"Balancing security and personal freedom in the age of artificial intelligence: Civil Law perspectives"

Abstract

The rapid development of artificial intelligence (AI) has profoundly reshaped legal systems, particularly concerning surveillance and individual rights. This paper examines the tension between public security and personal freedom from a civil law perspective, analysing how AI-driven surveillance challenges existing frameworks such as the GDPR and national civil codes. Key issues include algorithmic bias, data ownership, and the attribution of liability in both contractual and extra-contractual contexts. Special focus is given to the opacity of AI ("black box" problem) and its implications for accountability and evidence in legal proceedings. The study evaluates alternative liability models—strict and vicarious—and their potential to address the shortcomings of traditional doctrines. By adopting a multidisciplinary and comparative approach, the article proposes legal adaptations aimed at reconciling technological innovation with the protection of fundamental rights, ensuring that AI surveillance operates within a coherent and just regulatory framework.

Keywords: Artificial Intelligence; Civil Liability; Privacy Rights; Algorithmic Bias; GDPR.

Introduction

The accelerated development of artificial intelligence (AI) has profoundly transformed contemporary society[1], particularly in the realm of public security[2] and data governance[3].

AI systems are increasingly integrated into surveillance mechanisms[4], predictive analytics[5], and public administration[6], providing unprecedented capabilities for monitoring[7], data processing[8], and decision-making[9]. These technological advancements have the potential to enhance public safety, prevent crime, and improve governmental efficiency[10]. However, they simultaneously raise profound concerns regarding the protection of fundamental rights, especially privacy and individual freedom.

The legal debate on AI centres on the tension between enhancing public security through technology and protecting individual autonomy from state and corporate overreach[11]. This tension is not new—throughout legal history, lawmakers have grappled with the need to balance collective safety with the protection of individual liberties. Yet, the scale and complexity of AI introduce novel legal and ethical challenges that require a reconsideration of existing regulatory frameworks[12].

---

[1] Frederick Kile, 'Artificial Intelligence and Society: A Furtive Transformation' in Karamith S Gill (ed), *AI & Society* (Springer 2012).

[2] Aleksei Tuborov, 'Artificial Intelligence and Security: Transformation and Consistency' (NRUHSE 2022) 41.

[3] Patrick Dunleavy and Helen Margetts, 'Data Science, Artificial Intelligence and the Third Wave of Digital Era Governance' (2025) 40 (2) PPA 39.

[4] Athina Sachoulidou and Niovi Vavoula, 'Artificial Intelligence and Surveillance' in Sonia Lucarelli and James Sperling (eds), *Handbook of EU Governance* (Edward Elgar 2025).

[5] Siti Zulaikha et al, 'Customer Predictive Analytics Using Artificial Intelligence' (2021) TSE Rev 12.

[6] Anca Florentina Vatamanu and Mihaela Tofan, 'Integrating Artificial Intelligence into Public Administration: Challenges and Vulnerabilities' in Anca Florentina Vatamanu and Diana-Camelia Iancu (eds), *Towards Sustainable and Resilient Economy: The Role of Artificial Intelligence in Transforming Public Administration* (MDPI 2025).

[7] Varanon Uraikul, Christine W Chan and Paitoon Tontiwachwuthikul, 'Artificial Intelligence for Monitoring and Supervisory Control of Process Systems' in Christine Chan, Raphael Idem and Paitoon Tontiwachwuthikul (eds), *Applications of Artificial Intelligence in Process Systems Engineering* (IFAC 2007).

[8] Abdulaziz Aldoseri, Khalifa N Al-Khalifa and Abdel Magid Hamouda, 'Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges' (2023) 13(12) AS 33.

[9] Vinoud U Vincent, 'Integrating Intuition and Artificial Intelligence in Organizational Decision-Making' (2021) 64(4) BH 13.

[10] Qin Hao and Li Zhi, 'A Study on Enhancing Government Efficiency and Public Trust: The Transformative Role of Artificial Intelligence and Large Language Models' (2023) 14(3) Intl JEMR 4.

[11] Bhupinder Singh, 'Cherish Data Privacy and Human Rights in the Digital Age: Harmonizing Innovation and Individual Autonomy' in Maja Pucelj and Rado Bohinc (eds), *Balancing Human Rights, Social Responsibility, and Digital Ethics* (IGI Global 2024).

[12] Ammar Zafar, 'Balancing the Scale: Navigating Ethical and Practical Challenges of Artificial Intelligence (AI) Integration in Legal Practices' (2024) 4 DAI 27, 18.

From a civil law perspective, AI governance engages critical legal questions regarding the regulation of personal data[13], algorithmic transparency[14], and the attribution of liability for harms caused by automated decision-making[15]. The General Data Protection Regulation (GDPR) and national civil codes provide foundational legal mechanisms to address these issues[16], but the rapid evolution of AI technology reveals gaps and ambiguities that challenge traditional legal paradigms. For instance, the principles of proportionality and necessity embedded in the GDPR aim to prevent excessive data processing, but struggle to address the opacity of AI algorithms and their potential discriminatory effects[17].

The legal implications of AI in surveillance extend beyond data protection to encompass the fundamental principles of civil liability. Civil law traditionally assigns responsibility based on human agency and fault[18]; however, the autonomous and probabilistic nature of AI systems complicates the attribution of liability. Whether responsibility should rest with the developers, deployers, or manufacturers of AI remains a contentious issue. This ambiguity calls for a systematic legal framework capable of addressing the unique risks posed by AI while preserving core principles of justice and fairness.

This paper aims to provide a comprehensive analysis of the legal challenges posed by AI-driven surveillance from a civil law perspective[19]. It will examine the adequacy of existing legal frameworks in regulating AI technologies and safeguarding personal freedoms. Special attention will be given to the principles of algorithmic accountability, data protection, and the evolving concept of civil liability in the context of automated decision-making.

---

[13] Rowena Rodrigues, 'Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities' (2020) 4 JRT 12.

[14] Stefan Larsson and Fredrik Heintz, 'Transparency in Artificial Intelligence' (2020) 9(2) IP Rev 16.

[15] Eric Tjong Tjin Tai, 'Liability for AI Decision-Making' in Larry A DiMatteo, Cristina Poncibò and Michel Cannarsa (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press 2022).

[16] Giovanni Sartor and Francesca Lagioia, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence* (STOA-EPRS 2020) 84; Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 CBL Rev 130.

[17] Lilian Mitrou, 'Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?' (2019) SSRN EJ 90; Daria Bulgakova and Valentyna Bulgakova, 'The Processing of Personal Data in Accordance with the Principle of Proportionality under EU General Data Protection Regulation' (2023) 3(1) PEL Rev 18.

[18] Ex multis: Guido Alpa, *La responsabilità civile. Parte generale* (UTET 2010).

[19] Tulika Singh, 'AI-Driven Surveillance Technologies and Human Rights: Balancing Security and Privacy' in Arun K Somani et al (eds), *SIST – Smart Systems: Innovations in Computing* (Springer 2024).

By adopting a rigorous, multidisciplinary approach, this study seeks to advance the legal discourse on AI regulation and propose doctrinal solutions to ensure a balanced coexistence of technological innovation and the protection of fundamental rights[20].

1. The legal framework of AI surveillance: Civil Law approaches

The regulation of artificial intelligence in the context of surveillance raises intricate legal questions under civil law, particularly regarding the interaction between technological innovation and the protection of individual rights[21]. AI-driven surveillance systems, encompassing facial recognition[22], behavioural analysis[23] and predictive policing[24], present unprecedented challenges to existing legal frameworks. While these technologies promise to enhance public security, they simultaneously threaten fundamental rights to privacy and personal autonomy, necessitating a nuanced legal response.

At the European level, the General Data Protection Regulation stands as the primary legislative instrument governing the collection and processing of personal data. Under Article 5, the GDPR enshrines core principles such as data minimisation, purpose limitation, and transparency, which seek to constrain the invasive potential of AI-driven surveillance. In particular, Article 22 provides individuals with the right not to be subject to decisions based solely on automated processing, including profiling, which significantly affects their rights and freedoms.

This provision reflects the broader objective of preventing the erosion of human autonomy by automated systems[25].

[20] An initial proposal in this direction is represented by: Bernd Carsten Stahl, Rowena Rodrigues, Nicole Santiago and Kevin Macnish, 'A European Agency for Artificial Intelligence: Protecting Fundamental Rights and Ethical Values' (2022) 45 CLS Rev 25.

[21] Nikolaus Marsch, 'Artificial Intelligence and the Fundamental Right to Data Protection: Opening the Door for Technological Innovation and Innovative Protection' in Thomas Wischmeyer and Timo Rademacher (eds), *Regulating Artificial Intelligence* (Springer 2020).

[22] Thomas Gremsl and Elisabeth Hödl, 'Emotional AI: Legal and Ethical Challenges' (2022) 27(2) IP 11.

[23] Zouhair Elamrani Abou Elassad, Hajar Mousannif, Hassan Al Moatassime and Aimad Karkouch, 'The Application of Machine Learning Techniques for Driving Behavior Analysis: A Conceptual Framework and a Systematic Literature Review' (2020) 87 EAAI 27.

[24] John LM McDaniel and Ken G Pease, 'Predictive Policing and Artificial Intelligence' (2021) A Rev C 73.

[25] Razieh Nokhbeh Zaeem and K Suzanne Barber, 'The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise' (2020) 12(1) ACMTMIS 20.

1.1 The Limits of Traditional Liability Frameworks

Civil law further imposes specific duties of care on entities deploying AI in surveillance. National legal frameworks grounded in the Civil Code extend liability to actors responsible for wrongful or negligent conduct that results in harm. For instance, Article 2043 of the Italian Civil Code imposes an obligation to compensate for damages caused by illicit acts. This general principle of extra-contractual liability (delictual liability) could be applied to the use of AI technologies that infringe upon privacy rights or cause other forms of legally recognisable harm[26].

However, applying these traditional concepts to AI surveillance is fraught with practical difficulties. This opacity complicates liability attribution in practice[27]. When harm arises from automated decision-making, it may be unclear whether responsibility lies with the software developer, the public authority deploying the technology, or third-party service providers[28].

To address these gaps, legal scholars advocate for the introduction of a distinct liability regime tailored to the peculiarities of AI systems[29]. Such a framework would need to balance the promotion of innovation with the imperative to protect fundamental rights.

One proposed solution involves adopting a strict liability standard for entities that control or deploy AI surveillance technologies[30], thus eliminating the need to prove fault or negligence.

This approach aligns with existing legal doctrines applicable to inherently hazardous activities, where the potential for significant harm justifies the imposition of heightened responsibilities[31].

1.2 Proposals for Adapted Liability Models

Moreover, civil law must grapple with the intersection of public and private interests in AI surveillance. While public authorities may invoke national security imperatives to justify invasive surveillance measures, these objectives must be reconciled with the individual's right

[26] Marialuisa Gambini, 'Principio di responsabilità e tutela aquiliana dei dati personali' (2018) *Quaderni della Rassegna di diritto civile*, dir Pietro Perlingieri (ESI) 160.

[27] Manuel Carabantes, 'Why Artificial Intelligence Is Not Transparent: A Critical Analysis of Its Three Opacity Layers' in Simon Lindgren (ed), *Handbook of Critical Studies of Artificial Intelligence* (Edward Elgar 2023).

[28] Patrick Mikalef et al, 'Thinking Responsibly About Responsible AI and "the Dark Side" of AI' (2022) 31(3) EJIS 11.

[29] Bernhard A Koch et al, 'European Commission's Public Consultation on Civil Liability: Adapting Liability Rules to the Digital Age and Artificial Intelligence – Response of the European Law Institute' (ELI 2023) 32.

[30] Beatriz Botero Arcila, 'AI Liability in Europe: How Does It Complement Risk Regulation and Deal with the Problem of Human Oversight?' (2024) 54 CLS Rev 17.

[31] Paulius Čerka, Jurgita Grigienė and Gintarė Sirbikytė, 'Liability for Damages Caused by Artificial Intelligence' (2015) 31(3) CLS Rev 13.

to privacy[32]. The principle of proportionality, a cornerstone of European legal systems, mandates that surveillance measures must be necessary and proportionate to the legitimate aim pursued[33]. Judicial oversight mechanisms and independent auditing procedures are essential to ensuring compliance with these standards and preventing abuses[34].

The legal framework governing AI surveillance under civil law reveals both strengths and limitations. Existing doctrines of liability and data protection offer foundational safeguards, but the distinctive characteristics of AI necessitate an evolution of legal principles. Future regulatory developments must prioritise algorithmic transparency, the fair allocation of liability, and robust mechanisms for safeguarding personal freedoms in the face of technological advancement.

2. Algorithmic bias and civil liability

The integration of artificial intelligence into decision-making processes has amplified concerns regarding algorithmic bias[35] and its implications for civil liability. Algorithmic bias refers to systematic errors in AI outputs that disproportionately affect certain social groups, often resulting from the data used to train these systems. Such biases can produce discriminatory outcomes[36] that infringe on legally protected rights and raise fundamental questions about the allocation of legal responsibility.

Traditional legal doctrines require a direct causal link between a wrongful act and the harm caused[37]. However, AI operates through complex statistical models and machine-learning processes[38]. This ambiguity complicates the application of classic fault-based liability under Article 2043 of the Italian Civil Code or equivalent provisions in other civil law jurisdictions.

---

[32] Jana Misic, 'Algorithmic Europe: Narratives of Risks and Benefits of Public–Private Interaction in Public Sector AI' in Vaike Fors, Martin Berg and Meike Brodersen (eds), *The De Gruyter Handbook of Automated Futures* (De Gruyter 2024).

[33] Jonida Milaj, 'Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance' (2015) 30(3) I Rev LCT 15.

[34] Kilian Vieth and Thorsten Wetzling, 'Data-Driven Intelligence Oversight: Recommendations for a System Update' (2019) SSRN EJ 63.

[35] Ex multis: Nima Kordzadeh and Maryam Ghasemaghaei, 'Algorithmic Bias: Review, Synthesis, and Future Research Directions' (2021) 31(3) EJIS 21.

[36] Sara Moussawi, Xuefei Deng and KD Joshi, 'AI and Discrimination: Sources of Algorithmic Biases' (2024) 55(4) ACM SIGMIS D 5.

[37] Ex multis: Cesare Salvi, 'La responsabilità civile' in Giovanni Iudica and Paolo Zatti (eds), *Trattato di diritto privato*, vol 3 (Giuffrè 2019).

[38] Jose Vicente Abellan-Nebot and Fernando Romero Subirón, 'A Review of Machining Monitoring Systems Based on Artificial Intelligence Process Models' (2009) 47 Intl JAMT 20.

One of the core legal issues is whether algorithmic bias should be treated as a defect in the product[39] or as a failure of due diligence by the developer or deployer[40]. The EU Product Liability Directive provides a potential framework, classifying AI systems as products subject to strict liability for defects[41]. Under this regime, injured parties do not need to prove negligence but only that the AI system was defective and caused harm.

An alternative perspective advocates for the application of vicarious liability principles, holding entities that deploy AI responsible for the harms their systems cause, regardless of whether they directly created the algorithm. This would align with established doctrines of employer liability[42], which impose responsibility on principals for the actions of their agents. In the context of AI, such a framework would ensure that those who benefit from automated systems bear the corresponding legal risks.

Beyond the challenges posed by algorithmic bias in tort-based frameworks, a broader perspective on liability also requires re-evaluating the contractual and extra-contractual dimensions of AI governance.

3. Contractual and extra-contractual responsibility in AI governance

The rapid proliferation of artificial intelligence (AI) systems has given rise to complex legal issues surrounding both contractual and extra-contractual liability. Given the autonomous and self-learning nature of these technologies, it becomes increasingly difficult to determine responsibility when harm arises[43]. In AI governance, this difficulty is particularly pronounced in the context of surveillance applications[44], where the deployment of advanced monitoring

[39] Karni Chagal-Feferkorn, 'Am I an Algorithm or a Product: When Products Liability Should Apply to Algorithmic Decision-Makers' (2019) 30(1) SLP Rev 54.

[40] Marc H Pfeiffer, *First, Do No Harm: Algorithms, AI, and Digital Product Liability – Managing Algorithmic Harms Through Liability Law and Market Incentives* (Rutgers University 2023).

[41] "The New Product Liability Directive aims to modernize the product liability rules to bring them up to speed with advancing technologies, the circular economy business models and globalization of supply chains. It is also designed to remove obstacles for consumers wanting to seek compensation in respect of defective products. The New Product Liability Directive therefore changes the current product liability risk landscape for companies selling products in the EU significantly. Below we provide an overview of what companies selling products into the EU should know about the new product liability rules and how they can prepare in 2025 to mitigate increasing product liability risks" in Lena Niehoff, David Hilger, Megan Howarth and Katie Chandler, 'New Product Liability Directive 2024/2853: New Product Liability Risks for Products in the EU' (Taylor Wessing 2025) https://www.taylorwessing.com/en/insights-and-events/insights/2025/01/di-new-product-liability-directive accessed 26 May 2025.

[42] Ian Stone, 'Employers' Liability and Responsibility' in Hamid Ghodse (ed), *Addiction at Work*, vol 1 (Routledge 2005).

[43] Sruthi Rajendran and Akshay Dinesh Kumar, 'Liability for Harm Caused by AI: Examining the Legal Responsibility for the Actions of Autonomous Systems' (2023) 6(2) Intl JLMH 10.

[44] Roger Clarke, 'Responsible Application of Artificial Intelligence to Surveillance: What Prospects?' (2022) 27(2) IP 16.

tools can infringe on privacy rights and cause other legally significant damages. Civil law frameworks must therefore adapt to allocate liability in a manner that balances technological innovation with the protection of fundamental rights.

Contractual liability arises from the breach of obligations agreed upon between parties. In the realm of AI, these obligations typically derive from contracts governing the development, deployment, and use of AI systems[45]. Such contracts may include specific terms regarding performance standards[46], data protection compliance[47], and the allocation of liability in the event of malfunction or misuse[48].

A key issue in AI governance is the enforceability of contractual clauses when harm results from autonomous decision-making[49]. Traditional contract law presumes human agency and intent, but AI systems operate through automated processes that may not be foreseeable by either party. This raises the question of whether liability should be allocated strictly based on the contractual relationship[50] or extended to third parties who may suffer harm from AI-related actions[51].

For example, in cases where AI surveillance systems misidentify individuals or generate biased outcomes[52], the injured party may seek redress under the contractual agreement between the AI provider and the public authority[53]. However, if the contract does not explicitly address liability for algorithmic errors, general principles of contract interpretation and implied terms may be invoked[54]. Civil codes in European jurisdictions, such as Article 1218 of the French Civil Code on non-performance, provide a basis for contractual liability when an autonomous system causes harm attributable to a breach of agreed obligations[55].

---

[45] Hannes Claes and Maarten Herbosch, 'Artificial Intelligence and Contractual Liability Limitations: A Natural Combination?' (2023) 31(2) ERPL 27.

[46] André Janssen, 'AI and Contract Performance' in Larry A DiMatteo, Cristina Poncibò and Michel Cannarsa (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press 2022).

[47] Marco Antonio Lasmar Almada, *Law & Compliance in AI Security & Data Protection* (Hellenic Data Protection Authority 2024).

[48] Miriam C Buiten, 'Product Liability for Defective AI' (2024) 57 EJLE 34.

[49] Maarten Herbosch, 'To Err Is Human: Managing the Risks of Contracting AI Systems' (2025) 56 CLS Rev 15.

[50] Mikhail M Turkin, Evgeny S Kuchenin, Renata R Lenkovskaya and Georgyi N Kuleshov, 'Liability of Artificial Intelligence as a Subject of Legal Relations' (2020) 14(2) EAJB 16.

[51] Paulius Čerka et al, ibid 31.

[52] Eman Alajrami, Hani Tabash, Yassir Singer and MT El Astal, 'On Using AI-Based Human Identification in Improving Surveillance System Efficiency' in *2019 International Conference on Promising Electronic Technologies (ICPET)* (IEEE 2019) 4.

[53] Ifejesu Ogunleye, *AI's Redress Problem: Recommendations to Improve Consumer Protection from Artificial Intelligence* (UC Berkeley, CLTC White Paper Series 2022) 18.

[54] Ahmed Oudah Mohammed Al-Dulaimi and Mohammed Abd-Al Wahab Mohammed, 'Legal Responsibility for Errors Caused by Artificial Intelligence (AI) in the Public Sector' (2025) 67(4) Intl JLM 17.

[55] Valentin Jentsch, 'Contractual Performance, Breach of Contract and Contractual Obligations in Times of Crisis: On the Need for Unification and Codification in European Contract Law' (2021) 29(6) ERPL 31.

Furthermore, the concept of "force majeure" may complicate contractual liability in AI governance[56]. If an AI system's malfunction is deemed unforeseeable or beyond the control of the contracting parties, liability may be excluded. However, courts have increasingly scrutinized such exclusions, especially when the harm arises from negligent design, insufficient oversight, or the absence of adequate safety mechanisms.

Extra-contractual liability (also known as delictual or tort liability) addresses harm caused outside the scope of a contractual relationship[57]. This form of liability is particularly relevant in AI governance, where third parties—such as consumers or private individuals—may suffer harm from AI applications without being a party to the underlying contract.

In the context of AI surveillance, this includes privacy violations, reputational harm, and discriminatory practices resulting from biased algorithms. Extra-contractual liability applies not only to the direct user of the AI system but also to developers and manufacturers under the principle of "*culpa in vigilando*" which holds entities accountable for failing to prevent foreseeable harm[58].

As previously discussed, the opaque nature of AI complicates the identification of causal responsibility[59]. This problem raises questions about how liability should be apportioned among the various stakeholders involved in the design, deployment, and maintenance of AI systems.

Building on the rationale of strict liability explored above, some legal scholars extend this to encompass AI harms in general, irrespective of contractual or product-based frameworks[60]. Under a strict liability regime, the injured party is not required to prove fault but only to demonstrate that the AI system caused harm. This approach is consistent with existing legal frameworks for hazardous activities where the potential for significant harm justifies the imposition of heightened liability standards. For instance, the European Product Liability Directive already provides a model for holding producers strictly liable for defective products, which could be extended to AI systems[61].

---

[56] Stefan Koos, 'Artificial Intelligence as Disruption Factor in the Civil Law: Impact of the Use of Artificial Intelligence in Liability, Contracting, Competition Law and Consumer Protection with Particular Reference to the German and Indonesian Legal Situation' (2021) 36(1) YURIDIKA 28.

[57] Tycho de Graaf, 'Liability for Artificial Intelligence in EU Law' in Vanessa Mak, Eric Tjong Tjin Tai and Anna Berlee (eds), *Research Handbook in Data Science and Law* (Edward Elgar 2024).

[58] Giosetta Pianezze, 'Culpa in Vigilando' (2013) *Scenari* (Giuffrè) 315; Ignacio Atienza López, 'Responsabilidad Extracontractual. Culpa in Vigilando del Empresario: Límites' (2009) 105 RPDCCP 3.

[59] Thomas Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box' in Thomas Wischmeyer and Timo Rademacher (eds), *Regulating Artificial Intelligence* (Springer 2019).

[60] Ex multis: Christiane Wendehorst, 'Strict Liability for AI and Other Emerging Technologies' (2020) 11(2) JETL 30.

[61] For a critical review see: Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer, 'Liability for AI' in *Münster Colloquia on EU Law and the Digital Economy VII* (Hart 2023) 17.

In line with the previously discussed vicarious liability model, a broader interpretation may apply to public or private organisations that integrate AI into surveillance infrastructure[62]. In the AI context, vicarious liability could apply to organisations that deploy AI systems for surveillance, even if the harm results from autonomous decision-making.

National legal systems often impose vicarious liability on employers for wrongful acts committed by their employees in the course of employment[63]. By analogy, entities that use AI systems as functional equivalents of human agents may bear responsibility for the consequences of the AI's operation. This interpretation aligns with the notion that legal responsibility should track the economic benefits derived from the use of advanced technologies.

However, applying vicarious liability to AI raises doctrinal challenges. Unlike human agents, AI systems lack legal personhood and independent volition. To address this gap, some scholars propose recognising AI as a distinct legal entity with its own liability framework[64].

Others advocate for imposing joint and several liability on all entities involved in the AI supply chain[65], from developers to end-users. The fragmentation of legal responsibility in AI governance underscores the need for a unified liability framework.

4. Privacy protection and the limits of AI regulation

As artificial intelligence continues to penetrate various aspects of public and private life, it significantly challenges traditional paradigms of privacy protection[66]. The ability of AI systems to collect, analyse, and interpret vast amounts of personal data—often without the explicit knowledge or consent of the individuals concerned—raises profound questions about the adequacy of existing privacy laws[67]. In particular, the balance between protecting individuals' right to privacy and the necessity for AI-driven surveillance to enhance public security presents an ongoing legal conundrum.

At the European level, the General Data Protection Regulation (GDPR) represents the primary instrument designed to safeguard personal data and privacy in the context of digital

[62] Mihailis Diamantis, 'Vicarious Liability for AI' (2023) 99(1) ILJ 17.
[63] Adekunle Saheed Abiola and Zaynab Omotoyosi Shittu-Adenuga, 'Artificial Intelligence: The Application of the Doctrine of Vicarious Liability' (2024) 1(1) FULJ 8.
[64] Ex multis: Simon Chesterman, 'Artificial Intelligence and the Limits of Legal Personality' (2020) 69(4) ICLQ 25.
[65] Ex multis: Bart Custers, Henning Lahmann and Benjamyn I Scott, 'From Liability Gaps to Liability Overlaps: Shared Responsibilities and Fiduciary Duties in AI and Other Complex Technologies' in Karamith S Gill (ed), *AI & Society* (Springer 2025).
[66] Ana Beduschi, 'Synthetic Data Protection: Towards a Paradigm Change in Data Regulation?' (2024) 11(1) BDS 5.
[67] Daniel J Solove, 'Artificial Intelligence and Privacy' (2025) 77(1) FL Rev 73.

technologies[68]. Under the GDPR, the processing of personal data is subject to strict limitations, ensuring that it is carried out in a manner that respects individuals' privacy rights[69]. Specifically, the principles of data minimisation, purpose limitation, and transparency are designed to ensure that personal data is processed in a way that is both necessary and proportionate to the intended purpose[70]. However, the GDPR's application in the context of AI-driven surveillance technologies presents several challenges.

4.1 Consent and Transparency in AI Surveillance

The 'black box' nature of AI systems complicates GDPR compliance, particularly the requirement for transparency, by preventing individuals from understanding how their data is processed. Moreover, the right to explanation, enshrined in Article 22 of the GDPR, provides individuals with the right not to be subject to automated decisions that produce legal effects or similarly significant effects, yet its practical application in the context of AI remains highly debated[71].

Furthermore, AI surveillance systems - such as facial recognition and behavioural analysis - present particular challenges with regard to consent and data subject rights. In many instances, individuals may be unaware that their data is being processed, let alone that it is being used to monitor their activities in real-time. This lack of informed consent is in direct conflict with the core principles of data protection law. While the GDPR attempts to address these issues, its application to AI is often ambiguous[72], especially when it comes to the deployment of AI surveillance technologies by public authorities.

4.2 The Regulatory Gap and the Role of the GDPR

The limits of AI regulation are further compounded by the speed at which AI technologies are evolving. Regulatory bodies struggle to keep pace with technological advancements, and

[68] Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' (2018) 34(1) CLS Rev 19.
[69] Michal S Gal and Oshrit Aviv, 'The Competitive Effects of the GDPR' (2020) 16(3) JCLE 42.
[70] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28(1) ICTL 33.
[71] Elena Falletti, 'Automated Decisions and Article No. 22 GDPR of the European Union: An Analysis of the Right to an "Explanation"' (2019) 31 *Europeanrights.eu: Osservatorio dei Diritti Fondamentali in Europa* (Fondazione Basso) 15.
[72] Ronan Hamon et al, 'Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making' (2022) 17(1) IEEE CIM 13.

existing laws—such as the GDPR—are frequently criticised for being too general or slow to adapt. While GDPR sets a strong foundation for data protection[73], it is clear that a more specialised, flexible regulatory framework may be necessary to address the unique risks posed by AI in the surveillance context.

In this light, privacy protection in the age of AI must be reimagined through a multifaceted approach. While existing data protection laws, such as the GDPR, offer vital safeguards, there is a growing need for supplementary measures that account for the dynamic nature of AI technologies. Specifically, regulators should consider introducing tailored standards for AI systems, focusing on algorithmic transparency, the prevention of bias, and the development of frameworks for ongoing oversight and accountability.

The regulation of AI-driven surveillance raises crucial questions about the future of privacy protection. While the GDPR provides a valuable foundation, it must be complemented by more adaptive, targeted regulatory approaches that address the specific challenges presented by AI technologies[74]. Only through a more nuanced and proactive regulatory framework can the delicate balance between security and privacy be maintained in the face of rapid technological change.

5. Data ownership in the context of AI surveillance

The increasing deployment of artificial intelligence systems in surveillance activities has raised complex legal questions concerning data ownership within the framework of private law[75].

While data itself is not traditionally recognised as a tangible object susceptible to property rights in many legal systems, the commodification and pervasive collection of personal data have prompted a reevaluation of its legal status[76]. The core issue revolves around identifying who holds the right to control[77], use[78], and derive economic benefit from the data generated by or through AI surveillance mechanisms[79]. In the context of private law, these inquiries are closely

[73] Ralf Kneuper, *Foundations of Data Protection According to GDPR* in *Data Protection for Software Development and IT* (Springer 2024).
[74] Lilian Mitrou, ibid 17.
[75] Catarina Fontes et al, 'AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them' (2022) 71 TS 12.
[76] Ivan Stepanov, 'Introducing a Property Right over Data in the EU: The Data Producer's Right – An Evaluation' (2020) 34(1) Intl Rev LCT 21.
[77] Jeffrey Ritter and Anna Mayer, 'Regulating Data as Property: A New Construct for Moving Forward' (2018) 16 DLT Rev 57.
[78] James Grimmelmann and Christina Mulligan, 'Data Property' (2023) 72 AUL Rev 55.
[79] Nestor Duch-Brown, Bertin Martens and Frank Mueller-Langer, 'The Economics of Ownership, Access and Trade in Digital Data' (2017) 1 JRC DEWP 57.

linked to the principles of contractual autonomy, property law doctrines, and the evolving landscape of digital assets.

5.1 Ownership vs Control: A Conceptual Tension

From a contractual perspective, ownership claims over data are frequently governed by the terms established between parties involved in data collection, processing, and utilisation[80]. Contracts play a pivotal role in defining the scope of data access and delineating proprietary claims. However, standard contractual frameworks often exhibit significant power imbalances[81], especially when individuals are required to consent to extensive data collection practices without meaningful negotiation. This asymmetry raises concerns regarding the voluntariness and informed nature of such agreements, challenging the traditional foundations of consent under private law. Furthermore, the unilateral imposition of data ownership clauses may conflict with established legal doctrines on unfair contract terms, particularly where individuals are deprived of control over their personal information.

In jurisdictions with robust data protection regimes, such as those under the General Data Protection Regulation (GDPR), data subjects retain specific rights over their personal data[82]. While these rights do not equate to full ownership in the proprietary sense, they afford individuals a degree of control analogous to possessory entitlements in tangible property.

5.2 Private Law and Data Subject Rights

The right to access, rectify, and erase data, for instance, reflects private law's enduring concern with protecting individual autonomy against the disproportionate exercise of control by data controllers. However, the intersection between data protection law and private law is not

[80] Patrik Hummel, Matthias Braun and Peter Dabrock, 'Own Data? Ethical Reflections on Data Ownership' in Luciano Floridi (ed), *Philosophy & Technology* (Springer 2020).

[81] Monika Kuffer et al, 'Data Are Power: Addressing the Power Imbalance Around Community Data with the Open-Access Data4HumanRights Curriculum' in Cristóbal Fernández-Muñoz (ed), *Vulnerable Groups Protection and Rights for Advocacy: From the Perspectives of Community-Based Policy Making and Initiatives – Societies* (2025) 15(2) (MDPI) 19.

[82] Jacob Noti-Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123 YLJ 16.

without tension. Private law principles traditionally focus on the allocation of ownership through contractual and property frameworks[83], whereas data protection laws emphasize the preservation of fundamental rights and personal autonomy[84].

Some scholars suggest viewing personal data as quasi-property, though privacy-based regulation remains dominant[85]. Moreover, AI surveillance often involves the collection of non-personal or anonymised data[86], further complicating ownership claims. In these instances, proprietary entitlements may be asserted by the entities that aggregate and process the data rather than the individuals from whom it originates. This dynamic challenges conventional notions of ownership and raises the possibility of recognising sui generis rights over data sets.

5.3 A Case for a Sui Generis Legal Category

Comparative legal approaches reveal a lack of uniformity in addressing these issues: while some legal systems lean towards recognising data as a proprietary asset subject to exclusive control[87], others emphasise a more relational model, focusing on the legal obligations arising from data processing rather than proprietary claims per se[88].

The proliferation of AI surveillance thus necessitates a re-examination of private law frameworks to determine whether they adequately capture the complex and multifaceted nature of data ownership[89]. Traditional property doctrines, which emphasise exclusivity and transferability, may prove ill-suited to address the relational and dynamic character of digital data[90]. Consequently, there is growing scholarly debate regarding the need to develop a distinct legal category for data ownership[91], one that balances proprietary interests with the protection of individual rights. Within this evolving landscape, private law remains a crucial arena for

[83] Sjef Van Erp, 'Ownership of Data: The Numerus Clausus of Legal Objects' (2017) 6 BKPRCJ 24.
[84] Antoinette Rouvroy, 'Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence' (2008) 2(1) SELT 51.
[85] Lauren Henry Scholz, 'Privacy as Quasi-Property' (2016) 101 IL Rev 28.
[86] Azamat Ergashev, 'Privacy Concerns and Data Protection in an Era of AI Surveillance Technologies' (2023) 3(8) Intl JLC 5.
[87] Christiane Wendehorst, 'Proprietary Rights in Digital Assets and the Conflict of Laws' in Andrea Bonomi, Matthias Lehmann and Shaeeza Lalani (eds), *Blockchain and Private International Law: International and Comparative Business Law and Public Policy*, vol 4 (Brill Nijhoff 2023).
[88] Louise Gullifer and Ignacio Tirado, 'Proprietary Rights and Digital Assets: A "Modest Proposal" from a Transnational Law Perspective' (2025) 87(2) LCP 21.
[89] Christine Carter, 'AI Surveillance: Reclaiming Privacy Through Informational Control' (2025) 16(2) ELLJ13.
[90] Ex multis: Olga Goriunova, 'The Digital Subject: People as Data as Persons' (2019) 36(6) TCS 20.
[91] Francesco Banterle, 'Data Ownership in the Data Economy: A European Dilemma' in Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou and Thalia Prastitou (eds), *EU Internet Law in the Digital Era: Regulation and Enforcement* (Springer 2020).

negotiating the competing claims of individuals, corporations, and public authorities in the age of AI-driven surveillance.

6. Liability in AI-driven consumer transactions: challenges and legal responses

The integration of AI systems into contractual relationships, ranging from automated decision-making processes to AI-driven product recommendations, has introduced complexities in determining responsibility for harm or breach of obligations.

Traditional liability frameworks, primarily rooted in contractual and tortious principles, face increasing strain in addressing the unique characteristics of AI-driven transactions.

In such contexts, issues arise concerning the identification of liable parties, the attribution of fault, and the assessment of damages. In consumer contracts involving AI, the primary challenge lies in defining the contractual obligations and determining whether the performance of an AI system constitutes a breach[92]. Under conventional contract law, liability is typically attributed to the contracting parties based on fault or strict liability doctrines[93].

However, the autonomous nature of AI systems disrupts the straightforward application of these principles, as decisions made by AI may not directly reflect the intent or actions of either party[94]. Consequently, questions emerge regarding whether liability should rest with the AI's developer, the service provider deploying the system, or the end-user.

The European legal framework, particularly through the lens of the Consumer Rights Directive and the proposed AI Liability Directive[95], attempts to address these ambiguities by extending liability to the parties that design, deploy, or control AI systems. Notably, under the Product Liability Directive, producers remain strictly liable for defects in AI-integrated products, thereby safeguarding consumer protection while allowing room for technological innovation[96]. Nevertheless, the classification of AI outputs as "defects" remains contentious, particularly when the AI operates in unpredictable or adaptive ways beyond the initial design parameters.

---

[92] André Janssen, ibid 46.

[93] Roy Kreitner, 'Fault and Strict Liability in Contract' in Mindy Chen-Wishart and Prince Saprai (eds), *Research Handbook on the Philosophy of Contract Law* (Edward Elgar 2025).

[94] Hongmei He et al, 'The Challenges and Opportunities of Human-Centered AI for Trustworthy Robots and Autonomous Systems' (2022) 14(4) IEEE TCDS 14.

[95] Philipp Hacker, 'The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future' (2023) 51 CLS Rev 42.

[96] Teresa Rodríguez de las Heras Ballell, 'The Revision of the Product Liability Directive: A Key Piece in the Artificial Intelligence Liability Puzzle' (2023) 24 JAEL 12.

Moreover, the principle of foreseeability underpins much of contractual and tortious liability[97]. Yet, the self-learning capacity of advanced AI systems complicates the determination of foreseeable harm. Courts may struggle to evaluate whether AI-driven outcomes were reasonably predictable or within the scope of intended use.

In response, some legal scholars advocate for a risk-based approach, wherein liability attaches to those who are best positioned to prevent or mitigate harm, thus shifting the focus from traditional fault to a broader assessment of control and accountability[98].

AI-driven consumer transactions also raise concerns regarding informational asymmetry and consumer autonomy[99]. Consumers often lack the technical expertise to fully understand how AI systems operate, increasing their vulnerability to non-trasparent decision-making processes. This asymmetry challenges the principle of informed consent, a foundational concept in contract law. In light of this, regulatory initiatives advocate for heightened transparency obligations, requiring service providers to disclose the AI's role and its potential limitations[100].

In addressing these challenges, private law is evolving to incorporate new liability paradigms while preserving established doctrines of fairness and accountability.

Hybrid models of liability, which combine elements of strict liability with fault-based considerations, are gaining traction as a means of balancing technological innovation with consumer protection[101]. Additionally, contractual clauses explicitly addressing AI-related risks are becoming increasingly prevalent, offering parties a mechanism to allocate liability in advance. Overall, the regulation of liability in AI-driven consumer transactions reflects a dynamic interplay between legal tradition and technological innovation.

As AI continues to permeate commercial activities, legal frameworks must adapt to ensure equitable outcomes, protect consumer interests, and maintain the coherence of private law principles.

7. Tort liability and AI-driven decision-making

[97] Edijs Brants, 'Role of Foreseeability in Imposition of Civil Liability' (2021) 20(2) Socrates 18.
[98] Tycho de Graaf and Gitta Veldt, 'The AI Act and Its Impact on Product Safety, Contracts and Liability' (2022) 30(5) ERPL 31.
[99] Sébastien Fassiaux, 'Preserving Consumer Autonomy through European Union Regulation of Artificial Intelligence: A Long-Term Approach' (2023) 14(4) EJRR 20.
[100] Rashmi Mishra and Deepika Varshney, 'Consumer Protection Frameworks by Enhancing Market Fairness, Accountability and Transparency (FAT) for Ethical Consumer Decision-Making: Integrating Circular Economy Principles and Digital Transformation in Global Consumer Markets' (2024) 50(7) AJESS 13.
[101] Enrico Moch, 'Liability Issues in the Context of Artificial Intelligence: Legal Challenges and Solutions for AI-Supported Decisions' (2024) 7(1) EAJLE 20.

The increasing reliance on artificial intelligence in decision-making processes raises complex questions regarding tort liability, particularly when algorithmic determinations result in harm to individuals[102]. In private law systems, as mentioned above, tort liability is traditionally rooted in the principles of fault, causation, and damage. However, the autonomous and non accessible nature of AI systems challenges the application of these classic parameters.

One of the primary concerns is the attribution of fault in cases where AI-driven decisions cause harm. Given that AI systems operate with a degree of autonomy, it becomes difficult to establish a direct causal link between human intervention and the resulting damage[103].

From a theoretical perspective, the debate revolves around whether the responsibility should rest with the developer, the deployer, or the user of the AI system. Jurisdictions rooted in civil law have adopted diverse approaches to these questions. In some systems, liability is tied to the concept of *culpa in eligendo*[104] or *culpa in vigilando*[105], which focuses on the duty of care in the selection and supervision of AI tools. In these cases, the entity responsible for deploying the AI may be held liable for the harm caused if it failed to exercise reasonable care in its oversight. Conversely, some legal frameworks advocate for strict liability, where the responsible party is held liable irrespective of fault due to the inherent risks associated with AI technologies. This approach mirrors traditional regimes governing inherently dangerous activities, recognizing that the complexity and unpredictability of AI systems make fault-based models insufficient to safeguard injured parties.

A critical issue in assigning tort liability for AI-driven decision-making is the challenge of establishing proximate causation[106]. AI systems, particularly those using machine learning, often function as "black boxes," rendering their decision-making processes inscrutable[107].

This opacity complicates the evidentiary burden placed on plaintiffs, who must demonstrate a causal link between the algorithm's output and the harm suffered[108].

Some legal scholars advocate for a presumption of causation in favour of claimants, thereby shifting the burden of proof to the AI deployer to demonstrate the absence of a causal

---

[102] Michal S Gal, 'Algorithmic Challenges to Autonomous Choice' (2018) 25(1) MTL Rev 47.

[103] Linda Eggert, 'Autonomised Harming' in Wayne Davis and Jennifer Lackey (eds), *Philosophical Studies* (Springer 2025).

[104] Giancarlo Taddei Elmi and Sofia Marchiafava, 'Sviluppi recenti in tema di Intelligenza Artificiale e diritto: una rassegna di legislazione, giurisprudenza e dottrina' (2023) 2 RIID 11.

[105] Giuseppe Cricenti, *I principi della responsabilità civile* (Cacucci 2018).

[106] Joshua Knobe and Scott Shapiro, 'Proximate Cause Explained: An Essay in Experimental Jurisprudence' (2021) 88(1) UCL Rev 71.

[107] Walter A Mostowy, 'Explaining Opaque AI Decisions, Legally' (2020) 35(4) BTLJ 40.

[108] Mohan K Mannava, 'Causal Inference in AI Based Decision Support: Beyond Correlation to Causation' in *Proceedings of the Fourth International Conference on Ubiquitous Computing and Intelligent Information Systems* (IEEE 2024) 6.

connection[109]. This shift aligns with broader doctrinal trends in product liability and medical malpractice, where evidentiary asymmetries justify procedural adjustments to protect injured parties. Moreover, the standard of care applicable to AI-driven decision-making is evolving. Courts may assess the reasonableness of the AI system's design, the adequacy of testing and monitoring protocols, and the foreseeability of the harm caused.

In this context, the emergence of "ex ante" regulatory standards plays a crucial role in defining the expectations of AI governance[110]. Compliance with these standards may serve as a defence against tort claims, while deviation could constitute prima facie evidence of negligence.

The intersection of AI and tort liability requires a recalibration of traditional doctrines to account for the distinctive characteristics of autonomous decision-making systems.

The legal responses vary across jurisdictions, reflecting divergent policy choices between protecting injured parties and fostering technological innovation. Nevertheless, a coherent framework must balance these interests while ensuring that victims of AI-driven harm retain effective avenues for redress.

8. Product liability in the age of AI systems

The advent of artificial intelligence in consumer and industrial applications necessitates a reassessment of conventional product liability frameworks[111]. In private law, product liability typically imposes responsibility on manufacturers[112], distributors[113], and sellers[114] for harm caused by defective products. However, the unique characteristics of AI systems—such as their capacity for autonomous decision-making and continuous learning—challenge the adequacy of existing legal doctrines grounded in static, human-designed products.

---

[109] Rūta Liepiņa, Adam Wyner, Giovanni Sartor and Francesca Lagioia, 'Argumentation Schemes for Legal Presumption of Causality' in *ICAIL '23: Proceedings of the Nineteenth International Conference on Artificial Intelligence and Law* (Proceeding 2023).

[110] Gianclaudio Malgieri and Frank Pasquale, 'From Transparency to Justification: Toward Ex Ante Accountability for AI' (2022) BLSLSRPS 712, 27.

[111] Greg Swanson, 'Non-Autonomous Artificial Intelligence Programs and Products Liability: How New AI Products Challenge Existing Liability Models and Pose New Financial Burdens' (2019) 42 SUL Rev 22.

[112] Friedrich Kessler, 'Products Liability' (1967) 76(5) YLJ 52.

[113] Frank J Cavico Jr, 'The Strict Tort Liability of Retailers, Wholesalers, and Distributors of Defective Products' (1987) 12(1) NL Rev 34.

[114] Gaylord A Jentz, 'The Increasing Legal Responsibility of the Seller in Products Liability' (1966) 4 ABLJ 22.

The legal question thus arises: to what extent can AI systems be treated as "products" within the meaning of product liability regimes, and how should liability be apportioned when harm results from their operation[115]?

In civil law jurisdictions, product liability is generally governed by statutory regimes that impose strict liability on manufacturers for defective products. This model, which obviates the need to prove negligence, is based on the principle that those who profit from placing products on the market should bear the risks associated with their defects[116].

However, AI systems complicate the traditional tripartite classification of defects[117]—design defects, manufacturing defects, and warning defects—due to their capacity for autonomous adaptation. For instance, an AI system may function as intended at the point of sale but evolve in a manner that subsequently causes harm. This raises the question of whether liability attaches to the original developer, the entity responsible for system updates, or the user overseeing the AI's deployment.

One of the principal challenges lies in defining the point at which an AI system becomes "defective"[118]. Traditional product liability regimes focus on defects existing at the time the product enters the market[119]. However, in the case of machine-learning algorithms, harm may arise from post-market evolution, making it difficult to identify a singular moment of defectiveness[120]. Some legal scholars advocate for a dynamic interpretation of product defect, extending liability to encompass foreseeable harms resulting from the system's adaptive processes[121]. Others suggest the adoption of a sui generis liability regime tailored specifically to AI technologies[122], recognising their departure from traditional product paradigms.

Another contentious issue is the allocation of liability among the various actors involved in the AI lifecycle. In the context of AI-driven products, multiple parties contribute to the system's functionality, including developers, software engineers, data providers, and end-users[123].

---

[115] Kathryn Bosman Cote, 'Outsmarting Smart Devices: Preparing for AI Liability Risks and Regulations' (2024) 25(1) SDILJ 40.
[116] Steven Shavell and AM Polinsky, 'The Uneasy Case for Product Liability' (2010) 123(6) HL Rev 56.
[117] Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer, ibid 61.
[118] Miriam C Buiten, ibid 48.
[119] Richard A Epstein, 'The Unintended Revolution in Product Liability Law' (1989) 10(8) CL Rev 29.
[120] Mark Geistfeld, *Products Liability Law* (Aspen 2021).
[121] Ex multis: Nasir Muftić, 'Liability Within the Wider Framework' in Artificial Intelligence and Tortious Liability: European Union and Its Neighbours in a Globalized World (Springer 2025) 21, 45.
[122] Uchenna Nnawuchi and Carlisle George, 'Decoding Accountability: The Importance of Explainability in Liability Frameworks for Smart Border Systems' (2025) 28(64) DC 19.
[123] Nasir Muftić, 'Allocation of Liability', ibid 121.

This complex supply chain dilutes the attribution of responsibility, challenging the application of conventional product liability rules. Some legal systems respond by adopting joint and several liability, enabling injured parties to seek redress from any liable entity[124].

However, concerns arise regarding the fairness of imposing liability on downstream actors, such as distributors, who may lack the technical capacity to foresee or mitigate algorithmic risks. Furthermore, the evidentiary burden of proving defect and causation is heightened in the case of AI systems[125]. The opacity of algorithmic processes—the so-called "black box" problem—complicates a claimant's ability to demonstrate the causal nexus between the AI's functioning and the resultant harm. To address this, certain scholars propose reversing the burden of proof, requiring the AI producer to disprove defectiveness once a claimant establishes prima facie evidence of harm[126]. This evidentiary shift aligns with broader trends in consumer protection law, which prioritise access to remedies over rigid fault-based principles.

Product liability in the age of AI demands a recalibration of existing legal frameworks to accommodate the distinctive risks posed by autonomous and adaptive technologies. Whether through the reinterpretation of existing doctrines or the creation of bespoke liability regimes, legal systems must ensure that injured parties maintain access to effective redress while fostering an environment conducive to technological innovation. This balancing act is essential to uphold the foundational principles of private law while responding to the novel challenges posed by AI-driven products.

9. Causal uncertainty and proof of damage in AI-driven systems

The integration of artificial intelligence into everyday processes has intensified the complexity of establishing causal links and proving damage under private law[127].

Traditional liability regimes are predicated upon the claimant's ability to demonstrate a clear causal connection between the wrongful conduct and the resulting harm[128]. However, AI systems—particularly those employing machine-learning models—operate through opaque and dynamic mechanisms that obfuscate causal relationships. This "black box" effect poses

[124] Bart Custers, Henning Lahmann and Benjamyn I Scott, ibid 65.
[125] David Fernández Llorca et al, 'Liability Regimes in the Age of AI: A Use-Case Driven Analysis of the Burden of Proof' (2023) 76 JAIR 31.
[126] Ex multis: Peter Rott, 'Digital Fairness and the Burden of Proof' (2025) JCP 18.
[127] Yaniv Benhamou and Justine Ferland, 'Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages' in Pina D'Agostino, Carole Piovesan and Aviv Gaon (eds), *Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law* (Thomson Reuters 2020).
[128] James Fleming Jr and Roger F Perry, 'Legal Cause' (1951) 60(5) YLJ 51.

significant challenges to the evidentiary framework underpinning private law, especially in cases where the harm is the product of algorithmic decision-making.

In civil law systems, the principle of causation typically follows a bifurcated analysis[129], distinguishing between factual causation (causa efficiens)[130] and legal causation (causa juridica)[131]. Factual causation is assessed through the conditio sine qua non test[132], which asks whether the harm would have occurred "but for" the defendant's conduct. Legal causation, on the other hand, limits liability to consequences that are foreseeable and sufficiently proximate. Yet, in the context of AI, these well-established tests falter due to the system's capacity for autonomous learning and unpredictable outcomes. For instance, an AI-powered medical diagnostic tool may evolve beyond its initial programming, producing erroneous outputs without any identifiable human error[133]. This raises the question of how to allocate liability when the causal chain is obscured by algorithmic complexity.

A core difficulty lies in proving the existence of a direct causal link when AI systems act as independent intermediaries between human input and tangible harm[134]. Traditional legal frameworks rely on human agency as the locus of responsibility[135]; yet AI disrupts this model by performing actions without direct human oversight. As a result, legal scholars have proposed various adaptations to the causation standard. One emerging approach is the adoption of a "probabilistic causation" model[136], whereby courts accept statistical evidence to infer causation where direct proof is unattainable. This approach, while facilitating claims involving complex technologies, raises concerns about eroding the presumption of innocence and diluting the burden of proof in civil litigation.

Another proposed solution involves reversing the burden of proof in cases where algorithmic opacity prevents the claimant from establishing causation. Under this model, once the claimant demonstrates prima facie evidence of harm, the burden shifts to the defendant—typically the

---

[129] Pier Giuseppe Monateri, Davide Gianti and Mauro Balestrieri, 'Causazione e giustificazione del danno' in Pier Giuseppe Monateri (ed), *Trattato sulla responsabilità civile* (Giappichelli Editore 2016).

[130] Richard Wright, 'The New Old Efficiency Theories of Causation and Liability' (2015) 7(1–2) JTL 30.

[131] Sarah Green, *Causation in Negligence* (Hart Publishing 2015).

[132] Fabrizio Piraino, 'Causalità (nesso di) nella responsabilità civile: B) Profili applicativi' in Claudio Scognamiglio (ed), *Enciclopedia del diritto. I Tematici VII-2024: Responsabilità civile* (Giuffrè 2024).

[133] Michelle M Mello and Neel Guha, 'Understanding Liability Risk from Using Health Care Artificial Intelligence Tools' (2024) 390(3) NEJM 7.

[134] Karen Yeung, 'A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility Within a Human Rights Framework' MSI-AUT 5 (Council of Europe 2018) 94.

[135] Erik Lagerstedt, Maria Riveiro and Serge Thill, 'Agent Autonomy and Locus of Responsibility for Team Situation Awareness' in HAI '17: Proceedings of the 5th International Conference on Human Agent Interaction (ACM 2017) 8.

[136] Jos Lehmann, Joost Breuker and Bob Brouwer, 'Causation in AI and Law' (2006) 12 AIL 36.

AI producer or operator—to disprove a causal link[137]. Such an approach aligns with broader principles of consumer protection and recognises the informational asymmetry inherent in AI litigation.

Moreover, the concept of collective liability has emerged as a response to causal indeterminacy in AI-related harm. This model reflects a "risk-based" approach whereby liability is distributed across all entities involved in the AI's design, development, and deployment. Such a framework ensures compensation for injured parties without requiring precise identification of the causal agent. However, collective liability risks overburdening peripheral actors who may lack meaningful control over the AI's behaviour, raising concerns about fairness and the equitable distribution of legal responsibility.

The issue of damage quantification also becomes more intricate in the context of AI-driven harm[138]. In private law, compensation is generally tied to the principle of full reparation, which aims to restore the injured party to the position they would have occupied but for the wrongful act[139]. However, AI-generated harm may manifest in novel forms - such as algorithmic discrimination[140] or reputational damage[141] - that defy conventional categories of pecuniary and non-pecuniary loss.

The intersection of causal uncertainty and AI-driven harm necessitates a reconfiguration of the evidentiary and liability paradigms in private law. Whether through probabilistic models, burden-shifting doctrines, or collective liability frameworks, legal systems must adapt to ensure effective redress for claimants while preserving fundamental principles of fairness and legal certainty. As AI technology continues to evolve, so too must the legal mechanisms that govern its societal impact, striking a balance between fostering innovation and upholding the core tenets of private law.

Conclusion

[137] Susana Navas, 'Producer Liability for AI-Based Technologies in the European Union' (2020) 9(1*)* ILR 8.
[138] Frank S Giaoui, 'From Causal Inferences to Predictive Analytics: Using AI to Settle on Damages' (2024) 25(1) JMPP 124.
[139] For a critical review, see: Cesare Salvi, 'Il risarcimento integrale del danno non patrimoniale, una missione impossibile. Osservazione sui criteri per la liquidazione del danno non patrimoniale' (2014) 3 EDP 15.
[140] Frederik Zuiderveen Borgesius, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (Council of Europe 2018) 94.
[141] Matthias Holweg, Rupert Younger and Yuni Wen, 'The Reputational Risks of AI' (2022) 64 CM Rev 12.

The advent of artificial intelligence in public surveillance has posed unique and complex challenges to the traditional frameworks of civil law[142]. AI can improve public security but raises serious concerns over fundamental rights, especially privacy and freedom.

This tension between technological innovation and the safeguarding of individual freedoms is at the heart of the legal debate surrounding AI regulation[143].

From a civil law perspective, existing legal mechanisms, such as the General Data Protection Regulation (GDPR) and national civil codes, provide important protections for personal data and privacy. However, these legal instruments face significant challenges in adapting to the rapid evolution of AI technologies[144]. The opacity of AI algorithms, the risk of algorithmic bias, and the complexities of assigning responsibility for harm caused by automated decision-making highlight the inadequacies of current legal frameworks in fully addressing the risks posed by AI-driven surveillance[145].

In particular, the principle of transparency—central to both the GDPR and civil liability regimes—remains a critical issue in the regulation of AI surveillance systems. The "black box" problem, wherein the decision-making processes of AI systems are not fully understood by either the individuals affected or the entities deploying the technology, underscores the need for clearer regulatory standards. The current inability to guarantee algorithmic accountability[146], especially when it comes to discriminatory outcomes or violations of privacy, poses significant risks to the legal protection of individuals.

Furthermore, while contractual and extra-contractual liability frameworks provide some recourse for harm caused by AI systems[147], the complexity of attributing fault in the context of autonomous decision-making necessitates the development of a more tailored liability regime[148]. The application of strict liability, vicarious liability, and more transparent standards

---

[142] Benjamin Alarie, Anthony Niblett and Albert HY Yoon, 'How Artificial Intelligence Will Affect the Practice of Law' (2018) 68(1) UTLJ 18.

[143] Jędrzej Niklas and Lina Dencik, 'What Rights Matter? Examining the Place of Social Rights in the EU's Artificial Intelligence Policy Debate' (2021) 10(3) IP Rev 29.

[144] Aleksandr Kesa and Tanel Kerikmäe, 'Artificial Intelligence and the GDPR: Inevitable Nemeses?' (2020) 10(3) TTJES 22.

[145] Lyytinen Lescrauwaet et al, 'Adaptive Legal Frameworks and Economic Dynamics in Emerging Technologies: Navigating the Intersection for Responsible Innovation' (2022) 16(3) LE 18.

[146] Reuben Binns, 'Algorithmic Accountability and Public Reason' in Luciano Floridi (ed), *Philosophy & Technology* (Springer 2017).

[147] Jan De Bruyne, Orian Dheu and Charlotte Ducuing, 'The European Commission's Approach to Extra-Contractual Liability and AI – An Evaluation of the AI Liability Directive and the Revised Product Liability Directive' (2023) 51 CLS Rev 20.

[148] Tomasz Braun, 'Liability for Artificial Intelligence Reasoning Technologies – A Cognitive Autonomy That Does Not Help' (2025) CG 18.

for determining responsibility in AI governance are essential to ensure that those who deploy AI systems are held accountable for the harm they cause.

Looking forward, it is evident that a comprehensive, multi-dimensional regulatory approach is required to address the challenges of AI surveillance[149]. While existing legal frameworks provide a foundation, they must be adapted and extended to meet the specific needs posed by AI technologies. Proposals for more robust regulation should focus on enhancing algorithmic transparency, ensuring stronger safeguards against discriminatory biases, and establishing clearer liability regimes for AI-related harm.

To this end, regulators must take proactive steps to develop new legal standards that are flexible and adaptable to the rapid pace of technological change. This includes exploring innovative regulatory tools, such as real-time oversight mechanisms, mandatory impact assessments, and the establishment of independent auditing bodies to ensure compliance with privacy protections and human rights standards[150]. Furthermore, the adoption of international standards for AI regulation is critical in ensuring that legal protections are consistent across jurisdictions and that global cooperation can address the cross-border challenges posed by AI technologies.

In conclusion, balancing the advancement of AI technologies with the protection of fundamental rights requires a nuanced and proactive legal approach[151]. While AI surveillance has the potential to contribute significantly to public safety, it must not come at the expense of individual freedoms. The future of AI regulation must centre on ensuring that technology serves the public good while respecting the core principles of justice, fairness, and human dignity.

Ultimately, the integration of AI into critical decision-making processes demands not only sector-specific adaptations, but a coordinated legislative strategy that places legal clarity, human rights protection, and technological accountability at the heart of future regulatory frameworks.

[149] MD Jewel Ali, 'AI and the Legal Frontier: Balancing Innovation and Challenges in the Age of Artificial Intelligence' (2024) 2(3) LFIJDLR 23.

[150] Xukang Wang and Ying Cheng Wu, 'Balancing Innovation and Regulation in the Age of Generative Artificial Intelligence' (2024) 14 JIP 31.

[151] Venkata Rajesh Krishna Adapa, 'Navigating the Privacy Paradox: Balancing AI Advancement and Data Protection in the Digital Age' (2024) 10(6) Intl JSRCSEIT 11.