scripted

Volume 22, Issue 2, December 2025

Book review: *Data Protection, Privacy and Artificial Intelligence: To Govern or to Be Governed, That Is the Question*

Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (ed.)
London: Hart Publishing 2025. 328 pages.
ISBN 9781509983995. £55.00 (hardback), £49.50 (eBook).

*Reviewed by Anıl Sena Bayındır**

DOI: 10.2218/scrip.220225.227

* PhD Candidate, School of Law, University of Galway, Galway, Ireland, snbayindir@gmail.com.

1 The Question of The Century: "*To Govern or To Be Governed?*"

Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question is a product of the papers and the discussions from the 2024 Computers, Privacy, Data Protection.ai (CPDP) international conference. The reader can feel the diversity of a conference atmosphere in the book as they go through it, with a wide range of selection of topics and the perspectives that the authors embrace in their arguments. As Wojciech Wiewiórowski highlights in his concluding piece in the book, that CPDP serves as a bridge between generations and ideas, the essence of the conference has been encapsulated eternally for the ones who could not attend and for future generations.[1]

The book examines the impacts of artificial intelligence (AI) technologies and their use cases with a specific focus on right to privacy, right to data protection, right to effective remedy, right to a fair trial, freedom of expression and freedom of peaceful assembly, which are the core values of a well-functioning democratic society. The title of the book references "To be or not to be (…)" from William Shakespeare's play *Hamlet*, in which the weight of existence was being portrayed, and from a similar existential viewpoint the book chooses this opening line to touch upon the weight of possible risks of AI technologies. This choice of title hints to the reader to grasp the whole existential importance of the topics that will be discussed throughout the book.

[1] Wojciech Wiewiórowski, 'Devising a Trajectory towards a Just and Fair Future: The Identity of Data Protection in Times of AI' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025) 283.

The volume adopts predominantly a European perspective, focusing on the European Union (EU)'s regulatory approach to AI technologies, with a single exception of a paper examining the Canadian context in employment law. Consequently, it does not provide a comprehensive global overview, particularly regarding AI regulation in the United States (U.S.), its potential effects on U.S.–EU relations, or the consequent influence on the EU's regulatory stance. The conference theme is data protection, privacy, and AI, considered through the lens of "to govern or to be governed," and this theme frames the book's main focus. While the book is founded on a broad spectrum of issues at the intersection of privacy, data protection, and AI, due to the constraints inherent in a single volume, some topics are not discussed in depth. Examples of these are the protection of minors' data in the era of AI, the development of smart cities and their implications for fundamental human rights, AI-driven content moderation and its impact on democratic processes, and the social and ethical consequences of digital duplicates. Although these issues would have fallen within the thematic scope of the work, they are not examined, or not examined in substantive detail.

All in all, it's a thought-provoking book that gives lessons to its readers and makes them ask more questions. To illustrate this part of the book, the review will focus on the common lessons that can be drawn from the papers and the questions that they raise.

2 Lessons and Questions

The principal takeaways from the book can be summarised under four main points: i) AI's application sphere is remarkably diverse, ii) AI literacy and understanding the impacts of AI technologies are vital for the responsible, human-rights-oriented use of these technologies, iii) the EU AI Act adopts a risk-

based approach to regulation but leaves many issues unaddressed, and iv) AI is like fire[2] considering its negative impacts on society.

While lessons and takeaways are important, a piece is particularly effective when it prompts readers to ask further questions. Lessons and takeaways represent end points, whereas questions create opportunities for future discussion and deeper understanding. This book succeeds in stimulating such inquiry. Some of the questions it raises include: i) to what extent is the deployment of AI necessary for all tasks for which it is technically capable? ii) what measures can promote awareness and understanding of AI technologies? iii) what is the best way to regulate a technology with inherently uncertain risks, and does the AI Act get anything right?, and iv) can AI serve to extinguish a fire that is already burning?

The following section provides a detailed analysis of the lessons and questions raised.

2.1 AI's application sphere is remarkably diverse, but to what extent is the deployment of AI necessary for all tasks for which it is technically capable?

The book begins by exploring the use of AI technologies for deepnude applications, with the second paper of the book titled "*The Scourge of Deepnude Applications: A Fundamental Rights Perspective*," written by Aurélie Gilen, Catherine Van de Heyning, and Michel Walrave.[3]

---

[2] Murat Durmuş, 'Fighting AI With AI' (*LinkedIn*, 29 June 2025) <https://www.linkedin.com/pulse/fighting-ai-murat-durmus-vjghe/> accessed 17 December 2025, specifically the author states: "*If we must fight fire with fire, we should at least wear oven mittens. And maybe ... just maybe, we shouldn't stop setting things on fire in the first place*".

[3] Aurélie Gilen, Catherine Van de Heyning and Michel Walrave, 'The Scourge of Deepnude Applications: A Fundamental Rights Perspective' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025), 11-32.

The third paper, "*AI Risk Assessments in EU Large-Scale IT Systems for Third-Country Nationals and Access to Remedies: A Bumpy Road Ahead*," written by Alexandra Karaiskou and Niovi Vavoula, continues with the use of these technologies in border control and migration management.[4] Karaiskou and Vavoula discuss how these technologies can shift the focus from an individual's current behaviour to their socio-demographic identity and background, which are factors over which individuals have little control, within the context of migration.[5] This observation, however, can be extended to any form of profiling.

Other possible use cases appear in the use of AI technologies for law enforcement and policing purposes. These use cases are discussed in the fifth paper, titled "*The Semi-Perfect AI Act – A Missed Opportunity for a Human Rights-Centred Approach to AI and the Case of Facial Recognition*," written by Anže Erbežnik[6]; in the seventh paper, titled "*From Human Agency to Meaningful Human Oversight? Mapping the Opportunities and Pitfalls in the Decision-Making Process of Place-Based Big Data Policing*," written by Naomi Theinert, Robin Khalfa, and Wim Hardyns[7]; and in the eighth paper, titled "*The AI Act as a Safeguard for Equality of*

[4] Alexandra Karaiskou and Niovi Vavoula, 'AI Risk Assessments in EU Large-Scale IT Systems for Third-country Nationals and Access to Remedies: A Bumpy Road Ahead' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025), 33-76.

[5] Ibid 68.

[6] Anže Erbežnik, 'The Semi-perfect AI Act – A Missed Opportunity for Human Rights Centred Approach to AI and the Case of Facial Recognition' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025), 115-133.

[7] Naomi Theinert, Robin Khalfa and Wim Hardyns, 'From Human Agency to Meaningful Human Oversight? Mapping the Opportunities and Pitfalls in the Decision-Making Process of Place-Based Big Data Policing' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025), 167-200.

Arms in Data-driven Criminal Investigations," written by Johan van Bannin, with a specific focus on criminal investigations and equality of arms.[8]

On the other hand, it is also known that these technologies can be utilized for employment purposes, such as decisions regarding recruitment, promotion, and termination. The sixth paper, titled *"Artificial Intelligence and Employment Law: Through a Canadian Lens,"* by Fife Ogunde, discusses how these technologies can be applied for these purposes.[9]

In the ninth paper, titled "*Assessing the Risks of Emotion Recognition Technology in Domestic Security Settings: What Safeguards against the Rise of 'Emotional Dominance*'?", Francesco Paolo Levantino maps how AI technologies that can be utilized to identify, infer, and analyse emotions or intentions by processing biometric data work, as well as the possible downfalls of these applications.[10] For instance, these technologies may be employed for emotion recognition in surveillance contexts or for predicting an individual's personality traits or potential criminality based on facial images, thereby posing significant risks to fundamental rights, including the freedoms of expression and peaceful assembly, the right to a fair trial, and the presumption of innocence.[11]

---

[8] Johan van Banning, 'The AI Act as a Safeguard for Equality of Arms in Data-driven Criminal Investigations' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025), 201-224.

[9] Fife Ogunde, 'Artificial Intelligence and Employment Law: Through a Canadian Lens' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025), 135-166.

[10] Francesco Paolo Levantino, 'Assessing the Risks of Emotion Recognition Technology in Domestic Security Settings: What Safeguards against the Rise of "Emotional Dominance"?' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025), 225-257.

[11] Ibid 228, 235.

And finally, the use of AI technologies for summarisation solutions for call centres and health and safety monitoring solutions for workplaces is discussed in the tenth paper, titled "*Legislative Lag vs Technological Leap: Privacy and Data Protection Challenges when Using AI-Driven Workplace Solutions*," written by Ezgi Ercan and Geert Somers.[12]

The various use cases of AI systems and their potential social, economic, and legal implications are being provided in the book, while the question of how the law should react to such technologies is being elaborated. This kind of flow gets the reader to question whether the deployment of AI is necessary for all tasks for which it is technically capable, and if not, where and how the limits should be drawn.

2.2 AI literacy and understanding the impacts of AI technologies are vital for the responsible, human-rights-oriented use of these technologies. What measures can promote this awareness?

The various use cases of AI systems discussed above bring unique challenges, and this situation brings the need for critical oversight over these technologies. This can only be achieved with a proper notion of agency, in the meaning of an individual's capacity to act independently and to make their own free choices. Building on this, Theinert, Khalfa and Hardyns argue that agency and oversight can only be possible where adequate training and awareness are ensured for all decision makers and users.[13]

---

[12] S Ezgi Ercan and Geert Somers, 'Legislative Lag vs Technological Leap: Privacy and Data Protection Challenges when Using AI-Driven Workplace Solutions' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025) 261-274.

[13] Theinert, Khalfa and Hardyns (n7) 170-171.

AI literacy and understanding are vital for every actor in the arena to encourage a responsible human-rights-oriented use of these technologies. This requires the participation of all segments of society. These include i) the decisionmakers, ii) developers, iii) users of the technologies as the deployers[14], iii) users of the technology as the end-users[15] and iv) the individuals who will be affected by these technologies.

First, AI literacy and understanding are essential for decision-makers, including policymakers, lawmakers, and the judiciary, to establish policy priorities, draft legislation concerning these technologies, and utilise them in a human-rights-oriented and ethical manner.

Second, developers of such technologies should ensure they have a strong understanding of their social and ethical consequences, in addition to being equipped with the technical expertise to build them to make sure such technologies are developed with an awareness. The same expectation applies to users of these technologies as deployers. For example, van Banning talks about the levels of the black box problem and mentions how it depends on the context regarding who tries to explain the AI technology and its consequences.[16] With this reference, he implicitly highlights the value of AI literacy obligations in addressing the black box problem of these systems to a certain extent. He highlights that only if information on the functioning of, or the way these tools have been deployed, is available, lawyers and judges can assess whether the investigation was carried out lawfully.[17] A lack of technical information and

[14] In this context, deployers are the people or companies that implement a technology in real-world settings and introduce its use to the consumer market.
[15] End-users are the individuals who ultimately use the technology for its intended purpose as consumers.
[16] van Banning (n8) 207.
[17] Ibid 210-211.

understanding might make it impossible for the defence to effectively challenge the evidence, thereby infringing the principle of equality of arms.[18]

Colonna comprehensively discusses how AI literacy is a cornerstone provision to enable the human oversight provisions of the EU AI Act in her paper "*Complex Normativity: Understanding the Relationship between Human Oversight by Design and Standardization in the Context of AI Development and Deployment*" which will be discussed further in section 2.3 below.[19]

Thirdly, as an example of the problems associated with end-users' lack of awareness, Gilen, Van de Heyning and Walrave highlight research indicating that young adults often lack awareness of the consequences associated with deepnude technology[20], which in turn affects how they use such technologies. In other words, if the young adults as end-users had been made aware of the risks associated with this technology, and of the illegality of using these technologies without individuals' consent, they might have chosen to refrain from their use, thereby avoiding potential legal and ethical issues.

Fourth, as an example of the problems associated with lack of awareness and understanding of the individuals who will be affected by these technologies, Karaiskou and Vavoula discuss how lack of literacy can affect third-country nationals in their visa and residency card applications where the migration authorities are using AI technologies for migration management.[21] Similarly, Ogunde examines how employees or potential employees may be unable to

[18] Ibid 212.
[19] Liane Colonna, 'Complex Normativity: Understanding the Relationship between Human Oversight by Design and Standardization in the Context of AI Development and Deployment' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025) 87.
[20] Gilen, Van de Heyning and Walrave (n3) 13.
[21] Karaiskou and Vavoula (n4) 60.

determine whether they have been victims of algorithmic discrimination, since an employee or a job applicant will be highly unlikely to have sufficient knowledge of the nature of an organisation's use of AI.[22]

As Ogunde highlights, statutory disclosure requirements may increase the accessibility of information, which will increase awareness and understanding of such technologies and empower individuals to make informed decisions on how to challenge certain applications on the grounds for illegality.[23]

Thus, the book demonstrates the importance of AI literacy and understanding the impacts of AI technologies and raises the question of which measures, alongside the literacy obligations in the EU AI Act, can promote this awareness.

2.3 The EU AI Act adopts a risk-based approach to regulation but leaves many issues unaddressed. What is the best way to regulate a technology with inherently uncertain risks, and does the AI Act get anything right?

Vladan Joler emphasises in the first paper titled "*Behind the Visual Identity of CPDP.ai 2024*" that AI systems come with hidden environmental and social costs and generally maximise the profits for few, whereas the destruction they cause is shared by all.[24] Similarly, Shubham Kaushik highlights that technology is seen as the fastest way to profit and growth, but its social and environmental effects are largely ignored in the eleventh paper titled "*Brick by Brick: What Will it Take*

[22] Ogunde (n9) 144.
[23] Ibid 146.
[24] Vladan Joler, 'Behind the Visual Identity of CPDP.ai 2024' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025) 6.

to Centre People, the Planet and Democracy in our Digital Futures?".[25]

To balance this asymmetry, lawmakers are called to a mission. Upon the call, international organisations and the EU have acted. As Ercan and Somers discuss, the Council of Europe adopted the Framework Convention on Artificial Intelligence in 2024, creating the first international legally binding treaty for this purpose.[26] This treaty dealt with the issue with a risk-based methodology by stating that all AI systems pose potential risks to human rights, democracy, and the rule of law, and it requires high-level obligations and a framework for risk assessment.[27]

Then, the EU enacted an EU AI Act again in 2024 with another risk-based methodology which classified AI system use cases into four categories: unacceptable risk, high risk, limited risk, and minimal risk. The Act prohibited use cases deemed to pose an unacceptable risk and imposed differentiated obligations for the remaining risk categories.

The Act has been criticised on many fronts because of the methodology it is based on. Wiewiórowski describes it as an internal market legislation for commercialising AI systems, and he highlights how it is completely different from being a tool to protect fundamental rights in concluding paper titled "*Devising a Trajectory towards a Just and Fair Future: The Identity of Data Protection in Times of AI*".[28]

---

[25] Shubham Kaushik, 'Brick by Brick: What Will it Take to Centre People, the Planet and Democracy in our Digital Futures?' in Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder (eds), *Data Protection, Privacy and Artificial Intelligence, Volume 17: To Govern or To Be Governed, That Is the Question* (Hart Publishing 2025) 277.

[26] Ercan and Somers (n12) 263.

[27] Osman Gazi Güçlütürk, 'Understanding the Council of Europe's Draft Framework Convention on AI, Human Rights, Democracy, and the Rule of Law' (*Holistic AI Blog* , 17 January 2024) <https://www.holisticai.com/blog/europe-committee-artificial-intelligence-draft-framework-convention> accessed 17 December 2025.

[28] Wiewiórowski (n1) 284.

Erbežnik describes this as a "*missed opportunity*", arguing that the regulation fails to prioritise fundamental rights. He characterises AI systems as a "*civilisation-altering technology*" and criticises the product-safety approach adopted in drafting the EU AI Act.[29] Similarly, Kaushik emphasises that the EU institutions tried to "*sell an idea of security that threatens fundamental rights*", which makes people more unsafe.[30]

In addition to this risk-based approach methodology, Erbežnik criticises how the EU AI Act delegates power to the Commission to decide on high-risk systems by giving the institution the ability to amend Annex III, creating concerns over democratic accountability and oversight for these systems.[31]

On the other hand, Theinert, Khalfa and Hardyns highlight that the High-Level Expert Group on AI, which was influential in the drafting of the EU AI Act, only consisted of four representatives from civil society out of fifty-two, where half of these were industry representatives.[32] The authors also make it clear that civil society is the most affected group from the adverse impacts of these technologies, but they are also the least represented group.[33] This shows how even the law-making process lacked the public representation it should have had for a more democratic law-making process.

EU AI Act embraces a risk-based approach; however, Theinert, Khalfa and Hardyns point out that the EU AI Act cannot recognise the context-specific nature of AI systems and their use, and it fails to recognise the power asymmetries that will come along with big data policing applications.[34] Similarly,

[29] Erbežnik (n6) 117.
[30] Kaushik (n25) 276.
[31] Erbežnik (n6) 122.
[32] Theinert, Khalfa and Hardyns (n7) 178.
[33] Ibid.
[34] Ibid 176.

for example, the EU AI Act deals with deepfakes as a limited-risk AI system and only puts transparency obligations on the providers and deployers; however, the use case of deepfakes can significantly change the stakes of this risk, as in the example of deepnude discussed by Gilen, Heyning and Walrave.[35]

On the prohibited practices under the EU AI Act and the exceptions to these prohibitions, Kaushik highlights that even the ban on live mass facial recognition and other public biometric surveillance by police is a modest step for protecting human rights, since the wide exceptions to it open the way for their legitimate use under certain circumstances.[36] On top of that, Erbežnik reaches a conclusion regarding the Brussels effect of the EU legislation, mentioning that the EU, in a way, gave its permission to use real-time biometric identification for law enforcement purposes, which causes the EU AI Act to normalise surveillance to a certain extent.[37] Similarly, Levantino mentions that emotion recognition is fully prohibited only in workplace and educational settings, allowing the use of these technologies for emotion recognition purposes for law enforcement purposes.[38] This could be seen as another unfortunate green light that the EU has given for the use of AI for surveillance in a way. Kaushik argues in his paper that surveillance is being presented as the only way to combat crime, but he concludes that this is patently false.[39]

The nature of the regulation has shifted over the course of time. Colonna refers to Colin Scott's post-regulatory state[40], and how the power asymmetries

[35] Gilen, Van de Heyning and Walrave (n3) 28.
[36] Kaushik (n25) 279.
[37] Erbežnik (n6) 125-126.
[38] Levantino (n10) 231, 249.
[39] Kaushik (n25) 276.
[40] Colin Scott, 'Regulation in the Age of Governance: The Rise of the Post Regulatory State' in J Jordana and D Levi-Faur (eds), *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance* (Edward Elgar Publishing 2004) 145–174.

are being shifted so that the sharp distinction between state and market, and public and private, has started to dissolve.[41] Erbežnik and Theinert, Khalfa and Hardyns likewise discuss how AI technologies are making law enforcement and policing dependent on private companies.[42] This situation affects the way lawmakers deal with AI. Colonna portrays the fact that the ultimate goal of the regulation and the key challenge intersect on the same thing, which is to motivate the behaviour that achieves the desired outcome.[43] Here, the desired goal is encouraging the use of AI systems for ethical purposes in ethical ways, but since this requires technical standards to be achieved due to the nature of the subject of the regulation, co-regulation appears as a possibility.

Co-regulation, as Colonna discusses, might allow discretion and flexibility to technology providers and users to implement the rules.[44] Similarly, the EU AI Act brings a human-oversight-by-design obligation for providers and deployers of high-risk AI systems but leaves room for providers and deployers to ensure compliance with those values.[45] For this obligation to be fulfilled, the design of the system must enable humans to detect anomalies, dysfunctions, and unexpected performances, as well as be aware of automation bias, and this oversight should minimise the health, safety, and fundamental rights risks.[46]

Here, the legal requirements ask for a technical way to ensure a regulatory objective, but they do not prescribe the method by which it must be achieved. [47]

[41] Colonna (n19) 80.
[42] Erbežnik (n6) 123; Theinert, Khalfa and Hardyns (n7) 183.
[43] Colonna (n19) 82.
[44] Ibid 103.
[45] Ibid 84-85.
[46] Ibid 85.
[47] Ibid 91.

In this regard, industry expertise will be leveraged[48]; however, this will create a situation in which industry will develop its own internal compliance for AI, as Erbežnik points out.[49]

This kind of approach to AI regulation might also affect legal foreseeability. For example, a particular method may be sufficient to achieve the required level of fundamental protection at one moment, yet the same method may no longer be deemed adequate as the state of the art evolves. This also puts providers and deployers in a more dynamic and adaptive position.

All the things the EU AI Act might have failed to do, it nonetheless achieves a number of important objectives. For example, Colonna discusses how the EU AI Act manages to embrace a life-cycle approach to the allocation of obligations and explicitly includes both providers and deployers in order to mitigate potential responsibility gaps.[50] This is something that is missing in the Artificial Intelligence and Data Act (AIDA) in Canada, since the Act applies only to organisations that design, develop, and make an AI system; however, the businesses that will use these technologies for hiring and management decisions are left outside the scope of the AIDA, as Ogunde explains.[51]

The EU AI Act's literacy requirement also appears positive, particularly considering the importance of AI literacy and understanding discussed in section 2.2 above. Under Article 14, the EU AI Act requires human oversight as a legal requirement, imposing an obligation to provide a human interface to enable human oversight while the AI system is in use. Theinert, Khalfa and Hardyns highlight that this requirement reinforces the need for explainable AI to address

[48] Ibid 80.
[49] Erbežnik (n6) 120.
[50] Colonna (n19) 87.
[51] Ogunde (n9) 156.

both human and machine bias, since explainability can facilitate effective human oversight.[52]

The asymmetries in the distribution of social and environmental costs of AI technologies on the societies require regulatory intervention. The book examines the regulatory frameworks of the Council of Europe and the EU, placing particular emphasis on the EU AI Act. The Act adopts a product safety approach, and it does not adequately address several concerns highlighted by authors in the book, raising the question of whether it effectively achieves any of its objectives. Regarding this, the life-cycle approach and AI literacy obligations in the EU AI Act appear to be positive aspects.

2.4 AI is like fire[53], considering its negative impacts on society, but can it serve to extinguish a fire that's already burning?

AI systems bring new challenges as they are incorporated into different areas. Following this, two key questions arise: i) whether these challenges stem from the technology itself or from the way in which it is incorporated by humans; and ii) whether, alongside their efficiency and speed advantages, such systems might also present opportunities to address some already existing problems.

On the first question, Gilen, Van de Heyning and Walrave conclude that the issue concerning the use of these technologies does not lie in the technology itself, but lies in their utilisation without fully realising the consequences.[54] Similarly, Theinert, Khalfa and Hardyns state that explainable AI is not and will not be a magical fix for systemic problems and bias in policing, because, as the technology generally is not the reason for the human rights violation but the use

[52] Theinert, Khalfa and Hardyns (n7) 193.
[53] Durmuş (n2).
[54] Gilen, Van de Heyning and Walrave (n3) 29.

of it, the fix will not be in the technology, but in the oversight mechanisms and the technology's contribution to the ethical design and implementation of big data policing models.[55] Because even if the most explainable AI technology is developed, the persistence of human error and bias in the human oversight prevents the process from being ethically improved. Since the technology itself is not the sole problem associated with the use of AI systems in various contexts, the solution cannot, and will not, be purely technological.

Theinert, Khalfa and Hardyns, also, make an important point on human error, and they emphasise that with or without AI, human error exists and persists.[56] Even if the human oversight is thought to make the AI more ethical, the AI has the potential to continue to reflect the already existing human bias.[57] Also, they highlight that AI presents opportunities for crime preventative policing, transparency, and oversight[58], suggesting that the second question raised earlier may indeed be relevant. On the same note, Ogunde discusses the use of AI systems in employment contexts, and he highlights the risk of perpetuating existing discrimination or bias.[59] He also emphasises how the AI systems can reduce the likelihood of other forms of discrimination taking place as well.[60]

3 Concluding Remarks – *"Nothing Happens Twice"*

Based on the lessons it conveys and the questions that it prompts readers to consider it should be more obvious now that "*Data Protection, Privacy and*

[55] Theinert, Khalfa and Hardyns (n7) 194.
[56] Ibid 174.
[57] Ibid.
[58] Ibid 196.
[59] Ogunde (n9) 138.
[60] Ibid 139.

Artificial Intelligence: To Govern or to Be Governed, That Is the Question," edited by Eleni Kosta, Dara Hallinan, Paul De Hert, and Suzanne Nusselder, is a significant book, with ideas and arguments both from academia and industry distilled from the conference. It offers a comprehensive overview of the issues raised by AI technologies in relation to data protection and privacy and serves as a valuable reference for future discussions.

Wiewiórowski ,in his concluding piece, highlights that the law will not always draw a clear line between what is right and what is wrong[61], but he still concludes the conference and the book on an optimistic note by quoting a Polish poet: evolution and change will eventually come.[62] AI poses risks and places humanity in unprecedented times, but this is also a common feature of every innovation. The law may fall short at certain points in demonstrating what is right and what is wrong, which will inevitably have consequences. Nevertheless, one way or another, evolution and change will occur in a world shaped by these technologies, as long as we keep asking questions, as this book encourages its readers to do, and critically work on these questions for a better world.

[61] Wiewiórowski (n1) 284.
[62] Ibid 286.