[52] Kirsten E.H. Jenkinsa, Shannon Spruitc, Christine Milchramc, Johanna Höffkend, Behnam Taebic, 'Synthesizing Value Sensitive Design, Responsible Research and Innovation, and Energy Justice: A Conceptual Review' (2020) 69 Energy Research & Social Science 1, 3 (explaining that "VSD ascribes to the idea that technological design process itself can embed values, and that protecting or realizing values is not only a matter of regulation and the management of externalities. This means that designers and design teams bear a large responsibility for translating knowledge about behaviour (sic) and values into technological artefacts.").

[53] Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81, 99–100; Briseida Sofia Jiménez-Gómez, 'Risks of Blockchain for Data Protection: A European Approach' (2020) 36 Santa Clara High Technology Law Journal 281, 313–314 (discussing how developers are in a key position to control blockchain technologies); see generally Roger Brownsword, 'Code, Control, and Choice: Why East is East and West is West' (2005) 25 Legal Studies 1 (discussing regulation through code, also called "techno-regulation").

[54] Kirsten Martin, 'Ethical Implications and Accountability of Algorithms' (2019) 160 Journal of Business Ethics 835, 844 (2019).

[55] *Id.*

[56] Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81, 99–100 citing Briseida Sofia Jiménez-Gómez, 'Risks of Blockchain for Data Protection: A European Approach' (2020) 36 Santa Clara High Tech. L.J. 281, 313.

[57] Barbara Adam and Chris Groves, 'Futures Tended: Care and Future-Oriented Responsibility' (2011) 31 Bulletin of Science, Technology & Society 17.

[58] Barbara Adam and Chris Groves, 'Futures Tended: Care and Future-Oriented Responsibility' (2011) 31 Bulletin of Science, Technology & Society 17, abstract.

that designers should follow a "roadmap" of ethical issues that may arise from the use of the technology under development which considers the "epistemic concerns relating to the quality of evidence upon which a system relies," as well as "normative concerns such as unfair outcomes," and the traceability of decisions.[59] Likewise, technology providers should be expected to adopt a "mindset" by, for example, proactively testing for security vulnerabilities during development and deploying other technical and organizational measures as a way of operationalizing DPbD.[60]

Luger *et al*. have created an approach based on ideation cards to raise data protection issues early within the design process, in an effort to help shift "the locus of responsibility" towards designers and to encourage them to engage with regulatory requirements.[61] Other anticipatory methods could build on ongoing work concerning human rights impact assessments and risk assessments to describe and analyze those "intended and potentially unintended impacts" that a technology might have on data protection rights.[62] These obligations could be combined with a fiduciary duty of care to anticipate and protect the human rights of end users.[63] Furthermore, data protection certifications that demonstrate compliance with DPbD principles are also a possible way to support a proactive, *ex ante* approach to DPbD by technology providers.

4.2 A RELATIONAL CONCEPT

Since DPbD is "a meta requirement"[64] representing the "backbone" of the GDPR,[65] it can be argued that its implementation, by its very nature, requires interaction, dialogue, transparency, and understanding from all actors in the supply chain and all individuals affected by the technology to ensure effective protection of data subjects.[66] As Dignum puts it: "Given the impact AI systems can have on people, inter-personal interactions, and society as a whole, it seems to be relevant to consider a relational stance to approach the specification, development and analysis of AI systems."[67] The GDPR is mainly concerned with the relationship between the data controller and the data subject, although data processors also bear some responsibility for DPbD in relation to both the data subject and the data controller.[68] As mentioned above, technology providers do not have any binding legal responsibility for DPbD to the individual or groups of individuals that are affected by their systems, unless they are classified as a controller or processor. This is true even though they have been recognized as "key enablers" of DPbD because they have greater knowledge about the potential risks that the use of a product or service may involve and are more likely to be familiar with the state of the art.[69]

[59] Heike Felzmann, Eduard Fosch-Villaronga, Christoph Lutz and Aurelia Tamò-Larrieux, 'Towards Transparency by Design for Artificial Intelligence' (2020) 26 Science and Engineering Ethics 3333, 3345–3346 *citing* Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, Luciano Floridi, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 Big Data & Society 1.

[60] *For more, see* Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework* (Springer 2018).

[61] Ewa Luger, Lachlan Urquhart, Tom Rodden, Michael Golembewski, 'Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process' in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (ACM Press 2015) 457–466, 457, 465.

[62] Richard Owen, *From Co-Operative Values to Responsible Innovation*, 11 Projectics / Proyéctica / Projectique 5, 11 (2012), available at https://www.cairn.info/revue-projectique-2012-2-page-5.htm.

[63] *See further* Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, 102 (New York University Press 2004); Danielle Citron, *Big Data Brokers as Fiduciaries*, Concurring Opinions (June 19, 2012), available at https://archive.org/details/perma_cc_82VQ-NX92; Daniel M. Filler *et al*., 'Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data' (2022) 54 Connecticut Law Review 105–149.

[64] Liane Colonna, 'Reconciling Privacy by Design with the Principle of Transparency' in S. de Vries and U. Bernitz (eds.), *General Principles of EU Law and the EU Digital Order* (Kluwer Law International 2020), 405–422, 409.

[65] Michael Birnhack, Eran Toch and Irit Hadar, 'Privacy Mindset, Technological Mindset' (2014) 55 Jurimetrics 55, 65.

[66] See Mark Coeckelbergh, 'Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability' (2020) 26 Science and Engineering Ethics 2051, 2065 (explaining that "A relational approach to responsibility should never be an excuse for evading responsibility but instead should highlight the need for responsible action understood as having the aspects of *interaction*, dialogue, transparency, and understanding…").

[67] Virginia Dignum, *Relational Artificial Intelligence*, 10, available at https://arxiv.org/abs/2202.07446.

[68] For a complete analysis, see Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81.

[69] Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81, 84 *citing* Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020, paragraph 94.

Given the non-linear, complex feedback loops and interactions between algorithms and humans, it is a mistake to focus on the data controller-data subject relationship rather than the entire design system and the relationships and interdependencies within it. The deployment of AI is not a linear process, but involves complex feedback loops and interactions between algorithms and humans to ensure the safety and fairness of algorithms functioning in society.[70] For example, "prospective choices" are made at the design phase and "responsive choices" are subsequently made to improve the original design selections after taking note of how AI performs at the early stages.[71] It is thus possible to reconsider initial design choices after observing how the algorithm functions "in the wild."[72] Given the malleability of software and its need for maintenance, there is also a need to ensure that data controllers are aware of software updates and other forms of technological progress.[73] Throughout this non-linear process, various risks to safety and fundamental rights may emerge. It may be the case that problems occur at the nexus between system design decisions made by technology providers and subsequent decisions made by deploying organizations as to how to use the AI, requiring a broad understanding of responsibility.

Like human intelligence, which evolves continuously, AI develops its accuracy and efficiency for better outcomes. Some AI may also capable of changing as a reaction to an event or behavior, making it highly adaptive.[74] Furthermore, it has an anticipatory nature in that it can foresee certain actions, even before humans.[75] These features demonstrate that AI is not necessarily a static technology, neatly under the control of a single entity.

The AI Act, a new legislative proposal designed to regulate AI, acknowledges the complexity of modern software development and places more responsibility on the actors in the supply chain.[76] First, it defines various actors in the supply chain, such as technology providers, small-scale providers, users, importers, and distributors.[77] Second, it defines the obligations for each of the relevant actors, several of which can be considered DPbD measures, such as the provisions on data governance.[78] Third, it acknowledges the feedback loops that are involved in modern data processing, for example by requiring post-market surveillance.[79] However, the AI Act is largely focused on the technology providers of high-risk AI and, in any event, these providers do not (yet) bear responsibility in direct relationship to the individual. There are neither obligations for providers to consult directly with civil society organizations and affected communities,[80] nor any legal rights built into the law to allow individuals to assert claims against the providers of AI or before an enforcement authority. Basically, the law lacks an approach which ensures that those who are affected or at risk of being affected by AI can bring complaints or rely on other redress mechanisms to hold providers of AI accountable for the technologies that they place

[70] Charlotte A. Tschider, 'Beyond the Black Box' (2021) 98 Denver Law Review 683, 713–14; *see also* Salomé Viljoen, 'A Relational Theory of Data Governance' (2021) 131 Yale Law Journal 573, 607 (discussing a "relational" theory of data governance and distinguishing between "vertical relations" between a particular individual and a data collector, but also "horizontal relations" between the individual and "others that share relevant population features with the data subject."); *see further* forthcoming, Solow-Niederman, Alicia, *Information Privacy and the Inference Economy*, Northwestern University Law Review (September 10, 2021), available at SSRN: https://ssrn.com/abstract=3921003 or http://dx.doi.org/10.2139/ssrn.3921003 (emphasizing the need to "recognize the more complex individual organizational relationships at stake" in the context of AI and setting forth a triangular model in the context of the inference economy).

[71] Charlotte A. Tschider, 'Beyond the Black Box' (2021) 98 Denver Law Review 683, 713–14.

[72] *Id.*

[73] Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81,100.

[74] Alex Mihaildis, Liane Colonna, 'A Methodological Approach to Privacy by Design Within the Context of Lifelogging Technologies' (2020) 46 Rutgers Computer and Technology Law Journal 1–52, 16.

[75] *Id.* at 17.

[76] Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM (2021) 206 final (Apr 21, 2021) (hereinafter "AI Act"), Article 3.

[77] AI Act, Article 3.

[78] AI Act, Article 10.

[79] AI Act, Article 61.

[80] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22 Computer Law Review International 97, 105 (noting that "It is unclear whether limited existing efforts to include stakeholder representation will enable the deep and meaningful engagement needed from affected communities.").

on the market. While there are calls for a more victim-centered approach to be included in the AI Act – in particular, one that encompasses a right to explanation from an AI provider, a right to object to a decision made by AI, and a right to redress if an individual is harmed by AI – it is unclear at this stage in the negotiations whether this will be used in the final law.

Elsewhere, it has been argued that the proposal for an AI Act is overly technocratic and could benefit from broader dialogue and greater engagement with stakeholders to foster more creative strategies to protect people that are harmed, disempowered, or marginalized by AI.[81] In particular, this work found that the AI Act does not sufficiently take into consideration the relationship between providers and AI end users such as the communities that are disproportionally impacted by the technology.[82] The AI Act introduces many requirements on technology providers that supply high-risk AI, such as adherence to strict data governance provisions[83] and risk analyses[84] to be implemented already at the design and development phases, which could protect the data protection rights of individuals. However, it does not fully remedy the responsibility gap between technology providers and end users. This is because it fails to consider the relational perspective between those who provide AI and the end users who are harmed by it.

The failure to hold technology providers responsible to the end users that are ultimately affected by their tools raises a concern that technology providers have too much authority over those tools, producing a power asymmetry between technology creators and users.[85] Delgado *et al*. explain that there is an "…asymmetry of power and knowledge often found in technology development in which computer scientists and designers hold a relative advantage over most other stakeholders."[86] An additional consequence of failing to hold technology providers responsible for the design of their artefacts is that technology providers tend to think in abstract and formalist ways rather than more broadly about the sociotechnical framework.[87] Existing and novel ways of placing responsibility on technology providers for the designs they create must be considered, especially vis-à-vis their obligations to the end users. This could alleviate some of the concerns described above and alter power relationships.[88]

If a technology provider operates too far downstream in the supply chain to be a controller or processor under the GDPR and cannot be held responsible for DPbD to the end user, it should still have a responsibility to meet certain standards or requirements that further the goals of data protection. It should also support controllers to meet their DPbD obligations. This could be enforced by supervisory authorities. There has already been a serious discussion about requiring technology providers to assist data controllers to stay up to date with the "state of the art" of technology development, so that controllers can understand the effectiveness of any DPbD measures that are put in place during the lifespan of the technology.[89] Here, despite the lack

[81] Liane Colonna, 'Artificial Intelligence in Higher Education: Towards a More Relational Approach' (2022) 8 Loyola University Chicago Journal of Regulatory Compliance 18.

[82] *Id.* at 54.

[83] AI Act, Article 10.

[84] AI Act, Article 9.

[85] *See* Ari Ezra Waldman, 'Privacy's Law of Design' (2019) 9 UC Irvine Law Review 1239, 1244.

[86] Fernando Delgado, Solon Barocas, Karen Levy, *An Uncommon Task: Participatory Design in Legal AI*, In: Proceedings of the ACM on Human-Computer Interaction, 6, CSCW1, Article 51, 1–22, 5 (April 2022), https://arxiv.org/ftp/arxiv/papers/2203/2203.06246.pdf*; see also* Ari Ezra Waldman, 'Privacy's Law of Design' (2019) 9 UC Irvine Law Review 1239, 1244.

[87] Ben Green and Salomé Viljoen, 'Algorithmic Realism: Expanding the Boundaries of Algorithmic Thought' in: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20), 19–31, 23 (explaining, "…a significant risk of algorithmic formalism is that it contributes to formal methods dominating and crowding out other forms of knowledge and inquiry (particularly local forms of situated knowledge) that may be better equipped to the tasks at hand"); Andrew D. Selbst, Danah Boyd, Sorelle A. Friedler, Suresh Venkatasubramanian, Janet Vertesi, 'Fairness and Abstraction in Sociotechnical Systems' in Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT* '19), 59–68, 63 (stating, "…the social must be considered alongside the technical in any design enterprise.").

[88] Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81, 89.

[89] Guidelines of the European Data Protection Board on Data Protection and Design (Oct 20, 2020), available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en at para. 96 (stating that "Producers and processors should play an active role in ensuring that the criteria for the "state of the art" are met, and notify controllers of any changes to the "state of the art" that may affect the effectiveness of the measures they have in place. Controllers should include this requirement as a contractual clause to make sure they are kept up to date"); see also Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81,100–102.

of any binding legal obligation, the European Data Protection Board contends that technology providers should assist data controllers in staying updated about technological progress.[90] The European Data Protection Board suggests that this obligation could gain the force of law, if controllers include the requirement as a contractual clause.[91]

An even wider exchange of technical information to support DPbD can be imagined. Understanding technical information about, for example, the specific technique(s) utilized by the system, such as machine learning, the environment the system is designed to be used in, such as publicly accessible spaces, and the outputs generated by the system, may support actors further along in the supply chain to deploy the system in contexts that are not offensive to privacy or other fundamental rights. Here, a broad disclosure of key technical information can facilitate DPbD by assisting upstream actors to better assess the impact that the technology may have on data protection and provide technical and organizational measures to minimize the effects on individuals' rights. It could further assist different actors within the supply chain to better understand the legal obligations in regard to DPbD and more appropriately define who is in the best position to meet these obligations.[92]

In the proposed AI Act, there is already a requirement to exchange technical information to support the development of responsible AI across the value chain. According to Article 11, the providers of high-risk systems need to create technical documentation containing, at a minimum, the information listed in Annex IV to demonstrate the technology's conformity to supervisory authorities. The technical information required to be provided is extensive and includes, for example, the system's intended purpose, versions of relevant software or firmware, and user instructions.[93] Additionally, according to Article 60, providers must register some of this information, such as the description of the intended purpose of the AI system, in an public EU database.[94] Users also have a right to some of the information under the transparency requirements set forth in Article 13.

As noted above, the AI Act is limited in scope to high-risk AI and is therefore insufficient on its own as a mechanism to achieve the level of information exchange necessary to truly support DPbD within the supply chain. Additionally, the most extensive technical information exchange only happens between the provider and the regulator, not between actors within the supply chain or end users. Nevertheless, even if high-risk AI is not involved and the AI Act is not applicable, a requirement on the exchange of technical documentation to support DPbD could be incorporated as a contractual obligation between actors in the value chain. A requirement on the technical exchange of information may even be conceived as a safety requirement under product liability rules, at least to the extent that providing such information may make the technology safer by avoiding some of the dangers of a privacy-intrusive technology. At the very least, standards on technical documentation which can act as soft law instruments should be adopted.

Lastly, it is important to mention that a further route to imposing DPbD requirements onto technology providers to increase their responsibility towards end users may exist within the context of cybersecurity regulation. The recently proposed Cyber Security Resilience Act, like the proposed AI Act, will directly regulate technology providers by imposing requirements regarding products with digital elements, throughout their entire lifecycle.[95] Since this proposal is at an early stage of negotiation, it may be possible to include DPbD requirements, at least those related to information security, as part of the essential requirements of the law and thereby help upstream users of the technologies, such as data controllers, to meet their obligations under the GDPR.

[90] Guidelines of the European Data Protection Board on Data Protection and Design (Oct 20, 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en, para. 96.

[91] Id.

[92] Alex Engler, Andrea Renda, *Reconciling the AI Value Chain with the EU's Artificial Intelligence Act*, CEPS (30 SEPT 2022), 24, available at https://www.ceps.eu/ceps-publications/reconciling-the-ai-value-chain-with-the-eus-artificial-intelligence-act/#:~:text=Reconciling%20the%20AI%20Value%20Chain%20with%20the%20EU's%20Artificial%20Intelligence%20Act,-Alex%20Engler%20%2F%20Andrea&text=The%20EU%20Artificial%20Intelligence%20Act,and%20to%20mitigate%20its%20risks.

[93] AI Act, Annex IV(1).

[94] AI Act, Article 60 and Annex VIII (5).

[95] Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 ("Cyber Resilience Act"), Brussels, 15.9.2022 COM(2022) 454 final 2022/0272 (COD).

4.3 A DISTRIBUTED CONCEPT

While acknowledging that there are great controversies concerning the concept of responsibility, and the preconditions to assigning responsibility, this paper contends that a traditional prerequisite to legal responsibility at least includes causality.[96] Black's Law Dictionary defines causation as: "the producing of an effect."[97] Within the specific context of AI and law, Greenstein states that "…a central tenet of the law is that there must be a causal link between an act and the damages or crime."[98] In short, causality implies that a given agent is somehow causally involved in the action or outcome for which it is held responsible.[99]

The idea of causality is bound up in the liability model which is "the most common model of assigning responsibility" in law.[100] It derives from legal reasoning employed to establish guilt or fault for a harm.[101] Young explains that "[u]nder this liability model, one assigns responsibility to a particular agent (or agents) whose actions can be shown to be causally connected to the circumstances for which responsibility is sought."[102] Basically, an actor is held responsible for a specific outcome because there is evidence that they directly contributed to it.

To hold a controller liable under the GDPR, it is a requirement to establish a causal relationship between an unlawful act (i.e., an act incompatible with the requirements of the GDPR such as Article 25) and the existence of incurred damages.[103] Article 82 explicitly states that damages must be "a result of" an infringement of the law to have a right to compensation and liability. Chamberlain and Reichel explain that causality is "inherent in the GDPR's wording."[104]

Ostensibly, a central reason why technology providers are not held responsible for DPbD is because of a lack of causal connections between them and those that are harmed by the technological artefacts they create. First, it can be argued that technology providers should be absolved of responsibility because of the multi-stability of technologies, an idea proposed by Ihde, which refers explicitly to the unpredictable uses of technology that differ from the originally intended ones.[105] According to this line of reasoning, technology providers cannot foresee all the possible uses and misuses of the tools they create (and build safeguards into the system to prevent harms to individual rights to data protection and privacy) because they lack a full awareness of the technology's ultimate context of use.[106] For example, FRT developed for

[96] Aimee van Wynsberghe, 'Responsible Robotics and Responsibility Attribution' in Joachim von Braun, Margaret S. Archer, Gregory M. Reichberg, Marcelo Sánchez Sorondo (eds.), *Robotics, AI, and Humanity* (Springer Cham 2021), 239–249, 243; *see further* Tomer Shadmy, 'Superheroes' Regulation: Human Rights Responsibilities As A Source of Transnational Authority' (2018) 43 North Carolina Journal of International Law 130, 145–51 (explaining, "In the legal arena, the term "responsibility" is usually used retrospectively. It identifies the subject of a legal proceeding--the responsible party. In this context, responsibility is a combination between accountability, causation, and capability. To say one is legally responsible means that she should be accountable for a certain previous act or a state of affairs; that she is capable of being party to the proceedings (i.e., she is legally competent); and also that there is a causal relationship between the party's activity and the harm. (internal citations removed)").

[97] Causation, Black's Law Dictionary (11th ed. 2019).

[98] Stanley Greenstein, 'Liability in the Era of Artificial Intelligence' in Liane Colonna and Stanley Greenstein (eds.) 2020–2021 Nordic Yearbook – Law in the Era of Artificial Intelligence (The Swedish Law and Informatics Research Institute (IRI) 2022), 185–205, 195.

[99] Ibo van de Poel and Jessica Nihlén Fahlquist, 'Risk and Responsibility' in Sabine Roeser, Rafaela Hillerbrand, Per Sandin, Martin Peterson (eds.) Handbook of Risk Theory (Springer Dordrecht 2012), 877–907, 115.

[100] Iris Marion Young, 'Responsibility and Global Justice: A Social Connection Model' (2006) 23 Social Philosophy and Policy 102, 116.

[101] *Id.*

[102] *Id.*

[103] Brendan Van Alsenoy, 'Liability Under EU Data Protection Law from Directive 95/46 to the General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 271–288, 274.

[104] Johanna Chamberlain and Jane Reichel, 'The Relationship Between Damages and Administrative Fines in the Eu General Data Protection Regulation' (2020) 89 Mississippi Law Journal 667, 679.

[105] Don Ihde, Technology and the Lifeworld: From Garden to Earth 1–22 (Indiana University Press 1993); Mireille Hildebrandt, 'Profiling and the Rule of Law' (2009) 1 Identity in the Information Society 55–70, 67; Andrew D. Selbst, Danah Boyd, Sorelle A. Friedler, Suresh Venkatasubramanian, Janet Vertesi, *Fairness and Abstraction in Sociotechnical Systems*, In: Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT* '19), 59–68 (explaining that "When a technology is inserted into a social context, it has both intended and unintended consequences. Chief among the unintended consequences are the ways in which people and organizations in the system will respond to the intervention.").

[106] *For more, see* Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford Law Books 2010).

medical purposes like health monitoring can be used for surveillance purposes by public and private actors alike.[107]

Second, the modular nature of modern software development adds further complexity and suggests a lack of coordination between actors concerning design requirements, making it more difficult to establish a clear link between the technology provider and the harm. In addition to open-source software, general purpose AI may be used which allows an across-the-board, foundational AI model to be applied in more specific applications by "fine tuning" the model.[108] Multiple AI models provided by different technology providers may also be used to create a new kind of AI, like the exam proctoring software referred to at the outset of this article. Franssen explains how "sociotechnical systems are hardly if ever designed and implemented as a whole and from scratch," but rather "are extended through design: they grow almost organically by having designed modules added to them or by having parts of the system replaced by designed modules."[109] Here, there is a lack of evidence that can establish or ascribe responsibility when it comes to technology providers. Often, no legal relationships are defined between various actors in the supply chain, for example in the form of a contract, particularly where open source code is relied upon. Wallach makes the following point: "As systems become more complex, it is extremely difficult to establish blame when something does go wrong."[110]

Third, it is important to highlight that causation in law is often considered a linear phenomenon.[111] However, as described above, AI is often built on feedback loops between numerous stakeholders, which makes it hard to conclude, based on facts or other evidence, that a certain technology provider had a decisive role in causing the harm.[112] The interdependence of AI components as well as the semi-autonomous and evolving nature of AI are also relevant as they make it very difficult to squarely attribute liability – unpredictable little problems can cascade into larger ones.[113]

Fourth, the opacity of certain kinds of AI makes it challenging to identify what exactly caused the harm. It is often the case that the technology providers cannot understand how input data results in a specific decision,[114] although significant work is being done on the issue of transparency in AI.[115] The Expert Group on Liability explains that: "The more complex emerging

[107] Mark Coeckelbergh, 'Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability' (2020) 26 Science and Engineering Ethics 2051, 2057 (explaining that "AI software may … be developed in and for one context of application, but later used in an entirely different context of applications. For example, in principle "medical" face recognition software can also be used for surveillance purposes and become "police" AI.").

[108] Future of Life, *General Purpose AI and the AI Act*, available at https://artificialintelligenceact.eu/wp-content/uploads/2022/05/General-Purpose-AI-and-the-AI-Act.pdf.

[109] M. Franssen, 'Design for Values and Operator Roles in Sociotechnical Systems' in J. van den Hoven, P. Vermaas, I. van de Poel (eds.)), *Handbook of Ethics, Values, and Technological Design* (Springer Dordrecht 2014), 117–149, 123; Mark A Chinen, 'The Co-Evolution of Autonomous Machines and Legal Responsibility' (2016) 20 Virginia Journal of Law and Technology 338, 345 (explaining that "… a growing reality in which the machines and systems in question are designed and manufactured by large organizations or through long supply chains in which sophisticated machines are already being used and in which such new machines will operate in systems or organizations of which people are also a part.); *see also* Seda Gurses and Joris van Hoboken, 'Privacy after the Agile Turn' in Jules Polonetsky, Omer Tene and Evan Selinger (eds.), Cambridge Handbook of Consumer Privacy (Cambridge University Press 2017).

[110] Wendell Wallach, Colin Allen, *Moral Machines: Teaching Robots Right From Wrong* (Oxford University Press 2009), 198.

[111] Stanley Greenstein, 'Liability in the Era of Artificial Intelligence' in Liane Colonna and Stanley Greenstein (eds.) 2020–2021 Nordic Yearbook – Law in the Era of Artificial Intelligence (The Swedish Law and Informatics Research Institute (IRI) 2022), 185–205, 197.

[112] Barbara Adam and Chris Groves, 'Futures Tended: Care and Future-Oriented Responsibility' (2011) 31 Bulletin of Science, Technology & Society 17, 18.

[113] Miriam Buiten, Alexandre De Streel, Martin Peitz, *EU Liability Rules for the Age of Artificial Intelligence*, Center on Regulation in Europe Report (2021), 1–72, 26 https://cerre.eu/publications/eu-liability-rules-age-of-artificial-intelligence-ai/.

[114] Miriam Buiten, Alexandre De Streel, Martin Peitz, *EU Liability Rules for the Age of Artificial Intelligence, Center on Regulation in Europe Report* (2021), 1–72, 27 https://cerre.eu/publications/eu-liability-rules-age-of-artificial-intelligence-ai/.

[115] *See, e.g.,* Bernhard Waltl and Roland Vogl, 'Increasing Transparency in Algorithmic Decision-Making with Explainable AI' (2018) 42 Datenschutz Datensich 613 (2018); Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31 Harvard Journal of Law & Technology 841; Chris Reed, Keri Grieman, Joseph Early, 'Non-Asimov Explanations Regulating AI through Transparency' in Liane Colonna and Stanley Greenstein (eds.), *2020–2021 Nordic Yearbook – Law in the Era of Artificial Intelligence* (The Swedish Law and Informatics Research Institute 2022).

digital technologies become, the less those taking advantage of their functions or being exposed to them can comprehend the processes that may have caused harm to themselves or to others" which makes it "… increasingly difficult for victims to identify such technologies as even a possible source of harm, let alone why they have caused it."[116] Basically, the "black box" nature of certain AI challenges a fundamental requirement of law, namely the identification of a chain of causation between fault and harm, making it difficult to identify a single, culpable party.

Ultimately, the timeline of events or sequence of facts leading up to a data protection infringement like the one described at the outset of this article is very complicated. While there have been many "different methods of solving causation issues" incorporated into the law over the years, it is unclear whether they will be able to "deal with the complexity of AI technologies."[117] For example, there are certain judicial constructs and principles that can be used to alleviate the evidentiary burden of the data subject.[118] These constructs include, for example, the principles of "proof proximity" and *res ipsa loquitur* ("the thing speaks for itself"), and acknowledge that the relevant evidence for a data subject's claim is often held by a data controller and allow the data subject's claim to move forward even if they lack solid evidence to substantiate the claim.[119] However, it is not at all certain that the data subject will be able "to avail him- or herself of a particular presumption or construct," especially given that each Member State may have different legal rules.[120] Highlighting the complexity of AI, Greenstein argues that it will be increasingly difficult to explain what caused a particular harm as "there may be multiple factors that are relevant in connection with the damage and who was actually in control of what part of the technology may be rather blurry."[121]

One potential response to these challenges is for policymakers and judges to move away from the liability model and apply a more distributed approach to responsibility. Distributed responsibility is a concept that has been brought forward by contemporary philosophers such as Floridi and Simon.[122] It confronts the idea that it is possible to locate a single agent that is solely responsible for causing a particular outcome in a world that is increasingly mediated by digital technologies, electronic networks, and reliance on algorithmic decision-making.[123] Instead, it suggests that responsibility is inextricably interwoven between multiple actors and technologies operating in a complex sociotechnical system of systems.[124]

If one considers DPbD, there are many different places where responsibility may lie. Within the supply chain, there are various actors making decisions about data and algorithmic design, and system development. Sensors and other types of hardware with various electronic components may be involved. There will be some use of information networks and various data storage

[116] European Commission, Directorate-General for Justice and Consumers, *Liability for Artificial Intelligence and Other Emerging Digital Technologies* (Publications Office 2019) 1–65, 33 https://data.europa.eu/doi/10.2838/573689.

[117] Stanley Greenstein, 'Liability in the Era of Artificial Intelligence' in Liane Colonna and Stanley Greenstein (eds.), *2020–2021 Nordic Yearbook – Law in the Era of Artificial Intelligence* (The Swedish Law and Informatics Research Institute (IRI) 2022), 185–205, 196.

[118] Brendan Van Alsenoy, 'Liability Under EU Data Protection Law from Directive 95/46 to the General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 271–288, 275; *see also* Proposal for a Directive of the European Parliament and of the Council on adapting non contractual civil liability rules to artificial intelligence, European Commission, COM(2022) 496 final, 2022 ('AI Liability Directive') (containing rules to alleviate the burden of proof in relation to damage caused by AI systems under certain circumstances).

[119] Brendan Van Alsenoy, 'Liability Under EU Data Protection Law from Directive 95/46 to the General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 271–288, 275–276.

[120] *Id* at 276.

[121] Stanley Greenstein, 'Liability in the Era of Artificial Intelligence' in Liane Colonna and Stanley Greenstein (eds.) *2020–2021 Nordic Yearbook – Law in the Era of Artificial Intelligence* (The Swedish Law and Informatics Research Institute 2022), 185–205, 196.

[122] Luciano Floridi, 'Distributed Morality in an Information Society' (2012) 19 Science & Engineering Ethics 727, 728; *see also* Judith Simon, 'Distributed Epistemic Responsibility in a Hyperconnected Era' in Luciano Floridi (ed.) *The Onlife Manifesto* (Springer Cham 2015) 145–159.

[123] *Id.*

[124] Mark Coeckelbergh, 'Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability' (2020) 26 Science and Engineering Ethics 2051, 2056 citing M. Taddeo and L. Floridi, How AI Can Be a Force For Good (2018) 361 Science 751–752, 751 (stating that "The effects of decisions or actions based on AI are often the result of countless interactions among many actors, including designers, developers, users, software, and hardware…. With distributed agency comes distributed responsibility.").

models. User interfaces also have a key role in DPbD. All these actors are dependent on each other to ensure that data protection principles are respected in the design and, as explained above, there are important feedback loops between actors that inform the design process. The existence of all these different actors gives rise to a distributed responsibility for DPbD "where multiple, temporally distributed, actors, often in heterogeneous organizations and roles," each bear some level of influence on the data protection outcomes of an AI system.[125]

The growing case law of the Court of Justice of the European Union (CJEU), which significantly expands the notion of the data controller, shows how the distribution of agency in modern sociotechnical systems confounds and frustrates existing legal doctrine. In fact, it appears that the CJEU is already adopting a distributed approach to responsibility to the extent that it has defined an increasing number of actors in the supply chain as joint data controllers and thus made them responsible for all requirements under the GDPR, including DPbD.[126] While a substantial discussion of the case law is outside the scope of this article,[127] it can broadly be stated that the cases reflect a trend whereby the CJEU has examined data processing chains and found a broad category of actors to be joint controllers.[128] Generally, the Court is focused on holding those parties responsible to the extent that they share in the economic or commercial benefits.[129] The extension of the notion of "data controller" has been justified by the Court in the interest of ensuring "the effective and complete protection of data subjects."[130]

As regards DPbD, broadly defining the concept of a data controller to include more actors in the supply chain is problematic for numerous reasons. First, actors that may have only a very tenuous connection to the data processing can be held entirely responsible for meeting all of the requirements of the GDPR, including DPbD.[131] Millard explains that this may severely undermine "the essential nexus between responsibility and control."[132] Second, as explained in greater detail below, there is a lack of sound methodological approaches for dividing responsibility between joint data controllers, which suggests that a different way of conceptualizing distributed responsibility for DPbD may be more appropriate.

A better way to encourage a distributed responsibility for DPbD may exist under liability law, for instance regarding product liability and safety regulations. These instruments may be more adequately suited to address the downstream regulation of technology providers by ensuring that certain data protection design strategies and patterns are considered early in development. Here, Waldman argues that the application of product liability law could be used to inspire greater responsibility for technology providers to adopt DPbD strategies, helping to reduce the power asymmetry that exists between technology providers and end users.[133] He contends that a regime based on product liability "is less susceptible to legal endogeneity than compliance-based approaches because of the powerful role litigation and courts can play in influencing design across an entire industry."[134] In particular, he suggests that technology companies should be required, throughout a product's or service's lifecycle, to balance the benefits of the product or service to consumers against their foreseeable privacy risks and "only place in commerce those products that achieve reasonably similar consumer benefit with the least privacy risk."[135]

[125] S.C. Slota, K.R. Fleischmann, S. Greenberg, et al., 'Many Hands Make Many Fingers to Point: Challenges in Creating Accountable AI' (2021) AI & Society, 2.

[126] For a detailed discussion of the CJEU's expansive approach towards controllership, *see* Michèle Finck, 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU law' (2021) 11 International Data Privacy Law 33.

[127] *But see* Jennifer Cobbe and Jatinder Singh, 'Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges' (2021) 42 Computer Law & Security Review 1.

[128] *See,* e.g., Case C-2010/16, Wirtschaftsakademie Schleswig-Holstein (2018), ECLI:EU:C:2018:388; Case C-25/17 Jehovan todistajat (2018) ECLI:EU:C:2018:551; Case C-40/17 Fashion ID 2019 ECLI:EU:C:2019:629.

[129] Case C-40/17 Fashion ID 2019 ECLI:EU:C:2019:629, para. 80.

[130] Judgment in Wirtschaftsakademie, C-210/16, ECLI:EU:C:2018:388 para. 28 (citing Case C-131/12, Google Spain and Google, ECLI:EU:C:2014:317).

[131] Christopher Millard, 'At This Rate, Everyone Will Be A [Joint] Controller of Personal Data!' (2019) 9 International Data Privacy Law 217, 217.

[132] *Id.*

[133] Ari Ezra Waldman, 'Privacy's Law of Design' (2019) 9 UC Irvine Law Review 1239, 1263–82.

[134] Ari Ezra Waldman, 'Privacy Law's False Promise' (2020) 97 Washing University Law Review 773, 826.

[135] Ari Ezra Waldman, 'Safe Social Spaces' (2019) 96 Washing University Law Review 1537, 1577.

5 THE PRACTICAL PROBLEM OF DISTRIBUTION OF RESPONSIBILITY

Distributed responsibility suggests that no one is singularly at fault, but rather that different agents share "partial responsibility" for an outcome.[136] If the concept is adopted by courts, the more complex question then becomes to what extent an entity can be held responsible for DPbD. That is, even if a court finds that a technology provider bears some legal responsibility, for example, by broadly interpreting the concept of "data controller," it is unclear how it should divide DPbD obligations. Even if many actors and technical agents might contribute to an outcome, this does not necessarily mean that they should all bear equal responsibility for a particular outcome.[137] Coeckelbergh explains that "…it is clear that distributed responsibility does not imply that responsibility is and should always be distributed equally."[138]

In principle, Article 82 of the GDPR gives any individual that suffers material or non-material damage resulting from an infringement of the law a right to compensation.[139] Article 82(4) establishes joint and several liability for joint controllers,[140] although a joint controller that pays all of the compensation for the damages suffered can subsequently claim back that money from the other joint controllers.[141] Where it concerns indemnification, a joint controller can reclaim funds from other joint controllers "corresponding to their part of responsibility for the damage."[142]

Article 82(3) further exempts a controller from liability if it can prove that it is not in any way responsible for the event giving rise to the damage. Van Alsenoy explains that for a joint controller to prove that it is not responsible for the event that gave rise to a data protection harm, the controller must demonstrate three things: first, the occurrence of a particular event; second, that this caused the damage; and third, that it cannot be attributed to the controller.[143] Types of events that are "beyond a controller's field of action," include a "force majeure event" that consists of "abnormal occurrences which cannot be foreseen and avoided by any reasonable means."[144]

Recital 146 of the GDPR clarifies that "[t]he concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation." However, the CJEU has had very few occasions to comment on precisely how damages should be apportioned, although a judgement in *Österreichische Post* expected soon.[145] This case is discussed in greater detail below. The definition and calculation of recoverable damages is generally a matter for the national courts of each Member State. As the GDPR is silent on what method to use to calculate damages, Member States are free to formulate their own rules, as long as they respect the principles of equivalence and

[136] Alexandra Kapeller, Heike Felzmann, Eduard Fosch-Villaronga & Ann-Marie Hughes, 'A Taxonomy of Ethical, Legal and Social Implications of Wearable Robots: An Expert Perspective' (2020) 26 Science and Engineering Ethics volume 3229, 3239.

[137] Laura Cabrera and Jennifer Carter-Johnson, 'Emergent Neurotechnologies and Challenges to Responsibility Frameworks' (2020) 54 Akron Law Review 1, 16 ("If several persons share responsibility for what happens as a result of what they have done, what factors affect the degree to which each person involved is responsible for the outcome? While several individuals might be involved in the outcome, it is not clear that each have equal degrees of responsibility. …").

[138] Mark Coeckelbergh, 'Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability' (2020) 26 Science and Engineering Ethics 2051, 2056.

[139] GDPR, Article 82; *see also* Mona Naomi Lintvedt, 'Putting a Price on Data Protection Infringement' (2021) 12 International Data Privacy Law 1, 12.

[140] GDPR, Article 82(4) ("Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are… responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.").

[141] GDPR, Article 82 (5).

[142] GDPR, Article 82 (5).

[143] Brendan Van Alsenoy, 'Liability Under EU Data Protection Law from Directive 95/46 to the General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 271–288, 276.

[144] Arianna Alessi, Giuseppe Ciccarelli, Luca Cipolli, Lara Guidotti, Annalisa Marsano, *Privacy by Design and by Default in Software Development in Order to Prevent Unlawful Processing of Personal Data* in: e-Legal Game Digital edition 2020–2021, 1–56, 37, www.enel.com/content/dam/enel-com/documenti/e-legal-game/19-privacy-design-default-software-development-order-prevent-unlawful-e-legal-int.pdf.

[145] Case C-300/21: Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021—UI v Österreichische Post AG. OJ C 320, 9.8.2021, pp 25–26.

effectiveness.[146] Walree and Wolters highlight that national rules might lead to differences in the enforcement of data protection law.[147]

Arguably, distributing responsibility means placing proportionate obligations on relevant actors so if one actor had a bigger role in causing the harm or could more easily have prevented it, it should bear more legal responsibility.[148] This is consistent with Article 82 and the CJEU's case law on joint controllership where it has made clear that "the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data" and that "those operators may be involved at *different stages* of that processing of personal data and to *different degrees*, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case."[149] This approach, first announced in *Wirtschaftsakademie,* has been reaffirmed by the CJEU in numerous other cases.[150]

While the CJEU has concluded that joint data controllers may have "different degrees" of responsibility,[151] it has yet to offer consistent and explicit methodological advice regarding how to define the shares of responsibility.[152] Methodological approaches to apportioning responsibility are necessary but difficult to define, as it may not be obvious how the various parties interacted and how each specifically contributed to a given outcome.[153] This is especially true in the case of data processing, which often happens "behind closed doors."[154]

Contractual solutions offer a key mechanism for various actors in the supply chain to allocate responsibilities to those agents that can best ensure compliance. The various actors should have the freedom to allocate responsibilities through contractual obligations. Indeed, the GDPR presupposes that joint data controllers create arrangements on how to apportion responsibility, such as a joint controllership contract.[155] Likewise, contractual solutions may be a mechanism for technology providers to assist data controllers to "stay up to date" regarding the state of the art.[156] Since

[146] Gabriela Zanfir-Fortuna, 'Article 82: Right to Compensation and Liability' in Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020), 1160–1179, 1173–74 (further explaining, "…any application of liability rules by national courts must comply and align with the conditions set out in Article 82, even when they contradict or supplement the law and practice of non-contractual liability in the national legal systems concerned.").

[147] Tim F. Walree and Pieter T. J. Wolters, 'The Right to Compensation of a Competitor for a Violation of the GDPR' (2020) 10 International Data Privacy Law 346, 352.

[148] *See* Jiahong Chen, Lilian Edwards, Lachlan Urquhart, Derek McAuley, 'Who is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10 International Data Privacy Law 279–293, 291 (explaining that it is "…reasonable and necessary to differentiate the obligations of different controllers taking into account their respective roles in the whole process of determining the purposes and means of data processing" but discussing the methodological challenges of doing this in practice).

[149] Judgment in Wirtschaftsakademie, C-210/16, ECLI:EU:C:2018:388, para. 43.

[150] Case C-25/17, Tietosuojavaltuutettu v. Jehovan todistajat-- uskonnollinen yhdyskunta, ECLI:EU:C:2018:551, para 66; Case C-40/17 FashionID GmbH & Co. KG v Verbraucherzentrale NRW e.V. (2019), para 70.

[151] Judgment in Wirtschaftsakademie, C-210/16, ECLI:EU:C:2018:388, paragraph 43 ("operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case"): see also Case C-25/17, Tietosuojavaltuutettu v. Jehovan todistajat-- uskonnollinen yhdyskunta, ECLI:EU:C:2018:551 (July 10, 2018), para 66, 73.

[152] R. Mahieu, J. Hoboken, and H. Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and Its Application to Data Access Rights in Europe' (2019) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 1, 85–105, 95–97; Jiahong Chen, Lilian Edwards, Lachlan Urquhart, Derek McAuley, 'Who is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10 International Data Privacy Law 279–293, 291.

[153] Mark Coeckelbergh, Artificial Intelligence, 'Responsibility Attribution, and a Relational Justification of Explainability' (2020) 26 Science and Engineering Ethics 2051, 2056 (discussing "distributed responsibility" as "a good conceptual solution to the problem of many hands" yet "acknowledging the distributed character of responsibility in the case of AI does not solve the practical problem of how to distribute the responsibility, given that one may not know (the extent of) all the contributions and interactions, and given a number of other challenges.").

[154] Paolo Pontoniere, *What Your Doormat, Body Odor, or Wandering Gaze Can Tell Us that We Don't Already Know*, https://neo.life/2022/01/biometrics-on-the-rise/ (quoting Jacob Leon Kröger, a researcher at the Berlin-based Weizenbaum Institute for the Networked Society, "In the corporate world, data processing and analysis methods are usually developed and applied behind closed doors. They are considered trade secrets and not revealed to the public…").

[155] GDPR, Articles 26(3), 82(4); *see also* Art 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010) 00264/10/EN WP 169. Page 22.

[156] Guidelines of the European Data Protection Board on Data Protection and Design, para. 96 (Oct 20, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

data processing and analysis methods are often kept private to create a competitive advantage, it may be a good approach to let those that have a front row seat to the activities decide among themselves how to share the responsibilities. It can further be noted that this practice is already used in the provision of medical drugs and devices, where technology providers enter into "Quality Agreements" with the regulated entity in order to define expectations and responsibilities.[157]

However, a problem with apportioning responsibility based on the existence of legal agreements, is that case law shows that a joint controllership can exist where no such agreement has been made.[158] This might occur, for example, where a joint controllership arises as a result of technical or organizational configurations rather than an explicit legal arrangement between the concerned parties.[159] In this situation, which might occur in the context of open source development, for instance, it is especially difficult to apportion relative legal responsibility among the different actors.[160]

Where the existence of a legal agreement is lacking, yet legal responsibility remains, one way to apportion responsibility is to focus on ability.[161] In the *Google Spain* case, the CJEU found that a search engine that is classified as a data controller is responsible for obligations under the Data Protection Directive only to the extent that it has the "responsibilities, powers and capabilities," to meet the legal obligations set forth in the law.[162] While the CJEU used the notion of "responsibilities, powers and capabilities" to limit the controllership of Google Spain to those data processing activities that it carried out on its own accord, the Court's practical approach to understanding the responsibilities of controllers in a technologically complex world could be expanded. To put it differently, an ability criterion could be used to limit the requirements of DPbD to those actors that are in a position to control the way that personal data are processed and to design the system in the most privacy-preserving manner possible. Relevant considerations might include the complete lifecycle of personal data processing as well as who is in the best position to safeguard the rights of the data subject at the lowest cost (e.g., the "cheapest cost avoider"),[163] especially considering the foreseeable uses and misuses of the technology.

Importantly, the "responsibilities, powers and capabilities" approach can be contrasted to the approach taken by the CJEU in subsequent case law. This has focused on breaking up complex data processing operations into distinct phases or steps, and apportioning responsibility based on the specific phase or step of involvement.[164] Elsewhere, it has been argued that the CJEU should adopt an ability approach based on a factual examination of who has the power and capacity to implement DPbD.[165] This would be "a more holistic, balanced, and common-sense approach" that could include considerations like adherence to standards.[166]

[157] *See, e.g.,* FDA, U.S. Dep't of Health & Human Servs., *Contract Manufacturing Arrangements for Drugs: Quality Agreements, Guidance for Industry*, 1–15, 5 (2016), https://www.fda.gov/media/86193/download.

[158] Jiahong Chen, Lilian Edwards, Lachlan Urquhart, Derek McAuley, 'Who is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10 International Data Privacy Law 279, 291.

[159] *Id.*

[160] *Id.*

[161] Erik Persson & Maria Hedlund, 'The Future of AI in Our Hands? To What Extent Are We as Individuals Morally Responsible for Guiding the Development of AI in a Desirable Direction?' (2022) 2 AI Ethics 683, 689–690.

[162] Judgement in Google Spain, C-131/12, EU:C:2014:317, para. 38.

[163] Guido Calabresi and Jon T. Hirschoff, 'Toward a Test for Strict Liability in Torts' (1972) 81 Yale Law Journal 1055, 1060.

[164] René Mahieu and Joris van Hoboken, *Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?*, European Law Blog (2019), https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/; *see also* Yordanka Ivanova, 'Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World' in M. Tzanou (ed) Personal Data Protection and Legal Developments in the European Union (IGI Global, 2020), 61, 83.

[165] Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81; *see further* Yordanka Ivanova, 'Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World' in M. Tzanou (ed) Personal Data Protection and Legal Developments in the European Union (IGI Global, 2020), 61, 83.

[166] Liane Colonna, 'Implementing Data Protection by Design in the Ed Tech Context: What is the Role of Technology Providers?' (2022) 13 Case Western Journal of Law, Technology & the Internet 81, 105; Yordanka Ivanova, 'Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World' in M. Tzanou (ed) Personal Data Protection and Legal Developments in the European Union (IGI Global, 2020), 61, 83.

Another complication concerns the harm requirement. If DPbD is conceived of as a prospective responsibility and a proactive requirement, then there may not be any actual material or non-material harm to the data subject. Instead, the harm may simply be potential, as DPbD is a future-oriented, *ex ante* requirement. It is unclear whether it is sufficient to bring a claim based on Article 82 without material harm, for instance for significant emotional damage or personal impairment.

The question of whether a claim for damages can be brought by a data subject based merely on the fact that the provisions of the GDPR have been infringed has recently been referred to the CJEU in *Österreichische Post*. More specifically, the Austrian Supreme Court has referred a question to the CJEU about whether the award of compensation under Article 82 requires that an applicant has suffered harm, in addition to an infringement of the GDPR having occurred.[167] To put it differently, the question concerns whether a data subject can receive compensation for solely general preventive reasons.[168]

On 6 October 2022, Advocate General Campos Sánchez-Bordona delivered his opinion in Österreichische *Post*, suggesting that compensation claims under the GDPR should be restricted to cases of actual material or non-material damage.[169] In commenting on what actual material or non-material damage means in practice, the Advocate General explained that the general definition of damage "must be broad" but, at the same time, cannot create a rule under which "all non-material damage, regardless of how serious it is, is eligible for compensation."[170] However, if the CJEU ultimately rejects this reasoning and determines that a data subject does not need to suffer harm beyond the mere infringement of Article 25, this may further complicate the question of how to apportion responsibility within the supply chain. This is because courts will need to assess theoretical harms that have not yet materialized

6 CONCLUSION

Returning to the scenario presented at the outset of this paper, there is no doubt that allocating responsibility for a breach of DPbD is difficult due to the complex chains of actions that exist between different actors in the supply chain. AI is not a stationary technology squarely under the authority of a single entity, but rather a complex entanglement of moving components, some human, some technical. As AI systems become increasingly generalized and possible to use for multiple purposes through transfer learning, the modular nature of software development will only grow more complex, making it hard to view the data controller as the main entity responsible for DPbD.

Considering the sociotechnical reality, the rationale for focusing almost entirely on the data controller as the main party responsible for DPbD breaks down because other actors in the supply chain, such as engineers, designers, and manufacturers, play critical roles in meeting this requirement. Merely incentivizing these actors to comply with DPbD is insufficient. A more nuanced approach than the controller-data subject binary is necessary to allocate responsibilities in an appropriate way.

This paper has suggested that the responsibility for DPbD must be conceived of in a more future-oriented, relational, and distributed way. A future-oriented conception of responsibility would require technology providers to adopt more proactive approaches to DPbD. While there is a need for methodological approaches to operationalize proactivity, various strategies are already available, many coming from the field of Human and Computer Interaction. For example, technology providers can embrace anticipatory methods to DPbD by using ideation cards to identify data protection concerns early within the design process.[171]

[167] Case C-300/21: Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021—UI v Österreichische Post AG. OJ C 320, 9.8.2021, pp 25–26.

[168] Mona Naomi Lintvedt, 'Putting a Price on Data Protection Infringement' (2021) 12 International Data Privacy Law 1–15, 13.

[169] Case C-300/21: Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021—UI v Österreichische Post AG. OJ C 320, 9.8.2021, pp 25–26, Opinion of Advocate General Campos Sanchez-Bordana delivered on 6 October 2022, para. 83–94.

[170] *Id* at paras. 104 and 105.

[171] Ewa Luger, Lachlan Urquhart, Tom Rodden, Michael Golembewski, 'Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process' in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (ACM Press 2015) 457–466, 457, 465.

There is also a need to take a more relational approach to DPbD whereby technology providers bear greater responsibilities to those individuals or groups that are affected by their design choices. Downstream actors in the supply chain can bear part of the legal responsibility for DPbD, even if they do not qualify as (joint) controllers, by relying on existing and emerging legal instruments that reflect DPbD requirements. These instruments can be applied to non-data controllers to increase their responsibilities towards end users. For example, technology providers can assist data controllers to stay up to date on the state of the art of the technology and exchange other important technical information to facilitate DPbD.

Lastly, a distributed approach to DPbD should be adopted whereby responsibility is borne by many actors in the supply chain, not just the data controller. The CJEU already appears to be adopting this approach by broadly defining the concept of joint data controllers. However, this approach is problematic, as expanding the scope of controllership to include ever more actors in the supply chain will stretch the law beyond its reasonable limits. There is also a lack of methodological approaches for dividing responsibilities among multiple parties that are defined as joint controllers.

A better approach would be for the law to adopt a narrower understanding of a joint data controller yet rely on emerging or existing rules to require technology providers to design their systems in a privacy-aware way and hold them responsible when they do not. To put it differently, downstream actors in the supply chain should bear part of the legal responsibility for DPbD even if they do not qualify as (joint) controllers. This could be accomplished by relying on legal requirements that are applicable to various actors in the supply chain supporting DPbD. These requirements could be found in contract law, liability law, and the emerging EU *acquis* governing AI, data, and information security.

FUNDING INFORMATION

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 the blind peer reviewers of this article who provided extremely helpful comments on the manuscript.

COMPETING INTERESTS

The author has no competing interests to declare.

AUTHOR AFFILIATIONS

Liane Colonna
The Swedish Law and Informatics Research Institute (IRI), Stockholm University, Stockholm, Sweden

TO CITE THIS ARTICLE:
Liane Colonna, 'Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-oriented, Relational, and Distributed Approach' (2022) 27(1) *Tilburg Law Review* pp. 1–21. DOI: https://doi.org/10.5334/tilr.274

Published: 17 February 2023

Tilburg Law Review is a peer-reviewed open access journal published by Ubiquity Press.