MenschenRechtsMagazin
Informationen | Meinungen | Analysen

ISSN 2941-1149 | 30 (2025) 2 | pp. 97–116

Contribution

International Artificial Intelligence Law to the Test of Surveillance

William Letrone[1] • Tony Cabus[2]

[1]DCS, Nantes University, CNRS
[2]Walther-Schücking Institute for International Law, Kiel

Contents

Abstract

This paper takes a broad look at the privacy implications of emerging supranational frameworks on artificial intelligence (AI), taking AI-driven surveillance by the private and public sectors as a case example of privacy-adverse practices. To do so, this paper first examines the relationship between AI technologies and surveillance practices, highlighting the privacy risks raised by corporate surveillance and state surveillance. The paper then recalls the scope and content of privacy, before pinpointing remaining gaps in emerging frameworks on AI that stand in the way of achieving robust privacy guarantees in the context of AI-driven surveillance.

Keywords

Privacy, Surveillance, Artificial intelligence, International law, Digital law

Citation:
William Letrone/Tony Cabus, International Artificial Intelligence Law to the Test of Surveillance, in: MRM 30 (2025) 2, pp. 97–116.
https://doi.org/10.60935/mrm2025.30.2.26.

Received: 2025-07-04
Accepted: 2025-11-21
Published: 2026-02-17

"Man has become a document like any other, with an identity that he no longer 'owns', over which he has little control (...) and whose commercial purpose he underestimates."*[1]

I. Introduction

What are the privacy implications of emerging supranational frameworks on artificial intelligence (hereinafter AI)[2]? Especially since the release of generative AI, there have been multiple calls to action for addressing the risks posed by the deployment and use of AI systems. In many instances, these calls were followed by non-binding initiatives and technology-specific frameworks intended to complement existing frameworks such as data-protection regulations.

Initiatives such as the European Union's latest Artificial Intelligence Act (AI Act)[3] and the Council of Europe's Framework Convention on AI (Framework Convention) are most welcome. The other option, self-regulation by the tech sector, mostly through soft law, is not desirable due to the underlying economic interests driving their activities. Binding rules are preferable to soft law instruments, although the speed at which the sector is evolving requires that caution be exercised throughout any legislative processes taken to this end. Furthermore, many AI-driven activities know no border. Regulating technologies of such transnational nature requires concerted regulatory efforts at the global level.[4] Hence, the ongoing "rush to AI regulation"[5] is an opportunity to collectively address longstanding privacy issues in light of technological advances in the AI domain.

Among all possible uses of AI technology, surveillance activities, as the act of "watching, listening to, or recording of an

* This paper was presented at the MenschenRechtsZentrum's 30th Anniversary Conference "Human Rights and Artificial Intelligence – Addressing challenges, enabling rights," of 7th/8th November 2024, at the panel "AI as a challenge to regulation."

1 [Translated from French by the authors]: « *L'Homme est devenu un document comme les autres, disposant d'une identité dont il n'est plus 'propriétaire' dont il ne contrôle que peu la visibilité (...) et dont il sous-estime la finalité marchande. » Ertzscheid, O.*, L'homme, un document comme les autres, in: Hermès 53 (2009), pp. 33-40 (38).

2 This work is based on the definition of AI system contained in the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Framework Convention), which is of international reach. Hence, the Convention defines AI as "a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments." See Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law of 05 September 2024, CETS No. 225 (Framework Convention), Art. 2.

3 EU Regulation 2024/1689 of 12 July 2024, OJ L, 2024/1689 (AI Act).

4 *Talita de Souza Dias/ Rashmin Sagoo*, AI Governance in the Age of Uncertainty: International Law as a Starting Point, Just Security of 2 January 2024, available at: https://www.justsecurity.org/90903/ai-governance-in-the-age-of-uncertainty-international-law-as-a-starting-point/ (last visited 16 October 2025).

5 Expression borrowed from *Nathalie Smuha*, Biden, Bletchley, and the emerging international law of AI, Verfassungsblog of 15 November 2023, available at: https://verfassungsblog.de/biden-bletchley-and-the-emerging-international-law-of-ai/ (last visited 11 November 2025) See also *Itsiq Benizri/Arianna Evers/Shanon Togawa Mercer/Ali A. Jessani*, A Comparative Perspective on AI Regulation, Lawfare of 17 July 2023, available at: https://www.lawfaremedia.org/article/a-comparative-perspective-on-ai-regulation (last visited 11 November 2025).

individual's activities"[6], constitute major sources of privacy erosion. By definition, surveillance is antithetical to privacy. Regulating corporate surveillance and state surveillance would thus go a long way in order to mitigate many privacy risks stemming from AI technology. Moreover, United Nations members have expressly called "upon all Member States and, where applicable, other stakeholders to refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights."[7] Yet, no other area encapsulates the complexities and challenges of AI technology as profoundly as the surveillance practices of the private and public sectors, since these may involve AI tools at different levels. Although the burgeoning regulatory landscape pertaining to AI reveals that legislators worldwide have identified the key challenges associated with the technology, privacy generally takes the backseat.

This paper seeks to assess how some privacy concerns raised by AI - and their underlaying causes - are actually being addressed in emerging supranational legal frameworks on AI, focussing on AI-driven surveillance. To this end, the paper starts by exploring how AI technology and digital surveillance practices intersect (II). In a second section, the paper offers an attempt to conceptualise digital privacy (III). The paper then analyses emerging AI regulations, highlighting the remaining gaps when it comes to mitigating AI-driven surveillance (IV). A few concluding remarks question the capacity of international human rights law to rescue privacy (V).

II. AI systems for digital surveillance

Public and private actors are increasingly resorting to AI in their surveillance apparatus.[8] This part examines AI uses in the context of digital surveillance, starting with digital surveillance by the private sector, or "corporate surveillance" (1), before moving to digital surveillance by the public sector, or "state surveillance" (2).

1. AI in corporate surveillance

"Corporate surveillance" is a synonym of "surveillance capitalism", a term famously coined by Harvard Professor *emerita* Shoshana Zuboff, which she defined as "the unilateral claiming of private human experience as free raw material for translation into behavioural data."[9]

"Surveillance capitalism" thus refers to a paradigm where individuals' behaviours are tracked, their desires inferred and anticipated based on the information collected from them, for the purpose of steering consumption habits. When describing

[6] *Daniel J. Solove*, A Taxonomy of Privacy, in: University of Pennsylvania Law Review 154 (2006), pp. 477-560 (490).

[7] UN Doc. A/RES/78/265, para. 5.

[8] *Steven Feldstein*, The Global Expansion of AI Surveillance, Working Paper, Carnegie Endowment for International Peace, 2019, p. 6.

[9] *John Laidler*, High tech is watching you, The Harvard Gazette of 4 March 2019, available at: https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/ (last visited 11 November 2025); See also *Joseph Jones*, Don't Fear Artificial Intelligence, Question the Business Model: How Surveillance Capitalists Use Media to Invade Privacy, Disrupt Moral Autonomy, and Harm Democracy, in: Journal of Communication Inquiry 49 (2024), pp. 6-26 (9).

the advent of surveillance capitalism, authors speak of the "commodification" of both data and attention. Corporate surveillance proceeds from the dehumanizing rationale that economic value can (and must) be attached respectively, to users' data and attention.[10] While the underlying logics of corporate surveillance were already present in the advertising industry,[11] the ubiquity of AI surveillance tools makes it a more concerning trend today.

To commit corporate surveillance, digital companies rely on vast amounts of information *i.e.* big data, which aggregates information from a variety of sources.[12] This data is then exploited by algorithms to derive new insights into users' personalities and routines. AI-driven behaviour prediction is a crucial component of surveillance capitalism. Its ability to translate raw data into behavioural data is precisely what makes AI technology so valuable in this context, because it allows companies to predict users' behaviours with the highest degrees of accuracy. The ensuing practices are often justified on the grounds of more tailored advertising, richer service offerings, or the free enjoyment of certain services. In this context, "Privacy is now less a line in the sand beyond which transgression is not permitted, than a shifting space of negotiation where privacy is traded for products, better services or special deals."[13]

The resulting data commodification paradigm has been criticized for leaving individuals with no meaningful ways to consent to data collection, lack of legal protection regarding the inferences made from the bulk data collected, and lack of information regarding the processing and the parties involved.[14] At a more abstract level, corporate surveillance has been criticized for taking away users' capacity for judgement.[15] The level of conditioning achieved through extreme content personalisation results in users gradually losing the ability to ponder over choice. In the long term, these mechanisms are detrimental to privacy and individual autonomy.[16]

---

[10] *Evgeny Morozov*, The Real Privacy Problem, MIT Technology Review of 22 October 2013, available at: https://www.technologyreview.com/2013/10/22/112778/the-real-privacy-problem/ (last visited 11 November 2025). See also, generally, *Jerome Joseph*, Big-data: catalyst for a privacy conversation, in: Indiana Law Review 48 (2014), pp. 213–242 (234). See also *Jones* (fn. 9).

[11] See, generally, *Yahya Alshamy et al.*, Surveillance Capitalism & the Surveillance State: A Comparative Institutional Analysis, in: Constitutional Political Economy 23 (2024), pp. 1-38.

[12] *Heather Suzanne Woods*, Asking more of Siri and Alexa: feminine persona in service of surveillance capitalism, in: Critical Studies in Media Communication 35 (2018), pp. 1–16 (12). See also *Hao-Ping Lee et al.*, Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks, CHI'24: Proceedings of the CHI Conference on Human Factors in Computing Systems, 11 May 2024, pp. 1-19 (10).

[13] *Kevin D Haggerty/Richard Ericson*, The surveillant assemblage, in: British Journal of Sociology 51 (2000), pp. 605-622 (616).

[14] See, generally, *Jane Andrew/Max Baker*, The General Data Protection Regulation in the Age of Surveillance Capitalism, in: Journal of Business Ethics 168 (2019), pp. 565-578.

[15] *Laidler* (fn. 9). See also *Joseph* (fn. 10), p. 221.

[16] It will be shown later that the privacy harms resulting from these mechanisms relate to decisional privacy and informational privacy. A definition of both of these values is proposed in the next section. On this point, see *Joseph* (fn. 10). See also, generally, *Lena Vatne Bjørlo*, Freedom from interference: Decisional privacy as a dimension of consumer privacy online, in: AMS Review 14 (2024), pp. 12–36. And see generally, *Yuxi Wu et al.*, The Slow Violence of Surveillance Capitalism: How Online Behavioral Advertising Harms People, FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (2023), pp. 1826–1837. And see *Daniel J. Solove*, Artificial intelligence and Privacy, in: Florida Law Review 77 (2025), pp. 1-73 (46).

Of course, the convergence of big data and AI technology raised concerns before the emergence of generative AI.[17] AI technology was at work in the mechanisms involved in corporate surveillance very early on, in the form of predictive technology embedded into home and on-device assistants to gather data, and profiling algorithms designed to provide actionable insight into the habits of an individual and thus enable decision-making.[18] Today, technological advances in the AI domain enable marketers and data scientists to collect more information, to make sense of larger volumes of data, and to infer granular knowledge about users.[19] When it comes to generative AI in particular, the technology is notably used to power virtual companions[20] or digital versions of deceased loved ones.[21] These applications are controversial for many reasons, including from a privacy standpoint, as they may lead to the divulgation of very intimate data, thereby enabling higher levels of surveillance.

The wealth of data detained by the largest digital platforms makes them useful partners for governments. While the private sector may not always be aware of a state's tapping their databases, the private sector sometimes willingly cooperates with public agencies in state surveillance, repurposing commercial databases to accommodate the security needs of governments. For instance, China's state surveillance apparatus relies heavily on the private sector for the constitution of databases.[22] In the famous NSA surveillance case, US Telecom company AT&T reportedly copied and transmitted the communications of its consumers to government authorities.[23] Similarly, in the facts leading to ECJ's "*BCD case*", bulk communications data (BCD) was collected by the Security and Intelligence Agencies from mobile network operator,[24] and US Supreme Court's *United States v. Miller* case featured the communication of a bank's client information to US government agencies.[25]

2. AI in state surveillance

The term "surveillance state" is used to describe a model of governance relying on

[17] Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, 2019, available at: https://search.coe.int/cm?i=090000168092dd4b (last visited 16 October 2025).

[18] *Laidler* (fn. 9), p. 6; For a definition of 'profiling' see Art. 4 para. 4 of Regulation (EU) 2016/679 of 4 May 2016, OJ L 119, p. 1. For a more in-depth account on profiling, see *Klaus Wiedemann*, Profiling and (automated) decision-making under the GDPR: A two-step approach, in: Computer Law & Security Review 45 (2022), pp. 1-17 (3).

[19] See *Mireille Hildebrandt/Bert-Jaap Koops*, The challenges of ambient law and legal protection in the profiling era, in: Modern Law Review 73 (2010), pp. 428-460 (435).

[20] *Jessica Lucas*, The teens making friends with AI chatbots, The Verge of 4 May 2024, available at: https://www.theverge.com/2024/5/4/24144763/ai-chatbot-friends-character-teens (last visited 6 November 2025).

[21] *Zeyi Yang*, Deepfakes of your dead loved ones are a booming Chinese business, MIT Technology Review of 7 May 2024, available at: https://www.technologyreview.com/2024/05/07/1092116/deepfakes-dead-chinese-business-grief/ (last visited 6 November 2025).

[22] See, generally, *Fan Liang et al.*, Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure, in: Policy & Internet Special Issue: Social Media and Big Data in China 10 (2018), pp. 415-453.

[23] NSA Spying, Electronic Frontier Foundation, available at: https://www.eff.org/fr/nsa-spying (last visited 6 November 2025).

[24] ECJ, judgement of 6 October 2020, Case C-623/17, para. 25.

[25] Supreme Court of the United States of America, *United States v. Miller*, judgement of 21 April 1976, 425 U.S. 435 (1976).

pervasive surveillance tools to collect and analyse information about citizens for the purpose of anticipating crime, securing public spaces, and, more broadly, maintaining national security. State surveillance may be conducted through either digital or analogue means, although the increase in international terrorism in the 2000s and the subsequent digitization of society led to a generalization of the recourse to digital surveillance techniques. A prominent illustration of the surveillance state model is the extensively-documented national surveillance apparatus of the National Security Agency (NSA).[26]

Corporate surveillance and state surveillance share some similarities, the first being the mechanisms at play *i.e.* the massive collection and analysis of data, usually implicating AI solutions. Second, the imbalance of power that characterizes the relationship between individuals, states and private actors means that the former are usually left with few means to resist surveillance, let alone the coercive power it enables. Third, the two surveillances may have a negative impact not only on privacy, but also on other fundamental rights such as free speech. Finally, there are no *pure* surveillance capitalists nor *pure* surveillance states, but a handful of business and governance models involving varying degrees of privacy intrusion.

The end goals are however dissimilar between the two types of surveillance. Indeed, while corporate surveillance seeks economic advantage by steering positive behaviour, state surveillance seeks national stability by discouraging them. Of the two, state surveillance may appear more justifiable, which has notably led some authors warning against thinking of surveillance as a "malign plot hatched by evil powers."[27] For instance, state surveillance was useful in the context of the spread of the coronavirus during the pandemic. Yet, as pointed by Solove, "Too much social control, however, can adversely impact freedom, creativity, and self-development."[28] In the same vein, the independent high-level expert group on artificial intelligence appointed by the EU Commission emphasized the delicate process of striking a balance between the prevention of harm through surveillance practices and the protection of privacy and autonomy.[29]

Much like the former, state surveillance is the subject of increasing attention because of the growing reliance of states on AI surveillance tools.[30] AI technology is at play in several mechanisms of state surveillance, where it can be used to perform various image processing tasks such as object and behaviour detection in order to predict scenarios, so-called "algorithmic surveillance." Arguably more problematic, AI technology can also be leveraged to execute surveillance activities such as biometric identification, emotion recognition and biometric categorization for law enforcement.

The use of AI tools for the purpose of conducting state surveillance activities is problematic for a number of reasons. In 2023, the UN High-Level Advisory Body on Artificial Intelligence singled-

[26] *David Lyon*, Surveillance, Snowden, and Big Data: Capacities, consequences, critique, in: Big Data & Society 1 (2014), pp. 1-13 (2).

[27] *Kirstie Ball et al.*, A Report on the Surveillance Society, 2006, p. 4.

[28] *Solove* (fn. 6), p. 494.

[29] European Commission, Ethics Guidelines for Trustworthy AI, 8 April 2019, p. 13.

[30] *Feldstein* (fn. 8).

out real-time biometric surveillance for law enforcement purpose as posing an "unacceptable risk, violating the right to privacy."[31] Alongside the serious risk of biased outputs,[32] one main issue with the inclusion of AI technology into a state's surveillance apparatus is its ability to infer large quantities of information about physical persons based on the captured images. The French data protection authority speaks of a trend towards generalized "analysis", as opposed to the initial generalized surveillance.[33] Such analysis leads to what Lyon calls "anticipatory governance", where surveillance is "less concerned with the overall picture of a given individual as with 'premeditating and pinpointing potential dangers.'"[34] In this context, the likelihood of errors and misuse is significant.

Unfortunately, the level of data transparency exhibited by surveillance activities is often lacking, preventing many from fully grasping the true extent of personal information private companies and states can extract from a few data points, how their data weighs in surveillance outcomes, and more broadly, the impact surveillance activities may have on their private lives. In this context, privacy and by extension human autonomy and dignity, cannot be properly guaranteed.[35]

III. Beyond data protection; making sense of privacy in the digital era

The right to privacy is considered "one of the foundations of a democratic society."[36] This part offers a brief background to privacy, (1) before exploring the subset concept of digital privacy, (2) in order to explicate the nature of the legal harm resulting from surveillance activities.

1. Background to privacy

Given its prominent role in modern societies, the right to privacy is enshrined in many authoritative sources. At the international level, the right to privacy is enshrined in Art. 12 of the 1948 Universal Declaration of Human Rights[37] and Art. 17 of the 1966 International Covenant on Civil and Political Rights[38], both providing in identical terms; "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[39] The right to privacy

[31] United Nations Advisory Body on Artificial Intelligence, Interim Report: Governing AI for Humanity, December 2023, para. 29.

[32] *Jacob Snow*, Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots, ACLU of 26 July 2018, available at https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28 (last visited 20 October 2025).

[33] *Commission Nationale de l'Informatique et des Libertés* (CNIL), Position sur les conditions de déploiement cameras dites "intelligentes" ou "augmentées" dans les espaces publics, 2022, p. 9.

[34] *Lyon* (fn. 26), quoting *Marieke de Goede*, The politics of privacy in the age of pre-emptive security, in: International Political Sociology 8 (2014), pp. 100–104 (102).

[35] *Bjørlo* (fn. 16).

[36] UN Doc. A/HRC/RES/28/16, p. 2.

[37] Universal Declaration of Human Rights of 10 December 1948, UN Doc. A/RES/217 A (III) (UDHR), Art.12.

[38] International Covenant on Civil and Political Rights of 16 December 1966, UNTS vol. 999, p. 171 (ICCPR), Art. 17.

[39] Ibid.; UDHR, Art. 12.

is also replicated in Art. 7 of the Charter of Fundamental Rights of the European Union[40], Art. 8 of the European Convention on Human Rights[41], Art. 21 of the ASEAN Human Rights Declaration[42], and Art. 11 of the American Declaration of the Rights and Duties of Man[43], among other important documents.

Despite its ubiquity, the right to privacy remains an elusive concept. In 2006 Solove observed "[P]rivacy is a concept in disarray. Nobody can articulate what it means"[44] Almost twenty years later, privacy remains "a complicated concept to review"[45] This is due to the fact that privacy is inherently a protean concept. Privacy applies both horizontally, in person-to-person settings, and vertically, in institutions-to-person settings. Each context brings different expectations towards the conduct of external parties.[46]

In legal doctrine, privacy is apprehended simultaneously as a primary right susceptible of direct violation and as a source of more specific rights, the violation of which doubles as privacy infringement, such as with the right to protect reputation or the right to abortion.[47] The right to privacy is also an enabler of other rights and values. Hence, free speech, consumer protection and the right to public participation cannot exist without sufficient privacy guarantees.[48] But its intricate relationship with other rights and freedoms is not the sole source of difficulties when it comes to defining the concept of privacy.

Indeed, privacy and the protections stemming from it are in constant evolution. The social demand for privacy is itself in a state of flux, and varies based on societal, cultural and technological factors.[49] In addition, the right to privacy is not absolute because it admits exceptions that may differ from one domestic system to another. In fact, while, it would seem that most states are aware of the importance of safeguarding privacy, they do not necessarily approach it the same way. Take the example of the freedom of the press, which, until recently, was given primacy over privacy in the UK, while privacy had long prevailed over the freedom of the press in France.[50]

---

[40] European Union, Charter of Fundamental Rights of the European Union of 14 December 2007, 2012/C 326/02, Art. 7.

[41] Council of Europe, European Convention on Human Rights of 4 November 1950, as amended by Protocols Nos. 11, 14 and 15, ETS No. 005, Art. 8.

[42] Association of Southeast Asian Nations (ASEAN), ASEAN Human Rights Declaration of 18 November 2012, Art. 21.

[43] Inter-American Commission on Human Rights (IACHR), American Declaration of the Rights and Duties of Man of 02 May 1948, Art. 11.

[44] *Solove* (fn. 6), p. 477.

[45] See, generally, *Ali ALibeigi/Abu Bakar Munir/Md Ershadul Karim*, Right to Privacy, a Complicated Concept to Review, in: Library Philosophy and Practice (e-journal) 2019, pp. 2841-2876.

[46] See notably *Joseph* (fn. 10), p. 234.

[47] See, among many other, ECtHR, *Pretty v. The United Kingdom* (2346/02), judgement of 29 April 2002, para. 61; US Supreme Court, *Roe v. Wade*, 410 U.S. 113, decision of 22 January 1973, para. 79.

[48] See notably UNHRC, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression of 17 April 2013, UN Doc. A/HRC/23/40, para. 24.

[49] *Lee A. Bygrave*, Privacy and Data Protection in an International Perspective, in: Scandinavian Studies in Law 56 (2010), pp. 166–200 (174). *Samuel D. Warren/Louis D. Brandeis*, The Right to Privacy, in: Harvard Law Review 4 (1890), pp. 193-220 (195). See also ibid.

[50] *Kathryn F. Deringer*, Privacy and the Press: The Convergence of British and French Law in Accordance with the European Convention of Human Rights, in: Penn State International Law Review 22 (2003), pp. 191-211 (192).

Few legal instruments provide a clear definition of privacy. As remarked by the European Court of Human Rights (ECtHR) in *Pretty v. The U.K; "[...]* the concept of 'private life' is a broad term not susceptible to exhaustive definition."[51] Solove similarly states that "the term 'privacy' is an umbrella term, referring to a wide and disparate group of related things."[52] Be that as it may, the basic premises of privacy remain relatively discernible.

2. Digital privacy defined

Overall, privacy cases around the world have drawn from three theories of privacy; non-intrusion, self-determination, (or non-interference), and control over one's information.[53] Each theory highlights one dimension of privacy: the *physical*, the *decisional* and the *informational* dimension, which complement each other in different ways.[54] Exploring pivotal case law on privacy provides valuable insights into its three dimensions.

In 1890 US lawyers Samuel D. Warren and Louis Brandeis famously referred to the right to privacy as the "right to be let alone",[55] a rather rudimentary understanding of privacy mainly interpreted in the context of the relationship between the administration and individuals. The concept was directly drawn from the fourth US constitutional amendment, which recognizes the right "[...]to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, [...]"[56] The view was later criticized for being "both too broad and too narrow to count as a successful definition."[57] Still, the definition evokes the physical dimension of privacy: a safeguard for the physical premises of a person, or *physical privacy*.

Privacy does not only relate to the physical premises of a person, but extends to intangible values, such as one's ability to make choices and take decisions regarding intimate matters without interference, or *decisional privacy*.[58] Building on a longstanding jurisprudence, the US Supreme Court for example considered in the oft-cited 1973 *Roe v. Wade* case that the right to abortion was encompassed in the right to privacy.[59] Similarly, decisional privacy has been an important part of the jurisprudence of the European Court of Human Rights stemming from Art. 8 ECHR, notably in connection to family matters.[60] At present, it is receiving increasing inten-

[51] ECtHR (fn. 47), para. 61. And see ECtHR, *Niemietz v. Germany* (13710/88), judgement of 16 December 1992, para. 29. See also, an analysis of the relevant jurisprudence, at *Raphaël Gellert/Serge Gutwirth*, The legal construction of privacy and data protection, in: Computer Law & Security Review 29 (2013), pp. 522–530. For a thorough analysis of the different theories of privacy, see *Herman T. Tavani*, Philosophical Theories of privacy: implications for an adequate online privacy policy, in: Metaphilosophy 38 (2007), pp. 1-22 (6).

[52] *Solove* (fn. 6), p. 485.

[53] *Tavani* (fn. 51), p. 7.

[54] *Bjørlo* (fn. 16).

[55] *Warren/Brandeis* (fn. 49), p. 193.

[56] Constitution of the United States of America of 17 September 1787, Amendment IV.

[57] *James H. Moor*, The ethics of privacy protection, in: Library Trends 39 (1991), pp. 69–82 (71). See also *Tavani* (fn. 51).

[58] Ibid., p. 72. See also *Tavani* (fn. 51), p. 6.

[59] US Supreme Court, *Roe v. Wade,* 410 U.S. 113, decision of 22 January 1973.

[60] See for instance, ECtHR, *Schalk and Kopf v. Austria* (30141/04), judgement of 24 June 2010. See also *Bart van der Sloot*, Decisional privacy 2.0: the procedural requirements implicit in Art. 8 ECHR and its potential impact on profiling, in: International Data Privacy Law 7 (2017), pp. 190-201.

tion in the context of corporate surveillance.[61]

The third dimension of privacy, *informational privacy*, applies to situations implicating personal information, for instance, when one's reputation is damaged by a smear campaign or when one's personal data are being harvested without consent. Informational privacy is defined as the ability to exercise control over one's personal information, including image, correspondence and personal data. Informational privacy is sometimes referred to as "informational self-determination" or "informational autonomy."[62] The informational dimension of privacy was, for example, in question in the 2017 *Bărbulescu v. Romania* case before the ECtHR, where the Court considered that instant message communications qualified as "correspondence" protected under Art. 8 ECHR, even when sent from the workplace. In *Whalen v. Roe*, the US Supreme Court makes explicit reference to a constitutional right to informational privacy.[63] Guarantees such as the protection of reputation and data protection principles including consent, control over the data, right to erasure, and rectification of information, relate to the informational dimension privacy. These principles are covered in most data protection laws.

In light of the above, it can be asserted that the right to privacy is a claim that extends to physical locations, the body, personal decisions, and digital as well as non-digital information, as long as these closely relate to elements of the personality or the life of the rights-holder.[64]

Digital privacy, in particular, both relates to the second and third aspects of privacy. Specifically, it motivates expectations regarding the ways third parties should treat the digital components of the private sphere, and what they effectively do with them, as long as the end goals have repercussions on their autonomy, taking into account the invasive nature of the technologies at play. In that sense, digital privacy acts as a defence against attempts to encroach on individual autonomy involving the processing of private information.

It bears noting that not all privacy invasions are blatantly illegal. In modern digital societies, individuals are invited to surrender components of their private selves in an ongoing manner, to access services, use goods, and overall, to improve their quality of life. Nevertheless, to relinquish personal information should not be equated to a total abandonment of privacy. It is helpful to consider the current paradigm as a sort of constant bargaining state, where components of the private self are exchanged for things *via* digital platforms. While absolutist views of informational privacy are hardly tenable under the current paradigm[65], privacy still requires that guarantees pertaining to the

[61] *Bjørlo* (fn. 16).

[62] BVerfGE 65, 1, 68–69.

[63] US Supreme Court, *Whalen v. Roe*, 429 U.S. 589, decision of 22 February 1977. For an analysis of the US case law dealing with informational privacy, see *Carlek Shachar/Carleen Zubrzycki*, Informational privacy after Dobbs, in: Alabama Law Review 75 (2023), pp. 1-50.

[64] See, for instance, ECtHR, *Perry v. the UK* (63737/00), judgement of 17 July 2003, para. 47. See also generally *Joseph* (fn. 10); US Supreme Court, *United States v. Jones*, 565 U.S. 400, decision of 23 January 2012; Concurring opinion of judge Sotomayor in *United States v. Jones*, 565 U.S. 400, decision of 23 January 2012; and see *Brandon T. Crowther*, (Un)Reasonable Expectation of Digital Privacy, in: BYU Law Review 2012, pp. 343-370.

[65] Ibid., p. 237. See, for instance, *Florent Thouvenin*, Informational Self-Determination: A Convincing Rationale for Data Protection Law?, in: Journal

security and confidentiality of the information thus collected, and *in fine* the degree of autonomy kept by the right-holder, are assured.[66] In other words, the bargain should be based on trust and therefore, conditional.[67] Yet, as shown earlier, the privacy-adverse mechanisms involved in modern surveillance activities hardly, if ever, satisfy these criteria.[68]

When consent is not required, as is often the case with state surveillance, the validity of surveillance practices must be assessed from the perspective of individuals' expectations of privacy, which must be reasonable. That is to say, balanced with the objectives sought and the necessity of the practice under scrutiny. Consent-based data collection practices should themselves guarantee free and informed consent. However, the practice leading to corporate surveillance usually rely on suboptimal measures to ensure informed consent. Few individuals realize the amount of personal information collected by corporations, let alone what is inferred from these data, and which decisions are taken based on said inferences. Due to their opacity and irresistibility, corporate surveillance practices subvert the conditions of the bargain, thereby undermining the concept of consent.[69]

Besides, the commodification of attention and data that pervades surveillance activities inherently contradicts human dignity. As noted in the explanation paper to the Convention 108+, "[h]uman dignity requires safeguards to be put in place when processing personal data, in order for individuals not to be treated as mere objects."[70]

IV. AI-driven surveillance in emerging AI laws

Are the mechanisms involved in surveillance – namely, the extensive accumulation and analysis of data, and the subsequent inferences drawn therefrom – adequately addressed in emerging legal regimes on AI? Leaving aside non-binding instruments, this section covers supranational regulatory initiatives pertaining to AI, identifying gaps in their approach to privacy (1), before expanding the discussion to other relevant regimes (2).

1. AI-driven surveillance in emerging international AI regulations

a) The AI Act

While considering relevant regulatory trends tailored to AI, one inevitably stumbles upon the recent EU's AI Act. Inspired by product safety rules, the AI Act sets forth a comprehensive and horizontal framework for the regulation of AI systems in the Union. Much like the General Data Protection Regulation (GDPR)[71] before it, the AI Act could become a benchmark for AI regulation, the so-called "Brussel effect".

of Intellectual Property, Information Technology and E-Commerce Law 2021, pp. 246-256.

66 See notably *Solove* (fn. 6), p. 526.

67 *Bjørlo* (fn. 16).

68 *Bjørlo* (fn. 16).

69 *Lyon* (fn. 34), p. 9.

70 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows of 8 November 2001, ETS No. 181.

71 EU Regulation 2016/679 of 27 April 2017, OJ L 119 (GDPR).

The AI Act is based on the prescriptions set forth by the high-level expert group on artificial intelligence, which emphasized privacy as a core requirement to achieve "trustworthy AI", understood as an AI system that is "lawful," "ethical," and "robust."[72] The text lays down several obligations for providers and deployers of AI systems, which vary based on the degree of risk associated with the system and its use. Some prohibitions are targeted at AI systems deemed to pose "unacceptable risks." Importantly, the AI Act applies to both the public and the private sector, as long as the entity in question acts as provider or deployer of AI systems.

The AI Act does not deal specifically with data protection, since the GDPR already covers this important aspect of digital privacy. However, several privacy-adverse practices are addressed. Art. 5 AI Act notably prohibits particularly intrusive systems, which could be used for social control, and yield disproportionate harm to human rights, such as certain social-scoring practices and AI systems that create or expand "facial recognition databases through untargeted scraping of facial images."[73]

A first prohibition that seems relevant to corporate surveillance and its mechanisms relates to the use of AI systems for manipulative and exploitative purposes. The AI Act indeed prohibits some AI-enabled manipulative and exploitative practices involving the voluntary distortion of behaviours in ways that would cause significant harm to a person or a group of persons.[74] Recital 29 of the AI Act, which provides some interpretative guidance on the matter, clarifies that the prohibition applies to the commercial context as well, but also notes that "common and legitimate commercial practices, for example in the field of advertising, that comply with the applicable law should not, in themselves, be regarded as constituting harmful manipulative AI-enabled practices."[75]

Beyond the unclarities introduced by the use of the adjectives "common and legitimate", and although Recital 29 does not seem to evacuate completely the possibility that consumer manipulation practices akin to corporate surveillance fall into the scope of Art. 5 of the AI Act, the applicability of the relevant provisions is somewhat neutralised by a requirement of significant harm, or the likelihood thereof, which is hard to prove in the case of invasive advertising practices. How to measure the harm in the context of manipulative commercial practices remains unclear, although the Recital indicates that "unfair commercial practices leading to economic or financial harms to consumers are prohibited under all circumstances, irrespective of whether they are put in place through AI systems or otherwise."[76]

On this point, relevant provisions may also be found outside the AI Act, notably

[72] European Commission (fn. 29), p. 2.

[73] AI Act, Recital 43. See also European Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final of 4 February 2025, p. 77.

[74] "The placing on the market, the putting into service or the use of certain AI systems with the objective to or the effect of materially distorting human behaviour, whereby significant harms, in particular having sufficiently important adverse impacts on physical, psychological health or financial interests are likely to occur, are particularly dangerous and should therefore be prohibited.", AI Act, Recital 29, Art. 5 para. 1 lit. (a)(b).

[75] AI Act, Recital 29.

[76] Ibid.

in Directive 2005/29/EC (UCPD),[77] which, in its modernized form, notably protects European consumers against "coercion and undue influence", understood as the act of "exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision."[78] Therefore, depending on their characteristics, targeted advertising practices could sometimes amount to undue influence, although this should also be appreciated in light of consumers' own responsibilities.[79]

The 2021 Guidance submitted by the European Commission on the interpretation and application of the UCPD offers a more in-depth analysis of the mechanisms involved in corporate surveillance. Data-driven practices, dark patterns and commercial practices of social media are notably addressed.[80] Interestingly, the guidelines acknowledge that the superior knowledge extracted at the data aggregation phase, the constant fine-tuning of commercial practices on consumers to learn more about their behaviour, as well as the opacity of the practices, may help to distinguish "highly persuasive advertising or sales techniques from, on the other hand, commercial practices that may be manipulative and, hence, unfair under consumer law."[81] As the "significant harm" requirement of the AI Act is not replicated in the UCPD, it could be that its rules are easier to trigger than the AI Act's; although it is likely that the threshold for recognising undue influence in the commercial context remains high outside of clear instances of coercion, as over-inclusive criteria risk outlawing the majority of business practices.

Early 2025, in conjunction with the priority entry into force of the provisions on prohibited practices, the European commission published its Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act.[82] The document notably covers the question of the scope of the prohibition enshrined in Art. 5 para. 1, distinguishing between lawful persuasion, which "operates within the bounds of transparency and respect for individual autonomy", and manipulation, which involves "covert techniques undermining autonomy, leading individuals to make decisions they might not have otherwise made if they were fully aware of the influences at play."[83] The guidelines adds that "Both the AI Act and the UCPD aim to proactively prevent consumer harm from AI-driven business practices that are manipulative, misleading, or aggressive"[84] and clarifies that the AI Act's requirements are broader in scope than those of the UCPD in the sense that its provisions are not restricted to consumers and

[77] EU Directive 2005/29/EC of 11 May 2005, OJ L 149. (UCPD)

[78] Ibid., Art. 9. See also EU Directive 2019/2161 of 27 November 2019, OJ L 328, Art. 3, adding transparency requirements as regard the nature of commercial search result. See Art. 2 for definitions.

[79] See in that sense European Commission, Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, OJ C 526 of 29 December 2021, pp. 99 ff.

[80] Ibid.

[81] Ibid.

[82] European Commission, Communication from the Commission - Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 5052 final of 29 July 2025.

[83] Ibid., para. 128.

[84] Ibid., para. 136.

commercial harm.[85] But it transpires from the guidelines that the threshold set by the AI Act's requirements remains high. Ultimately, assessments will be made on a case-by-case basis, taking into account an array of parameters including transparency, conformity with data protection law, the vulnerability of the target, and the objective and impact of a technic, but the significant harm requirement makes it so that insidious techniques deployed by corporations to keep customers engaged with their product mostly fall outside the scope of the regulation, AI or not.

The AI Act is arguably more informative when it comes to state surveillance. Indeed, AI-driven social-scoring practices, which may be integrated in a state's surveillance apparatus[86] and lead to discriminatory and unjust decisions being taken to restrict the right of a person, are prohibited under the AI Act. The regulation is also concerned with surveillance practices involving biometric data in the form of biometric categorisation, real-time and post-remote biometric identification in publicly accessible spaces. The first two are in principle prohibited, while the third falls into the lower category of high-risk systems (Art. 26 para. 10 AI Act). This means that they are in principle authorised so long as some safeguards are in place. The AI Act also addresses profiling in the context of law enforcement. AI systems can be involved in profiling and decision-making processes, significantly contributing to the outcome, with potentially high impact on fundamental rights.[87] Art. 5 AI Act therefore prohibits, with exceptions, risks assessments and crime prediction when based solely on profiling.[88]

Finally, additional privacy-related requirements are contained in the regime for high-risk AI systems. Art. 10 AI Act indeed contains provisions on data governance, which may have some relevance to surveillance activities. Notably, Art. 10 para. 5 AI Act provides for the possibility to process special categories of data in order to mitigate biases in the outputs of an AI system. In this case, the AI Act demands that adequate privacy enhancing measures are deployed to complicate reidentification. Overall, bias reduction measures contribute to avoid unjust surveillance outcomes that may impact decisional privacy.

Be that as it may, the AI Act has been criticised for its permissive posture on real-time and post remote biometric identification, and overall lack of operational guidance. Particularly, the fact that the text still allows real-time remote biometric identification in "exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks"[89] has been described by human rights advocates as providing a "'blueprint' for how to conduct biometric mass surveillance practices" rather than strong privacy safeguards.[90]

---

[85] Ibid., para. 136.

[86] *Liang et al.* (fn. 22).

[87] *Wiedemann* (fn. 18).

[88] See also AI Act, Recital 42.

[89] AI Act, Recital 32.

[90] European Digital Rights, How to fight Biometric Mass Surveillance after the AI Act: A legal and practical guide, EDRi of 27 May 2024, available at: https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/ (last visited 7 November 2025). See also *Laura Lazaro Cabrera*, EU AI Act Brief – Pt. 2, Privacy & Surveillance, Center for Democracy and Technology (cdt) of 30 April 2024, available at:

Others have argued that the more lenient stance on post-remote biometric identification could be easily abused by authorities.[91] One might also regret the fact that AI uses in the context of national defence are excluded from the scope of the regulation, thereby leaving the door open to misclassification and *in fine* abuse.

b) The framework convention on AI

The Framework Convention, adopted in May 2024 by the Council of Europe and opened to signature in September 2024, is the second most influential development in the field of international AI regulation to date. The text, which constitutes the first binding convention on AI with international reach, is intended to apply to "the activities within the lifecycle of artificial intelligence systems that have the potential to interfere with human rights, democracy and the rule of law" (Art. 3 para. 1 Framework Convention). On this point, the text appears to have a broader scope than the AI Act.

The Framework Convention is the result of the work of the Committee on Artificial Intelligence (CAI), based on preliminary research carried out by the Ad hoc Committee on Artificial Intelligence. Its drafting involved the 46 Member States of the Council as well as 11 observer States, including Japan and the United States, and 68 representatives of civil society. Like the AI Act, the Convention aims to promote human rights friendly AI, by adopting a risk limitation approach (Art. 1 lit. b). However, the Convention does not create new rights but sets out a number of general principles such as human dignity and personal autonomy (Art. 7), transparency and control (Art. 8) and equality and non-discrimination (Art. 10), which draw directly from the guiding principles issued by the OECD.

As a *framework* Convention, the text seeks first and foremost to lay the foundations for more far-reaching international regulations in the future. Consequently, the Framework Convention is less technically detailed than the majority of national and European frameworks on the subject. The drafters chose not to name any specific activity involving AI that would fall within the scope of the text, leaving considerable room for manoeuvre for States to achieve its aims.

The Framework Convention on AI was also subject of criticism. Its broad formulation does not forecast strong effectiveness, which has led to it being heavily criticised, notably by the European Data Protection Committee (EDP).[92] Yet, the general wording of its provisions is a consequence of its openness, as the CAI seeks to bring together States with different legal traditions, particularly in terms of AI regulation, which requires significant concessions. A follow-up mechanism provided in the form of a "Conference of the Parties" grants the Convention some degree of adaptability. However, it appears unlikely that a framework specifically addressing AI-driven surveillance activities will later be developed under the Convention. The

https://cdt.org/insights/eu-ai-act-brief-pt-2-privacy-surveillance/ (last visited 7 November 2025).

[91] Ibid.

[92] EDPS statement in view of the 10th and last Plenary Meeting of the Committee on Artificial Intelligence (CAI) of the Council of Europe drafting the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law of 11 March 2024, available at https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-statement-view-10th-and-last-plenary-meeting-committee-artificial-intelligence-cai-council-europe-drafting-framework-convention-artificial_en (last visited 20 October 2024).

exception expounded in Art. 3 para. 2 and 4 Framework Convention makes it that AI systems used for surveillance activities could easily fall outside its scope if they are shown to relate "to the protection of national interests." The case of corporate surveillance is similarly uncertain under the Convention, as States are free to decide whether national private actors should be bound by the provisions of the Convention.

Hence, the Convention's initial contribution in limiting surveillance practices is very tenuous, even though many aspects of surveillance contradict the basic rationale laid down in the explanatory document to the Convention; "[A]ctivities within the lifecycle of artificial intelligence systems should not lead to the dehumanization of individuals, undermine their agency or reduce them to mere data points [...]."[93]

2. Guidance from non-AI specific regimes

AI systems rely on data to function. Their development and use therefore implicate data processing activities.[94] Therefore, a discussion on AI regulation mobilizes way more frameworks than technology-specific regimes. The AI Act also hints several times at the GDPR which provides data subjects with several rights that are directly relevant to this discussion.[95] The text notably recognises a right to object to data processing including profiling when for the purpose of direct marketing, (Art. 21 GDPR) a right not to be subject to fully automated decision-making producing legal effect (Art. 22 GDPR), as well as a right to information and transparency regarding the logic involved, the significance and the envisaged consequences of automated decision-making for the data subject, (Art. 13 to 15 GDPR). As per Art. 23 GDPR, these rights can be restricted, among other, for national security reasons. Additionally, principles such as purpose limitation and data minimization (Art. 5 para. 1 lit. (b)(c) GDPR) also impose checks on surveillance practices.

At this point, the GDPR has been extensively discussed in the literature. Authors have underlined its inadequacy when it comes to AI-enabled surveillance. Andrew and Baker for instance argue that the GDPR's complacency toward anonymisation and pseudonymisation "incentivize the use, collection, and trade of behavioural and other forms of de-identified data", thereby enabling surveillance practices. [96] In the same vein, Zarsky argues that the provisions contained in Art. 22 GDPR on fully automated decision-making could be easily sidestepped by a data controller.[97] He adds that Big Data capabilities challenge the distinction between the different categories of data contained in the GDPR, with the most sensitive data extrapolatable from regular information.[98] More generally, prominent commentators have argued that the "individual control" model, on which most data protection legislations are built, is doomed, because it fails to account for the power imbalance

[93] Council of Europe, Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225 of 5 September 2024, para. 53.

[94] See notably GDPR Recital 72.

[95] *Andrew/Baker* (fn. 14). And see AI Act, Art. 2 para. 7.

[96] *Andrew/Baker* (fn. 14).

[97] *Tal Zarsky*, Incompatible: The GDPR in the age of big data, in: Seton Hall Law Review 47 (2016), pp. 995-1020 (1016).

[98] Ibid., p. 1017.

between companies, states and individuals.[99] Joseph A. Cannataci, former UN Special Rapporteur on the right to privacy also deplored the EU's lack of competence in the field of national security, which impedes proper oversight of surveillance policies.[100] Finally, recent discussions in the realm of generative AI regulation have highlighted the GDPR's poor performance in capturing the particularities of generative AI systems.[101]

Much like the GDPR, the Convention 108+ modernizing the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data covers diverse aspects of AI-driven surveillance activities. Adopted in 2018, the modernization Protocol for the Convention 108 provides broad guidelines for the international protection of data worldwide which integrates provisions directly targeted at AI systems.[102] Unlike the first version, the amended Convention 108+ is fully applicable to the national security domain. It also applies to both the public and the private sector, which makes it a more impactful instrument than the Framework Convention when it comes to controlling corporate surveillance.

The Convention 108+ constitutes the only existing binding treaty on privacy and data protection in the digital context. The CoE's Committee of Minister has made multiple references to the Convention 108+, among others, at the occasion of a non-binding declaration on risks arising from surveillance technologies[103], and a recommendation dealing with automatic processing of personal data in the context of profiling.[104] When it comes to data processing in the context of national security, the Convention 108+ requires a test of proportionality and necessity. The Convention takes up several principles enshrined in the 2014 International Principles on the Application of Human Rights to Communications Surveillance,[105] a document drafted by privacy experts aiming

[99] *Daniel J. Solove/Woodrow Hartzog*, Kafka in the Age of AI and the Futility of Privacy as Control, in: Boston University Law Review 104 (2024), pp. 1021-1042 (1031).

[100] UNHRC, Report of the Special Rapporteur on the right to privacy of 16 October 2019, UN Doc A/HRC/40/63.

[101] *Juliette Sénéchal*, Publication de l'avis de l'EDPB du 17 décembre 2024 sur le traitement des données personnelles dans le contexte des modèles d'IA : prémices d'une mutation profonde du RGPD ?, Dalloz actualités of 17 January 2025, available at: https://www.dalloz-actualite.fr/flash/publication-de-l-avis-de-l-edpb-du-17-decembre-2024-sur-traitement-des-donnees-personnelles-da (last visited 7 November 2025).

[102] Committee of Ministers of the Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, CM/Inf (2018)15-final of 18 May 2018.

[103] Committee of Ministers of the Council of Europe, Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, Decl(11/06/2013) of 11 June 2013.

[104] Committee of Ministers of the Council of Europe of the Council of Europe, The protection of individuals with regard to automatic processing of personal data in the context of profiling Recommendation, CM/Rec(2010)13 of 23 November 2010. See also Committee of Ministers of the Council of Europe, Recommendation Rec(2002)9 on the protection of personal data collected and processed for insurance purposes, Rec(2002)9 of 18 September 2002; Committee of Ministers of the Council of Europe of the Council of Europe, Recommendation Rec(97)18 concerning the protection of personal data collected and processed for statistical purposes, Rec(97)18 of 30 September 1997.

[105] *Juan Carlos Lara/Valentina Hernández/Katitza Rodríguez*, International Principles on the Application of Human Rights to Communications Surveillance and the Inter-American System for the Protection of Human Rights of August 2026, available at: https://necessaryandproportionate.org/files/iachr-en-august2016.pdf (last visited 17 November 2025).

to provide state actors with precise guidelines regarding the conduct of surveillance activities.

So far, the Protocol modernizing Convention 108+ has been ratified by 33 States, the majority being European. The updated Convention will only enter into force once this number reaches 38. It is worth noting that the United States, which hosts the most powerful digital firms, was not a party to the original Convention 108+. Given the current priorities at the White House, it is unlikely that Convention 108+ will be ratified by the US government.

V. Conclusive remarks on advancing AI privacy discussions

Privacy should play a central role in the regulation of AI tools. Current legal development on the matter however show that this is not really the case and that non-AI-specific frameworks have weaknesses. It is therefore interesting to investigate whether human rights law, which by default applies to AI technology and its uses, is up to the task of filling the gaps left by more specific frameworks when it comes to mitigating AI-enabled privacy risks. After all, both the Framework convention and the Convention 108+ limit their exceptions on national security to the respect of international human rights law. Unfortunately, due to several theoretical and structural deficiencies, international human rights law might not provide sufficiently robust baseline protection to individuals whose privacy is infringed upon by AI-driven surveillance practices.

On an abstract level, the inherent fluidity of the concept of privacy makes it difficult to operationalize in practice. The absence of a clear definition for privacy and its subjective dimensions necessitate an ongoing evaluation of the numerous expectations stemming from it. Admittedly, privacy must be considered in context, and approached as a mutable concept. It must be able to satisfactorily respond to new challenges and mitigate harms to human dignity and autonomy while simultaneously allowing society to function. But privacy cannot be toned down on the basis that individuals are giving up so many of it nowadays. Human autonomy and dignity are invariable, and as such, should always guide assessments of privacy expectations.

At present, it is difficult for individuals to understand when their data is used for AI-training purposes, especially since the issue is relatively new, large databases already exist and so is a sense of resignation over the propriety of personal data.[106] While the constant bargaining taking place online is a source of privacy risks that the principle cannot eliminate entirely, societies cannot afford to allow countervailing considerations to prevail over privacy in the constant checks and balances imposed by ubiquitous computing environment.[107] This means, first and foremost, that data collection must be rationalized, in the sense of empowering the data subject to make free decisions regarding the amount of personal information that is relinquished in exchange for a ser-

[106] *Nora A. Draper/Joseph Turow*, The corporate cultivation of digital resignation, in: New Media & Society 21 (2019), pp. 1824-1839 (1831).

[107] *Stefan G. Weber/Andreas Heinemann/Max Mühlhäuser*, Towards an Architecture for Balancing Privacy and Traceability in Ubiquitous Computing Environments, paper presented at Third International Conference on Availability, Reliability and Security, 4-7 March 2008, pp. 958-964.

vice or goods. In situations where consent can be circumvented, it is imperative to ensure transparency with regard to the collection, use and the anticipated outcomes of such data processing operations.

Still, a blatant issue with privacy as enshrined in the various existing international documents is that it is centred around the individual and thus, struggles to accommodate collective needs related to data processing. If anything, surveillance activities are societal-scale undertakings. Profiling virtually concerns billions of users. At the individual level, the right to privacy may offer some degree of protection against data misuses, but it cannot address the full picture. Indeed, due to the situation of quasi-monopoly of a few companies, users do not really possess a negotiating power regarding the trade of data for services. This power imbalance, which favours the acceptance of companies' terms and conditions, counteracts any claim of arbitrariness and, ultimately, limits the relevance of the right to privacy as a safeguard since data subjects more often than not enter into data transaction without a proper understanding of the implications.[108] Even when basic privacy requirements are satisfied, the content of the right to privacy becomes gradually shallower as more data is required to access common services, and more data-sensitives activities are integrated in everyday life interactions.

The very individualistic and consent-oriented understanding of privacy as enshrined in international instruments is therefore lacklustre. Further advance in the protection of users' data against corporate surveillance will not come from the current approach, but from rebalancing the bargain between users and providers. As expressed by some authors; "A privacy and data protection framework that places the primary responsibility on individuals to manage their data across hundreds, even thousands, of digital relationships and channels fundamentally does not scale, and thus will not succeed in protecting individual privacy."[109] The concern was recently echoed by Solove and Hartzog, who called for the application of a "societal structure" model of privacy regulation also embracing AI.[110]

Another noticeable impediment to the performance of a human rights framework in the present case relates to the fact that human rights law is principally state-centric. While states are directly bound by the human rights treaties to which they commit, in addition to certain customary human rights which are binding upon all states, private entities are not directly bound by international human rights law. This is why State participation in instruments such as the International Covenant on Civil and Political rights is crucial. Although modern developments in the realm of human rights law have recognized the human rights responsibilities of private actors,[111] these actors are only liable for human rights harm under national law. It is thus the primary responsibility of states to ensure that the right to privacy is respected within their borders.

[108] *Solove/Hartzog* (fn. 99).

[109] *Jennifer King/Caroline Meinhardt*, Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World, White Paper of 22 February 2024, available at: https://hai.stanford.edu/policy/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world (last visited 20 October 2025), p. 30.

[110] *Solove/Hartzog* (fn. 99).

[111] United Nations Human Rights Office of the High Commissioner, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, HR/PUB/11/4 (Ruggie Principles) of 2011.

In addition, business firms usually enjoy greater freedom when it comes to data practices under the right to the freedom to conduct business, which may be used as a defence against certain claims. As a result, attempts to circumscribe the data practices of the private sector have been paradoxically weaker than for state surveillance.

Although regulators can influence the fairness of the bargain, their action is limited for several reasons. First, it might be difficult for regulators, to assess what is necessary when providers offer a wide range of services requiring various data to function properly, such as location and browsing data. Second, regulators might feel pressure to avoid undermining innovation and development in the digital sector, especially when national firms are concerned. Third, the promise of better population control through the use of AI technology is inherently attractive for authorities, and effectively curtails the right to privacy.

Nevertheless, the balance of interests between individuals, corporations and states must be readjusted, and new approaches to privacy might be the key. This difficult endeavour can only stem from national or regional initiatives, since value decisions are beyond the scope of international human rights law. To this end, the current momentum around AI regulation should be exploited fully. The longstanding paradigm revolving around the commodification of personal information for the purpose of influencing behaviours, especially when the objectives sought are of economic nature, needs to be challenged.

Vitae

Dr. William Letrone is a CNRS postdoctoral researcher in cybersecurity and data protection law at Nantes University, France and a member of the IPoP project.

Dr. Tony Cabus is a postdoctoral researcher at the Walther-Schücking Institute for International Law in Kiel, Germany.