

European Standards for the Protection of Privacy in the Context of Mass Biometric Surveillance

Professor **Svitlana KARVATSKA**¹

Resident lawyer **Florian GHEORGHE**²

Associate professor **Ivan TORONCHUK**³

Assistant professor, PhD student **Anastasia LABYK**⁴

Associate professor **Tetyana HREKUL-KOVALYK**⁵

Abstract

This article examines biometric surveillance as a highly intrusive tool of contemporary digital governance, weighing its security benefits against significant threats to privacy, informational autonomy, and individual liberty. Biometric data's distinctiveness, permanence, and irreversibility justify elevated legal safeguards and strict limits on collection, retention, and processing, especially regarding automated facial recognition. Comparative review of international instruments and European Court of Human Rights jurisprudence suggests biometric measures may be compatible with human rights only when anchored in precise law, legitimate aims, necessity, and proportionality, supported by procedural guarantees and independent oversight. Recent EU regulatory trends, including the GDPR and AI Act, embody a rights-centred governance model that Ukraine should adapt. The article advocates tailored statutory definitions of permissible purposes, a general ban on indiscriminate mass monitoring with narrow exceptions, mandatory human-rights impact assessments, empowered supervisory bodies, transparency and retention rules, technical safeguards, and effective remedies. Coordinated legislative, institutional, and technological reforms are essential for lawful biometric governance.

Keywords: human rights, biometric governance, biometric surveillance, protection of privacy, European Court of Human Rights.

JEL Classification: K33

DOI: 10.62768/TBJ/2026/16/3/04

¹ Svitlana Karvatska – Acting Head of the Department of International Law and Comparative Law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Ukraine. ORCID iD: <https://orcid.org/0000-0001-9948-4866>. E-mail: s.karvatska@chnu.edu.ua. **Corresponding author.**

² Florian Gheorghe – Resident lawyer at the Faculty of Law and Administrative Sciences, ‘Ștefan cel Mare’ University of Suceava, Romania; ORCID iD: <https://orcid.org/0009-0007-4043-390X>. E-mail: fg@fglegal.ro.

³ Ivan Toronchuk – Department of International Law and Comparative Law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Ukraine. ORCID iD: <https://orcid.org/0000-0003-3887-4750>. E-mail: i.toronchuk@chnu.edu.ua.

⁴ Anastasia Labyk – Department of International Law and Comparative Law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Ukraine. ORCID iD: <https://orcid.org/0009-0005-1376-6771>. E-mail: a.labyk@chnu.edu.ua.

⁵ Tetyana Hrekul-Kovalyk - Department of Legal Theory and Human Rights, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Ukraine. ORCID iD: <https://orcid.org/0000-0003-4339-3927>. E-mail: t.hrekul-kovalik@chnu.edu.ua.

<p>Please cite this article as: Karvatska, Svitlana, Florian Gheorghe, Ivan Toronchuk, Anastasia Labyk & Tetyana Hrekul-Kovalyk, ‘European Standards for the Protection of Privacy in the Context of Mass Biometric Surveillance’, <i>Juridical Tribune – Review of Comparative and International Law</i> 16, no. 3 (October 2026): 432-451.</p>	<p>Article History Received: 7 June 2026 Revised: 28 August 2026 Accepted: 20 September 2026</p>
---	---

1. Introduction

The widespread deployment of biometric surveillance technologies challenges established privacy protections and generates novel legal and ethical dilemmas across the European legal order. This article provides a structured analysis of current European standards governing the collection, processing, and retention of biometric data within mass video surveillance and automated identification systems. Drawing on a comparative review of statutory instruments, case law, and supervisory guidance, the paper distinguishes circumstances in which biometric techniques may be justified from those that pose unacceptable risks to fundamental rights. It pays particular attention to proportionality, purpose limitation, and data minimisation as guiding principles, and examines procedural and substantive safeguards such as data protection impact assessments, lawful bases for processing, and transparency and accountability obligations for data controllers. Complementing legal safeguards, the study assesses technical and organisational measures — including pseudonymisation, access restriction, and algorithmic auditability — and addresses the practical challenges of implementing these measures amidst rapid advances in artificial intelligence.

In addition, the article considers the broader constitutional and societal implications of biometric surveillance in public spaces. The analysis shows that the normalisation of constant identification practices may gradually alter the relationship between individuals and public authority, creating a chilling effect that touches freedom of movement, expression, and association. For this reason, the paper argues that privacy protection in this field cannot be reduced to formal compliance with data protection rules alone, but must be understood as a substantive condition for democratic governance and human dignity. The article’s contribution lies in integrating doctrinal legal analysis with operational realities of mass surveillance systems and in proposing concrete criteria for assessing the legality and ethical permissibility of biometric deployments in public spaces. The conclusion sets out targeted recommendations for legislators and supervisory authorities, encompassing clear admissibility thresholds, mandatory impact assessment procedures, mechanisms for independent oversight, and minimum technical guarantees designed to mitigate privacy harms while allowing responsible technological innovation. The findings of this study are intended to support legal scholars, data protection practitioners, and policymakers in balancing public-security objectives with the effective safeguarding of individual rights as digital technologies continue to evolve.

2. Argument and Methodology

The methodological foundation of this study comprises an integrated set of general scientific and specialised legal methods, whose combined application enabled a comprehensive examination of biometric surveillance as a complex legal phenomenon at the intersection of privacy, security, and digital technologies. The dialectical method facilitated analysis of the problem in its development and in the friction between state interests and the obligation to guarantee fundamental human rights. Through analysis, synthesis, and generalisation, the research identified the essential characteristics of biometric surveillance, delineated its principal risks to the right to privacy, and articulated conceptual premises concerning the lawfulness of deploying biometric technologies in contemporary conditions.

The specialised legal component of the methodology included formal-legal, comparative, and systemic-structural approaches. The formal-legal method was employed to examine the substance of international legal instruments, provisions of European Union legislation—most notably the GDPR and the AI Act — together with relevant provisions of Ukrainian domestic law governing biometric-data processing. This comparative-legal method made it possible to juxtapose approaches adopted by different legal systems for governing biometric surveillance, to detect converging trends and divergences in mechanisms for legal protection of individuals, while the systemic-structural method established the place of biometric monitoring within the broader system of state control measures and legal guarantees.

Considerable attention was devoted to the jurisprudence of the European Court of Human Rights, which made it possible to assess when interference with the right to respect for private life could be regarded as permissible. Analysis of judicial decisions substantiated the conclusion that use of biometric technologies can be regarded as lawful only where grounded in a clear legal basis, pursuing a legitimate aim, and satisfying requirements of necessity and proportionality, together with effective oversight of data processing. This methodological approach secured the scientific rigor of the findings and informed proposals for refining legal regulation of biometric surveillance in line with rule-of-law and human rights standards.

3. Biometric Data and Biometric Surveillance: Analysis of Core Concepts

3.1. Biometric Data as an Object of Legal Protection

The interpretation of biometric surveillance is directly connected to the notion of biometric data, the study of which has become even more significant in light of the large-scale use of artificial intelligence in everyday life, business, and public administration. Unlike surveillance as such, the term “biometric data” has become embedded both in the legislation of certain states and in international instruments. Notably, a central position among the international acts regulating this field is occupied by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 (hereinafter Convention 108).

Convention 108 itself contains no definition of biometric data — its drafters did not use the term at all. It appeared for the first time only in the 2018 Protocol amending the Convention and was further explained in the Protocol's Explanatory Report. There, biometric data were included among sensitive personal information and defined as physical, biological or physiological characteristics enabling the unambiguous identification or verification of a person.⁶

One of the first international instruments to give this concept legal expression was the EU General Data Protection Regulation (GDPR). Pursuant to Article 4(14) GDPR, biometric data means personal data generated through specific technical processing of a person's physical, physiological, or behavioural traits, provided that such processing allows or confirms that person's unique identification.⁷ It should be noted that one of the GDPR's achievements was the inclusion of the behavioural dimension within the concept of biometric data, rather than limiting it to defined physiological traits, which significantly expanded its scope and the potential for ensuring the right to personal data protection.

Within Ukrainian legislation of the highest legal force, the term "biometric data" has so far been enshrined only in the Law of Ukraine "On the Unified State Demographic Register and Documents Confirming Citizenship of Ukraine, Identifying a Person or His or Her Special Status." That statute characterises biometric data as a set of information about a person distinguished by stability (immutability) and uniqueness relative to the corresponding parameters of other individuals.⁸ The "Rules for Issuing Visas for Entry into Ukraine and Transit through Its Territory," which are subordinate regulatory instruments by nature, elaborate this category by listing types of biometric data, such as a digitised facial image or fingerprint records.⁹

Compared with the above-mentioned Law of Ukraine, this definition considerably narrows the content of the concept of biometric data, which is generally justified in view of the Rules' narrow specialisation and purpose. Nevertheless, in matters of confidentiality and privacy protection, the Ukrainian legislator interprets this term broadly, where an analogy with European acts in the relevant sphere may be observed, as an interconnected system of unique physiological, physical, and behavioural characteristics.

It is worth noting that this approach reflects global trends in understanding the legal nature of biometric data. Scholarly research shows that the definitions adopted in different legal systems, regardless of wording, point to the same essential characteristics

⁶ Council of Europe, *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, CETS No. 223, October 10, 2018, paras. 58–59, <https://rm.coe.int/16808ac91a>.

⁷ Regulation (EU) 2016/679 (General Data Protection Regulation), art. 4(14), *Official Journal of the European Union* L 119 (May 4, 2016): 1–88, <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.

⁸ Ukraine, Law No. 5492-VI of November 20, 2012, "On the Unified State Demographic Register and Documents Confirming Citizenship of Ukraine, Identifying a Person or His or Her Special Status," art. 3(1)(2), <https://zakon.rada.gov.ua/laws/show/5492-17#Text>.

⁹ Cabinet of Ministers of Ukraine, *Rules for Issuing Visas for Entry into Ukraine and Transit through Its Territory*, Resolution No. 118 of March 1, 2017, para. 2, first definition, <https://zakon.rada.gov.ua/laws/show/118-2017-%D0%BF#Text>.

of biometric data. These are usually identified as follows: (a) immutability, permanence, or stability over a sufficiently long period of time, and generally throughout a person's life; (b) uniqueness, meaning a feature that makes it possible to distinguish one individual from another without error through comparison of a specific parameter; (c) universality, that is, biometric data are traits inherent in every member of the human species, subject to rare exceptions such as *adermatoglyphia*, a hereditary condition in which a person is born without fingerprint patterns; (d) measurability, namely the technical possibility of capturing and recording the relevant characteristics; and (e) ethical and moral acceptability of collecting and processing such data.¹⁰

Biometric data may be broadly classified into two principal categories: behavioural and biological. The former encompasses data that can be captured exclusively through an individual's actions, interactions, or patterns of conduct, whereas the latter relates to relatively stable physiological attributes that constitute the person's physical identity and bodily characteristics.¹¹ In this regard, biological (physiological) biometric identifiers may encompass a range of data, including digitised fingerprints, iris patterns, facial scans, DNA profiles, and vascular biometrics based on the unique configuration of an individual's blood vessels. By contrast, behavioural biometric characteristics are functional in nature and are derived from patterns of human activity and conduct. Such identifiers may include voice characteristics, handwriting, keystroke dynamics, gait, and signatures, including their digital representations.¹² In light of the expanding deployment of advanced technologies, scholars have increasingly developed the concept of "cognitive biometrics" or "neural biometric data." The disclosure of the information underlying this concept does not necessarily cause substantial harm to the data subject. Isolated indicators, such as heart rate patterns or eye movements, generally possess limited significance for individuals lacking specialised medical expertise. However, the automated processing and cross-analysis of such data in conjunction with other personal parameters may enable the inference of highly sensitive personal characteristics. Revealing such inferred attributes may amount to an unjustified intrusion into the individual's privacy.¹³

3.2. Biometric Surveillance versus Traditional Surveillance

Biometric surveillance, for its part, may be defined as automated collection, processing, and analysis of an individual's physiological and behavioural characteristics for the purposes of unique identification, categorisation, or continuous tracking. Such

¹⁰ Andrii O. Hachkevych, "The Concept of Biometric Data in the Legislation of Ukraine and Other Countries," *Visnyk of Mariupol State University. Series: Law* 15, no. 30 (2025): 20, <https://doi.org/10.34079/2518-1319-2025-15-30-16-26>.

¹¹ Pietro Melzi et al., "An Overview of Privacy-Enhancing Technologies in Biometric Recognition," *ACM Computing Surveys* 56, no. 12 (2024): 2, article 310, <https://doi.org/10.1145/3664596>.

¹² Volodymyr Kopanchuk et al., "Biometric Identification Systems as a Tool of Public Administration to Ensure Internal Security," *Uspikhy i Dosiahnennia u Nauksi*, no. 9 (19) (2025): 532, [https://doi.org/10.52058/3041-1254-2025-9\(19\)-527-539](https://doi.org/10.52058/3041-1254-2025-9(19)-527-539).

¹³ Patrick Magee et al., "Beyond Neural Data: Cognitive Biometrics and Mental Privacy," *Neuron* 112, no. 18 (2024): 3018, <https://doi.org/10.1016/j.neuron.2024.09.004>.

surveillance relies on technological systems capable of extracting, comparing, and evaluating biometric identifiers to establish or verify identity, track movement, or classify individuals according to predefined criteria.¹⁴ In general, biometric surveillance cannot be reduced to a single practice or a limited set of operations. Depending on the specific biometric parameters analysed and the objectives pursued, it can range from legitimate and socially useful applications to practices that raise serious legal and ethical concerns. At the same time, more controversial uses may involve the integration of biometric technologies into autonomous weapon systems for the identification of enemy combatants, the monitoring of citizens' activities and movements, the tracking of participation in public demonstrations, protests, or political activities, as well as the surveillance of national, ethnic, or other minority groups. Such practices underscore the dual-use nature of biometric surveillance technologies and point to the need for strong legal safeguards to prevent abuse and protect fundamental rights and freedoms.¹⁵

When examining biometric surveillance through the lens of its distinctions from traditional forms of physical monitoring or conventional video surveillance, several key characteristics emerge that are of particular significance for building a suitable regulatory framework. Foremost among these is the unique nature of the data that constitute the object of biometric surveillance. Given the highly sensitive and inherently personal character of biometric information, its unlawful collection, processing, or disclosure may result in severe and, in many cases, irreversible harm to the individual concerned. Unlike traditional surveillance methods, which primarily rely on the observation and comparison of visible features, appearance, or behavioural patterns that may be intentionally altered or concealed, biometric surveillance focuses on the analysis of distinctive characteristics that are unique to a particular individual and remain largely stable throughout their lifetime. These characteristics include, inter alia, fingerprints, facial geometry, iris patterns, and other physiological identifiers. Consequently, while a person may modify aspects of their appearance or behaviour to avoid recognition, biometric traits generally cannot be changed without significant difficulty, rendering their misuse particularly intrusive and increasing the potential risks to privacy, personal autonomy, and informational self-determination.¹⁶

Another defining characteristic of biometric surveillance is its large-scale and highly automated nature. Whereas a human operator can monitor only a limited number of surveillance feeds simultaneously, facial recognition systems enhanced by artificial intelligence can analyse and compare thousands of images within seconds.

In particular, one-to-many and many-to-many identification methods represent some of the gravest threats to fundamental rights and freedoms. Given the emergence of mass surveillance and real-time processing of collected information, such systems

¹⁴ Patricia Haley, "The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent," *Sensors* 25, no. 10 (2025): 6, article 3160, <https://doi.org/10.3390/s25103160>.

¹⁵ Kelley M. Saylor, *Biometric Technologies and Global Security*, In Focus IF11783 (Congressional Research Service, updated April 16, 2026), <https://www.congress.gov/crs-product/IF11783>.

¹⁶ Youna Jung and Ethan D. Virgil, "Analysis of Legislative Framework Governing Biometric Data," *Procedia Computer Science* 241 (2024): 49, <https://doi.org/10.1016/j.procs.2024.08.009>.

enable the identification, tracking, and profiling of individuals on an unprecedented scale. This creates a significant risk that personal data is collected and retained in circumstances where location, timing, or context of data acquisition may expose highly sensitive information about a person. Consequently, biometric surveillance can enable discriminatory practices, unwarranted profiling, and a disproportionate encroachment on the right to respect for private life. This potential for continuous monitoring and automated decision-making further amplifies these concerns, underscoring the need for stringent legal safeguards, transparency requirements, and effective oversight mechanisms.¹⁷

Closely linked to the foregoing characteristics is the covert nature of the identification process inherent in biometric surveillance. Although processing biometric data typically calls for the data subject's informed consent, or another valid legal basis, individuals may often remain unaware that their biometric information has been collected, analysed, or stored. Unlike many conventional forms of data collection, biometric identification can occur remotely and without any active participation on the part of the individual concerned. This concern is particularly pronounced where law enforcement agencies deploy large-scale surveillance in public spaces. In such circumstances, biometric technologies may be deployed to scan and analyse the characteristics of an indeterminate number of individuals moving through monitored areas. As a result, persons who are neither suspected of wrongdoing nor otherwise connected to any investigation may nevertheless become subjects of biometric processing without their knowledge or reasonable expectation. The invisible nature of such surveillance gives rise to serious concerns about transparency, accountability, informed consent, and privacy safeguards, particularly where biometric data is gathered and analysed on an ongoing or indiscriminate basis.¹⁸

Another important feature of biometric surveillance is its capacity to facilitate automated profiling and categorisation of individuals. The concept of biometric categorisation is expressly addressed in the European Union Artificial Intelligence Act, which defines this process as the assignment of a natural person to a particular category — such as age, sex, or other characteristics — based on the processing of that person's biometric data.

More broadly, the Regulation recognises the considerable dangers posed by the use of biometric systems for classification purposes and therefore imposes strict limitations on their deployment. In particular, it prohibits certain biometric categorisation systems that seek to classify individuals according to sensitive characteristics, including political opinions, religious or philosophical convictions, racial or ethnic background, sexual orientation, and other protected attributes. Such restrictions reflect growing concerns that automated categorisation technologies may reinforce discriminatory practices, facilitate social sorting, and result in unjustified

¹⁷ Giulia Gabrielli, “The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights,” *European Journal of Risk Regulation* 16, no. 2 (2025): 517–18, <https://doi.org/10.1017/err.2025.26>.

¹⁸ Orit Kopel, “In the Face of Ethics: Police Use of Live Facial Recognition Technology” (PhD diss., King’s College London, 2024), 16, <https://kclpure.kcl.ac.uk/portal/en/studentTheses/in-the-face-of-ethics/>.

intrusions into fundamental rights, including the rights to privacy, equal treatment, and freedom from discrimination. The ability of biometric systems to infer sensitive personal information from physical or behavioural characteristics further underscores the need for rigorous legal safeguards and effective regulatory oversight.¹⁹ It is evident that the algorithmic processing, selection, and evaluation of biometric information may give rise to discriminatory outcomes based on the aforementioned protected characteristics, particularly given that artificial intelligence systems are themselves susceptible to various forms of bias. Such bias may stem not only from the deliberate incorporation of datasets containing pre-existing prejudices or discriminatory assumptions, but also from structural deficiencies embedded within the data and decision-making processes on which these systems are trained. Moreover, discriminatory effects may emerge unintentionally as a consequence of systemic inequalities and historical patterns of exclusion that are reproduced and amplified through machine-learning techniques. As a result, artificial intelligence systems may perpetuate or even exacerbate existing social biases, generating inaccurate classifications, disproportionate targeting of certain groups, and unequal treatment of individuals. Within the context of biometric surveillance, these risks are particularly acute, as algorithmic errors or biased inferences may directly affect fundamental rights, among them privacy, equality, non-discrimination, and effective legal protection. Consequently, the deployment of biometric technologies requires robust safeguards to ensure fairness, transparency, accountability, and ongoing scrutiny of automated decision-making processes.²⁰

The following two characteristics are closely interconnected and may be regarded as complementary elements of the same phenomenon: the de-anonymisation of the data subject through biometric surveillance and the creation of a digital footprint. When compared with traditional forms of video monitoring or physical surveillance, the information obtained through such methods is generally fragmented in nature. Typically, an operator receives isolated images or video recordings depicting an individual whose identity must subsequently be established through additional investigative efforts. By contrast, biometric surveillance technologies enable the rapid processing of vast quantities of data and their immediate comparison with information stored in relevant databases. Through automated matching procedures, these systems can identify individuals within seconds, significantly reducing the role of human intervention in the identification process.

At the same time, retaining and combining biometric data builds up an individual's digital footprint, understood as the cumulative body of digitised information associated with a particular person. Importantly, contemporary artificial intelligence systems are capable not only of collecting such information but also of autonomously organising, correlating, and analysing data originating from multiple sources. This enables the construction of comprehensive digital profiles that reflect an

¹⁹ Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts. 3(40) and 5(1)(g), *Official Journal of the European Union* L, 2024/1689 (July 12, 2024), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.

²⁰ Xiaomeng Wang et al., "A Brief Review on Algorithmic Fairness," *Management System Engineering* 1 (2022): 1, article 7, <https://doi.org/10.1007/s44176-022-00006-z>.

individual's identity, behaviour, movements, preferences, and social interactions. As a result, biometric surveillance technologies facilitate the creation of a coherent and persistent digital representation of a person, allowing for their reliable recognition and tracking across different contexts and over extended periods of time. Such capabilities raise profound concerns regarding privacy, the individual's control over their own information, and the preservation of anonymity within public and digital spaces.²¹

4. Biometric Surveillance as an Interference with the Right to Respect for Private Life

4.1. Privacy Rights and the Protection of Biometric Data in the Digital Era

The rapid advancement of biotechnological innovations has significantly enhanced the ability of modern societies to investigate criminal offences and identify individuals suspected of unlawful conduct. The use of DNA profiling, fingerprint analysis, and other biometric identification techniques has improved the efficiency and reliability of investigative procedures, reducing the likelihood of factual errors and contributing to the prevention of wrongful convictions or the avoidance of legal accountability. Nevertheless, these same advances have also created fresh challenges for private life, challenges that have become particularly acute with the emergence and large-scale deployment of artificial intelligence systems, automated surveillance technologies, and sophisticated mechanisms for the collection and processing of personal information.

Together with the right to life, freedom of expression, and the prohibitions against slavery, torture, and inhuman or degrading treatment, privacy and the protection of personal data are now counted among the essential guarantees of the contemporary human rights framework. Their prominence owes much to the close connection between these rights and individual autonomy, human dignity, personal integrity, and freedom of thought — a connection that places them at the centre of protecting individuals from unwarranted interference. Respect for private life, understood in this light, is what allows personality to develop freely and choice to be exercised meaningfully: it is the right through which a person keeps command of their own personal sphere and pursues their potential free from undue external intrusion.²²

The Universal Declaration of Human Rights (1948) was the first instrument of universal scope to formally acknowledge the right to privacy: its Article 12 protects individuals from arbitrary intrusion into their private and family life, home, and correspondence, together with unlawful affronts to honour and reputation. That provision went on to anchor the subsequent development of international standards for

²¹ Peter Fussey and Daragh Murray, "Policing Uses of Live Facial Recognition in the United Kingdom," in *Regulating Biometrics: Global Approaches and Urgent Questions*, ed. Amba Kak (AI Now Institute, 2020), 79, <https://ainowinstitute.org/wp-content/uploads/2023/09/regulatingbiometrics-fussey-murray.pdf>.

²² Novera Bhatti, "Digital Privacy as a Human Rights in the Era of Mass Surveillance," *DME Journal of Law* 5, no. 2 (2024): 122, <https://dmejournals.com/index.php/DMEJL/article/view/598>.

privacy and personal-data protection.²³ The International Covenant on Civil and Political Rights subsequently extended this protection, giving further expression to the right in Article 17, which similarly guards against unlawful or arbitrary interference with one's privacy, family, home, and correspondence, and regards the protection of honour and reputation as inseparable from the broader guarantee of privacy and personal integrity.²⁴ That founding declaration also fed directly into a series of regional instruments. Article 8 of the 1950 European Convention on Human Rights sets out a broadly comparable guarantee — that everyone is entitled to respect for their private and family life, home, and correspondence — while the Inter-American system addresses the same concerns through two separate provisions: Article 5 of the American Declaration of the Rights and Duties of Man, which covers honour, reputation, and private and family life, and Article 9, which safeguards the inviolability of the home.²⁵ African and Asian regional human rights instruments, by contrast, generally stop short of recognising privacy as a distinct and comprehensive right, though this is not to say the underlying concerns — confidentiality, personal data, private life — go unaddressed; rather, they tend to be dealt with through discrete international agreements, sector-specific frameworks, or domestic legislation. Protection in these jurisdictions accordingly depends more heavily on national legal approaches and on the discretion national authorities exercise in weighing privacy against competing public interests.²⁶

The limitations of conventional regulatory approaches have been exposed by the growing reliance of public institutions on automated decision-making, predictive analytics, and technology-assisted justice. Longstanding legal safeguards were simply not built for a governance environment in which digital technologies are now deeply embedded, and they often struggle accordingly to guard against the risks of extensive data processing, automated decision-making, and pervasive surveillance. What this points to is the need for more sophisticated legal and institutional frameworks — ones capable of preserving privacy and other fundamental rights amid rapid technological change and extensive digitalisation.²⁷

These challenges have not gone unanswered. The United Nations has, since

²³ United Nations General Assembly, *Universal Declaration of Human Rights*, Resolution 217 A (III), December 10, 1948, art. 12, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

²⁴ *International Covenant on Civil and Political Rights*, adopted December 16, 1966, by United Nations General Assembly Resolution 2200 A (XXI), annex, art. 17, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

²⁵ Organization of American States, *American Declaration of the Rights and Duties of Man*, Ninth International Conference of American States, Bogotá, 1948, arts. V and IX, https://www.oas.org/dil/access_to_information_human_right_American_Declaration_of_the_Rights_and_Duties_of_Man.pdf; see also *Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS No. 5, November 4, 1950, art. 8, https://www.echr.coe.int/documents/d/echr/convention_ENG.

²⁶ Vibhushinie Bentotahewa et al., “The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries,” *SN Computer Science* 3, no. 3 (2022): article 183, <https://doi.org/10.1007/s42979-022-01079-z>; Avani Singh and Michael Power, “The Privacy Awakening: The Urgent Need to Harmonise the Right to Privacy in Africa,” *African Human Rights Yearbook* 3 (2019): 207, <https://doi.org/10.29053/2523-1367/2019/v3a10>.

²⁷ Bhatti, “Digital Privacy,” 128.

2013, adopted a succession of resolutions confronting the implications of digital technologies for privacy, and the starting point for that effort — General Assembly Resolution 68/167 of 18 December 2013 — set out what has since become a foundational premise of digital rights discourse: that human rights offline and online are, and must remain, one and the same.

Member States were, on this basis, urged to take a fresh look at domestic legislation, policy, and administrative practice governing how personal data is collected, processed, retained, and used, with a view to rooting out existing privacy violations tied to information and communication technologies and reinforcing safeguards against future ones. In doing so, the Resolution acknowledged the growing reach of digital technologies into the exercise of fundamental rights and underscored states' responsibility to keep technological development compatible with international human rights standards.²⁸ A year later, Resolution 69/166 of 18 December 2014 built further on this framework: alongside reaffirming transparency, legality, and accountability as guiding principles for how personal data is gathered and handled, it pressed states to put in place effective mechanisms for enforcing privacy rights, with particular emphasis on accessible remedies for individuals whose rights had been violated and on holding those responsible for unlawful interference legally accountable. The underlying message was that privacy protection cannot rest on preventive safeguards alone — it equally demands robust mechanisms for remedy and enforcement.²⁹

Most directly relevant to this study is Resolution 75/176 of 16 December 2020, which turned specifically to the growing use of digital and biometric identification systems. States were urged to take all necessary measures so that the development, deployment, and operation of such technologies conform to applicable legal and technical safeguards and remain fully consistent with international human rights obligations — a stance reflecting the mounting international concern over what biometric technologies may mean for privacy, data protection, and fundamental rights more broadly in an increasingly digital world.³⁰

Of the legally binding instruments in this field, none merits closer attention than the European Union's General Data Protection Regulation (GDPR). Among its most significant contributions is situating biometric data within the GDPR's special category of personal data — a classification reserved for information warranting heightened, rather than merely ordinary, legal protection. That classification is far from merely declaratory: it underpins the distinct regulatory regime Article 9 of the GDPR establishes for processing such data.

Article 9(2) frames this as a general prohibition subject to enumerated exceptions: the GDPR bars the processing of what it terms special categories of personal

²⁸ United Nations General Assembly, *The Right to Privacy in the Digital Age*, Resolution 68/167, A/RES/68/167, December 18, 2013, paras. 3 and 4(b)–(c), <https://docs.un.org/en/A/RES/68/167>.

²⁹ United Nations General Assembly, *The Right to Privacy in the Digital Age*, Resolution 69/166, A/RES/69/166, December 18, 2014, para. 4(d)–(e), <https://docs.un.org/en/A/RES/69/166>.

³⁰ United Nations General Assembly, *The Right to Privacy in the Digital Age*, Resolution 75/176, A/RES/75/176, December 16, 2020, para. 7(q), <https://docs.un.org/en/A/RES/75/176>.

data — biometric data used to uniquely identify a natural person among them — unless one of those exceptions is met. The data subject's explicit consent is one; others include information the individual has manifestly made public, the protection of vital interests belonging to the data subject or a third party, and processing grounded in substantial public interest and authorised by law, alongside further grounds tied to preventive medicine, occupational health, social protection, public health, and the administration of justice. The balance the GDPR is striking, in other words, is between legitimate uses of biometric technology and a consistently high level of protection for individual privacy and personal data.³¹

The European Union Artificial Intelligence Act (Regulation (EU) 2024/1689) has since refined and considerably expanded these safeguards, marking a major advance in protecting biometric data and guarding against its arbitrary processing by public authorities and private actors alike.

Much as the GDPR does, the AI Act bars AI systems from using biometric data to infer or determine sensitive personal characteristics — racial or ethnic origin, political opinion, philosophical belief, religious affiliation, sexual orientation, trade union membership, and other protected attributes chief among them. Remote biometric identification systems, particularly those operating in real time, are subject to especially strict limitations: given the profound implications for privacy and individual autonomy, law enforcement may deploy them only in a narrowly defined set of circumstances, weighed against the seriousness of the threat or offence at issue and subject to prior authorisation by a competent public authority. Systems used for biometric identification, verification, categorisation, or emotion recognition are, in turn, classified as high-risk AI applications and must therefore operate under appropriate human oversight throughout. Procedurally, the Act also strengthens individual rights — to be informed when a biometric AI system is in use, to receive a meaningful explanation of how such a system functions and what it produces, to challenge outcomes reached through automated processing, and, where relevant, to object to the use of biometric technology altogether. Taken together, these measures are meant to reconcile technological innovation with meaningful protection for privacy, human dignity, and other fundamental rights.³²

None of these changes the fact that these safeguards remain, in practice, bounded by how far EU law reaches territorially. EU data protection legislation does carry an extraterritorial dimension in certain provisions, but enforcing it beyond the jurisdiction of Member States is another matter — one made harder still in legal systems where supervisory authorities lack the powers, institutional capacity, or independence needed for effective oversight and strict compliance. The resulting disparities in regulatory approach and enforcement remain a significant obstacle to anything resembling a universally consistent standard of protection.³³

³¹ General Data Protection Regulation, arts. 2(2)(d) and 9(1)–(2).

³² Artificial Intelligence Act, arts. 5(1)(g)–(h), 5(2)–(7), 6(2)–(3), 14, 26(11), 50(3), and 86; annex III, point 1.

³³ Bhatti, “Digital Privacy,” 125; General Data Protection Regulation, art. 3.

4.2. The European Court of Human Rights' Evolving Doctrine on Mass Surveillance

Alongside the European Union's legislative framework stands the jurisprudence of the European Court of Human Rights (ECtHR), which occupies a place of its own within Europe's human-rights protection architecture. The European Convention on Human Rights (ECHR) of 1950 was, as already noted, among the earliest international instruments to guarantee respect for private and family life, home, and correspondence; yet it nowhere defines “private life” itself — the substance of Article 8 has instead been built up gradually through the Court's jurisprudence. It is that process of judicial interpretation, more than the text, that has turned the provision into a comprehensive source of privacy protection able to respond to new social and technological realities.

Much of this has been possible through the ECtHR's doctrine of dynamic interpretation, first articulated in *Tyrer v. the United Kingdom* (1978), where the Court described the Convention as a “living instrument” to be read in light of present-day conditions. That approach is what has let the Convention framework absorb profound technological change, extending Article 8 to matters its drafters never envisaged — personal-data protection, digital privacy, electronic communications, and, more recently, the human-rights implications of mass surveillance and biometric monitoring.³⁴ The same interpretative method has allowed the Court to keep pace with evolving social and technological realities within a comparatively short span of time — a responsiveness that has mattered all the more as digital transformation has accelerated across contemporary society.

This evolutionary approach reached a turning point in *S. and Marper v. the United Kingdom* (2008), where the Court held unequivocally that the retention of biometric information — including fingerprints and DNA profiles — amounts to an interference with the right to respect for private life under Article 8. This judgment established a significant precedent, confirming that biometric data falls within the scope of protected personal information and merits heightened safeguards under the European human-rights system.³⁵

Examining the Court's jurisprudence over time shows a close interplay between technological change and the interpretative approaches the ECtHR has adopted at different points. Three broad stages emerge, each mirroring the prevailing international perception of mass surveillance at the time. *Klass and Others v. Germany* (1978) and

³⁴ Ivan Levy, “Territorial and Material Jurisdiction of the European Court of Human Rights: How Flexible Has the ‘Living Instrument’ Been Thus Far?” in *European Yearbook on Human Rights 2025*, ed. Philip Czech et al. (Brill | Nijhoff, 2025), 64, https://doi.org/10.1163/9789004751026_005; see also *Tyrer v. the United Kingdom*, application no. 5856/72, European Court of Human Rights, judgment of April 25, 1978, para. 31, <https://hudoc.echr.coe.int/eng?i=001-57587>.

³⁵ Vilma Eriksson, “Facial Recognition and the Right to Privacy: Facial Recognition Technologies in Law Enforcement: A Legal Analysis of Their Compability with European Human Rights and the Principle of Proportionality” (bachelor's thesis, Örebro University, 2025), 14, <https://www.diva-portal.org/smash/record.jsf?pid=diva2:1980446>; see also *S. and Marper v. the United Kingdom*, application nos. 30562/04 and 30566/04, European Court of Human Rights, grand chamber judgment of December 4, 2008, paras. 67–86, <https://hudoc.echr.coe.int/eng?i=001-90051>.

Uzun v. Germany (2010) are the leading examples of the first: a relatively restrictive approach to state surveillance powers, applied with a narrow margin of appreciation to the monitoring of private correspondence, the interception of telephone communications, and the tracking of an individual's movements or location.

Reasoning during this period was defined by its reliance on reasonable suspicion and by a distinctly individual-centred perspective: in both cases the ECtHR insisted that surveillance measures could be justified only on objective grounds indicating that a specific individual was involved in, or intended to engage in, criminal activity. That requirement served as a safeguard against indiscriminate monitoring, keeping surveillance powers from extending to individuals with no apparent connection to unlawful conduct. *Klass and Others v. Germany* shows the balance the Court sought to achieve — recognising that covert surveillance may sometimes be necessary to safeguard national security and democratic institutions, while requiring that such powers stay subject to rigorous legal limits and effective safeguards against misuse, in order to preserve the principles underlying a democratic society.³⁶

None of this is surprising given the technological realities of the period: covert surveillance existed, but the technical means for systematic, large-scale monitoring of entire populations did not, so surveillance measures required substantial human involvement and targeted identifiable individuals rather than broad categories of persons. The Court's jurisprudence was, in short, shaped by a world in which the principal threat to privacy came from targeted state interference rather than from technologically enabled systems capable of continuous, automated, mass surveillance of society at large.³⁷ Scholars have since observed that this approach sits uneasily with contemporary technological realities. Widespread video surveillance, the accumulation of digital footprints, and the growing use of automated data-processing have all but eliminated the time and resources once needed to identify and monitor individuals, so that surveillance is no longer confined to targeted measures against specific suspects but may extend to large-scale data collection affecting whole segments of the population. Legal safeguards built primarily around reasonable suspicion, in this light, are often ill-equipped to address the risks that modern digital and biometric surveillance pose.³⁸

The second stage marks a departure from the first, bringing with it the emergence of biometric data as a distinct legal category — a shift the Court's judgment in *S. and Marper v. the United Kingdom* and *Van der Velden v. the Netherlands* illustrate most clearly. Both recognised that retaining DNA profiles amounts to a particularly serious interference with respect for private life, distinguishing between

³⁶ *Klass and Others v. Germany*, application no. 5029/71, European Court of Human Rights, judgment of September 6, 1978, paras. 42 and 49–51, <https://hudoc.echr.coe.int/eng?i=001-57510>; *Uzun v. Germany*, application no. 35623/05, European Court of Human Rights, judgment of September 2, 2010, paras. 66 and 69–74, <https://hudoc.echr.coe.int/eng?i=001-100293>.

³⁷ Asaf Lubin, "The Liberty to Spy," *Harvard International Law Journal* 61, no. 1 (2020): 222, <https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/61.1-Lubin.pdf>.

³⁸ Didier Bigo, "Digital Controls, Mobility and Surveillance; the Social Universe of 'Reasonable Suspicion' and Its Different Guilds," in *EU Law in the Digital Age*, ed. Maria Bergström and Valsamis Mitsilegas (Hart Publishing, 2025), 378, <https://doi.org/10.5040/9781509981212.ch-020>.

different stages of personal data processing and underscoring the need for enhanced safeguards specific to biometric information. The ECtHR went further still, differentiating between stored information capable of identifying a specific individual and information that was not, pointing to the Commission's earlier decision in *Friedl v. Austria* — where no violation was found precisely because the authorities lacked the technical means to process the photographs and identify the persons, they depicted³⁹. What sets biometric data apart from ordinary photographs, the Court observed, is the unique information it carries about an individual and its distinctive capacity to enable accurate identification. On this basis, the ECtHR has found that the mere storage of biometric data can itself constitute an interference with the right to private life, irrespective of whether that information is, or is meant to be, used to identify a particular person.⁴⁰

The third stage — itself divisible into two sub-periods — is marked by a renewed emphasis on rigorous preventive safeguards and mechanisms of oversight, reflecting growing judicial concern over the widespread deployment of biometric identification technologies and the increasing role of private actors in data processing. The Grand Chamber's judgment in *Big Brother Watch and Others v. the United Kingdom* (2021) offers the clearest illustration: there, the Court effectively acknowledged that large-scale surveillance has become an entrenched feature of the digital era that cannot realistically be eliminated, meaning the lawfulness of surveillance measures increasingly hinges on how effectively the handling and use of collected data is safeguarded, rather than on the circumstances of its initial acquisition.⁴¹ Scholars have been quick to criticise this stance as excessively deferential to state surveillance powers. By treating mass surveillance as not inherently unlawful or disproportionate, and by shifting the emphasis toward safeguards on the subsequent processing of data rather than its initial collection, the Court is said to have effectively expanded the discretion states enjoy in conducting large-scale monitoring — a shift that critics contend weakens the protection Article 8 provides and reflects the mounting difficulty of safeguarding privacy amid pervasive digital surveillance.⁴² The same period, though, brought a genuine positive development: an expansion of the minimum safeguards meant to prevent abuse of mass surveillance systems by public authorities. *Big Brother Watch and Others v. the United Kingdom* is once again the key authority, with the ECtHR

³⁹ *Friedl v. Austria*, application no. 15225/89, European Court of Human Rights, judgment striking the case out following a friendly settlement of January 31, 1995, Series A, no. 305-B, <https://hudoc.echr.coe.int/eng?i=001-57917>; for the Commission's assessment of the photographs, see *S. and Marper*, para. 82.

⁴⁰ *S. and Marper*, paras. 67–86 and 119–25, <https://hudoc.echr.coe.int/eng?i=001-90051>; *Van der Velden v. the Netherlands*, application no. 29514/05, European Court of Human Rights, admissibility decision of December 7, 2006, “The law,” art. 8, <https://hudoc.echr.coe.int/eng?i=001-78858>.

⁴¹ *Big Brother Watch and Others v. the United Kingdom*, application nos. 58170/13, 62322/14, and 24960/15, European Court of Human Rights, grand chamber judgment of May 25, 2021, paras. 332–50, <https://hudoc.echr.coe.int/eng?i=001-210077>.

⁴² Sophie Duroy and Martin Scheinin, *National Security as Exception: The European Court of Human Rights and the Proceduralisation of Privacy in the Age of Mass Surveillance*, LAW Working Paper 2026/11 (European University Institute, 2026), 11, <https://cadmus.eui.eu/entities/publication/b622bfec-fa70-46de-9414-363d13180736>.

laying out the essential guarantees any such measure must satisfy — clear legal grounds for deploying bulk surveillance, specific conditions governing the interception of particular individuals' communications, procedural requirements for authorisation and data processing, effective oversight by independent supervisory bodies, avenues for ex post facto review, and adequate safeguards on transferring collected information to third parties.⁴³

Glukhin v. Russia (2023) marks a further significant turning point, being the Court's first major decision to confront real-time facial recognition as a form of mass biometric surveillance. The ECtHR reaffirmed that a legitimate expectation of privacy survives even in public spaces and, while accepting that monitoring a person's movements in public may sometimes be permissible, drew a firm line between ordinary video surveillance and the systematic recording, retention, and processing of an individual's image — the latter constituting an interference with the right to respect for private life precisely because storing and analysing such data allows a person to be identified and tracked through their unique biometric characteristics. Importantly, the Court went further still, holding that the stakes extend beyond the individual concerned: pervasive facial-recognition technology risks producing a chilling effect across society as a whole, affecting the exercise of freedom of expression and the functioning of democratic society itself.⁴⁴ In reformulating the concept of reasonable suspicion, the Court has progressively redirected its focus from the mere collection of personal data to the subsequent stages of its processing, thereby reshaping what legality and necessity require in a democratic society.⁴⁵

5. Conclusions

The findings of this study demonstrate that biometric surveillance has become one of the most intrusive instruments of contemporary digital governance. Although such technologies strengthen the capacity of public authorities to address security concerns, they simultaneously create significant challenges for the protection of privacy, informational autonomy, and individual freedom from arbitrary interference. Their rapid expansion therefore requires a regulatory framework capable of balancing legitimate public interests with effective safeguards for fundamental rights.

The unique, permanent, and sensitive nature of biometric data justifies enhanced legal protection. Unlike other categories of personal data, biometric identifiers cannot readily be replaced once they have been exposed, which heightens the risks tied to their unlawful collection, retention, disclosure, or processing. Consequently, any interference involving biometric data should be limited by clearly defined legal grounds, legitimate purposes, proportionality requirements, temporal restrictions, and effective oversight. These concerns are particularly evident in the use of automated facial recognition technologies, which enable large-scale monitoring

⁴³ *Big Brother Watch and Others*, paras. 350–61.

⁴⁴ *Glukhin v. Russia*, application no. 11519/20, European Court of Human Rights, judgment of July 4, 2023, paras. 65–73 and 83–89, <https://hudoc.echr.coe.int/eng?i=001-225655>.

⁴⁵ Gabrielli, “Use of Facial Recognition Technologies,” 534.

without individuals' knowledge or meaningful control over their personal information.

This study's review of international legal instruments and ECtHR case law shows that biometric surveillance can be reconciled with human rights only where it rests on a clear legal framework, serves a legitimate aim, and meets the principles of necessity and proportionality. References to national security or public safety alone cannot justify indiscriminate collection, prolonged retention, or unrestricted use of biometric data. Effective procedural safeguards, independent supervision, and access to judicial remedies therefore remain indispensable.

Recent European legislation — most notably the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act — reflects an increasingly stringent stance on biometric data processing and AI-driven surveillance. These instruments reinforce a human rights-oriented model of technological governance and offer guidance for Ukraine, where further legislative development is still needed to regulate the gathering, storage, transfer, and disposal of biometric data.

In order to mitigate legal risks and prevent misuse, legislation should clearly define the purposes of biometric surveillance, specify which entities are authorised to conduct it, and prohibit indiscriminate or large-scale biometric monitoring except in narrowly defined circumstances subject to enhanced oversight. Human rights impact assessments and proportionality evaluations should precede the deployment of new biometric technologies. Supervisory authorities should be empowered to audit institutions using biometric systems, while transparency obligations, limited data-retention periods, mandatory data deletion, and effective accountability mechanisms should be established. Technical safeguards, including encryption, access controls, cybersecurity assessments, and independent algorithmic audits, are equally essential to reduce bias, inaccuracies, and discriminatory outcomes. Individuals must also have access to effective judicial and non-judicial remedies against unlawful biometric processing.

Future research should examine comparative regulatory approaches across the European Union, Ukraine, and other jurisdictions; assess judicial oversight through ECtHR case law; explore the risks of AI-assisted facial recognition, including algorithmic bias and misidentification; evaluate the balance between national security and privacy; and develop legal standards governing biometric technologies in public administration and law enforcement.

In conclusion, the challenges posed by biometric surveillance cannot be addressed through isolated legal measures. Effective governance depends on a comprehensive framework that integrates legal regulation, institutional oversight, technological safeguards, and judicial accountability to ensure biometric technologies are deployed without compromising fundamental rights and democratic values.

Bibliography

I. Books and Articles

Bentotahewa, Vibhushinie, Chaminda Hewage, and Jason Williams. "The Normative Power of

- the GDPR: A Case Study of Data Protection Laws of South Asian Countries.” *SN Computer Science* 3, no. 3 (2022): article 183. <https://doi.org/10.1007/s42979-022-01079-z>.
- Bhatti, Novera. “Digital Privacy as a Human Rights in the Era of Mass Surveillance.” *DME Journal of Law* 5, no. 2 (2024): 120–37. <https://dmejournals.com/index.php/DMEJL/article/view/598>.
- Bigo, Didier. “Digital Controls, Mobility and Surveillance; the Social Universe of ‘Reasonable Suspicion’ and Its Different Guilds.” In *EU Law in the Digital Age*, edited by Maria Bergström and Valsamis Mitsilegas, 371–88. Hart Publishing, 2025. <https://doi.org/10.5040/9781509981212.ch-020>.
- Duroy, Sophie, and Martin Scheinin. *National Security as Exception: The European Court of Human Rights and the Proceduralisation of Privacy in the Age of Mass Surveillance*. LAW Working Paper 2026/11. European University Institute, 2026. <https://cadmus.eui.eu/entities/publication/b622bfee-fa70-46de-9414-363d13180736>.
- Eriksson, Vilma. “Facial Recognition and the Right to Privacy: Facial Recognition Technologies in Law Enforcement: A Legal Analysis of Their Compability with European Human Rights and the Principle of Proportionality.” Bachelor’s thesis, Örebro University, 2025. <https://www.diva-portal.org/smash/record.jsf?pid=diva2:1980446>.
- Fussey, Peter, and Daragh Murray. “Policing Uses of Live Facial Recognition in the United Kingdom.” In *Regulating Biometrics: Global Approaches and Urgent Questions*, edited by Amba Kak, 78–85. AI Now Institute, 2020. <https://ainowinstitute.org/wp-content/uploads/2023/09/regulatingbiometrics-fussey-murray.pdf>.
- Gabrielli, Giulia. “The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights.” *European Journal of Risk Regulation* 16, no. 2 (2025): 514–41. <https://doi.org/10.1017/err.2025.26>.
- Hachkevych, Andrii O. “The Concept of Biometric Data in the Legislation of Ukraine and Other Countries.” *Visnyk of Mariupol State University. Series: Law* 15, no. 30 (2025): 16–26. <https://doi.org/10.34079/2518-1319-2025-15-30-16-26>.
- Haley, Patricia. “The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent.” *Sensors* 25, no. 10 (2025): 3160. <https://doi.org/10.3390/s25103160>.
- Jung, Youna, and Ethan D. Virgil. “Analysis of Legislative Framework Governing Biometric Data.” *Procedia Computer Science* 241 (2024): 48–55. <https://doi.org/10.1016/j.procs.2024.08.009>.
- Kopanchuk, Volodymyr, Olena Kopanchuk, Oleh Kravchuk, and Vadym Torichnyi. “Biometric Identification Systems as a Tool of Public Administration to Ensure Internal Security.” *Uspikhy i Dosiahnennia u Nauksi*, no. 9 (19) (2025): 527–39. [https://doi.org/10.52058/3041-1254-2025-9\(19\)-527-539](https://doi.org/10.52058/3041-1254-2025-9(19)-527-539).
- Kopel, Orit. “In the Face of Ethics: Police Use of Live Facial Recognition Technology.” PhD diss., King’s College London, 2024. <https://kclpure.kcl.ac.uk/portal/en/studentTheses/in-the-face-of-ethics/>.
- Levy, Ivan. “Territorial and Material Jurisdiction of the European Court of Human Rights: How Flexible Has the ‘Living Instrument’ Been Thus Far?” In *European Yearbook on Human Rights 2025*, edited by Philip Czech, Lisa Heschl, Karin Lukas, Manfred Nowak, Gerd Oberleitner, and Hannes Tretter, 62–95. Brill | Nijhoff, 2025. <https://>

doi.org/10.1163/9789004751026_005.

- Lubin, Asaf. “The Liberty to Spy.” *Harvard International Law Journal* 61, no. 1 (2020): 185–240. <https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/61.1-Lubin.pdf>.
- Magee, Patrick, Marcello Ienca, and Nita Farahany. “Beyond Neural Data: Cognitive Biometrics and Mental Privacy.” *Neuron* 112, no. 18 (2024): 3017–28. <https://doi.org/10.1016/j.neuron.2024.09.004>.
- Melzi, Pietro, Christian Rathgeb, Ruben Tolosana, Ruben Vera-Rodriguez, and Christoph Busch. “An Overview of Privacy-Enhancing Technologies in Biometric Recognition.” *ACM Computing Surveys* 56, no. 12 (2024): article 310. <https://doi.org/10.1145/3664596>.
- Sayler, Kelley M. *Biometric Technologies and Global Security*. In Focus IF11783. Congressional Research Service, updated April 16, 2026. <https://www.congress.gov/crs-product/IF11783>.
- Singh, Avani, and Michael Power. “The Privacy Awakening: The Urgent Need to Harmonise the Right to Privacy in Africa.” *African Human Rights Yearbook* 3 (2019): 202–20. <https://doi.org/10.29053/2523-1367/2019/v3a10>.
- Wang, Xiaomeng, Yishi Zhang, and Ruilin Zhu. “A Brief Review on Algorithmic Fairness.” *Management System Engineering* 1 (2022): article 7. <https://doi.org/10.1007/s44176-022-00006-z>.

II. International Regulations and Documents

- Council of Europe. *Convention for the Protection of Human Rights and Fundamental Freedoms*. ETS No. 5. November 4, 1950. https://www.echr.coe.int/documents/d/echr/convention_ENG.
- Council of Europe. *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. CETS No. 223. October 10, 2018. <https://rm.coe.int/16808ac91a>.
- European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* L 119 (May 4, 2016): 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.
- European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). *Official Journal of the European Union* L, 2024/1689 (July 12, 2024). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.
- Organization of American States. *American Declaration of the Rights and Duties of Man*. Ninth International Conference of American States, Bogotá, 1948. https://www.oas.org/dil/access_to_information_human_right_American_Declaration_of_the_Rights_and_Duties_of_Man.pdf.
- United Nations General Assembly. *International Covenant on Civil and Political Rights*. Resolution 2200 A (XXI), annex. December 16, 1966. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
- United Nations General Assembly. *The Right to Privacy in the Digital Age*. Resolution 68/167,

A/RES/68/167. December 18, 2013. <https://docs.un.org/en/A/RES/68/167>.

United Nations General Assembly. *The Right to Privacy in the Digital Age*. Resolution 69/166, A/RES/69/166. December 18, 2014. <https://docs.un.org/en/A/RES/69/166>.

United Nations General Assembly. *The Right to Privacy in the Digital Age*. Resolution 75/176, A/RES/75/176. December 16, 2020. <https://docs.un.org/en/A/RES/75/176>.

United Nations General Assembly. *Universal Declaration of Human Rights*. Resolution 217 A (III). December 10, 1948. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

III. Case Law

European Court of Human Rights. *Big Brother Watch and Others v. the United Kingdom*. Application nos. 58170/13, 62322/14, and 24960/15. Grand Chamber judgment of May 25, 2021. <https://hudoc.echr.coe.int/eng?i=001-210077>.

European Court of Human Rights. *Friedl v. Austria*. Application no. 15225/89. Judgment striking the case out following a friendly settlement of January 31, 1995. Series A, no. 305-B. <https://hudoc.echr.coe.int/eng?i=001-57917>.

European Court of Human Rights. *Glukhin v. Russia*. Application no. 11519/20. Judgment of July 4, 2023. <https://hudoc.echr.coe.int/eng?i=001-225655>.

European Court of Human Rights. *Klass and Others v. Germany*. Application no. 5029/71. Judgment of September 6, 1978. Series A, no. 28. <https://hudoc.echr.coe.int/eng?i=001-57510>.

European Court of Human Rights. *S. and Marper v. the United Kingdom*. Application nos. 30562/04 and 30566/04. Grand Chamber judgment of December 4, 2008. <https://hudoc.echr.coe.int/eng?i=001-90051>.

European Court of Human Rights. *Tyrer v. the United Kingdom*. Application no. 5856/72. Judgment of April 25, 1978. Series A, no. 26. <https://hudoc.echr.coe.int/eng?i=001-57587>.

European Court of Human Rights. *Uzun v. Germany*. Application no. 35623/05. Judgment of September 2, 2010. <https://hudoc.echr.coe.int/eng?i=001-100293>.

European Court of Human Rights. *Van der Velden v. the Netherlands*. Application no. 29514/05. Admissibility decision of December 7, 2006. <https://hudoc.echr.coe.int/eng?i=001-78858>.