BIOMETRIC TECHNOLOGIES: ETHICAL CHALLENGES AND LEGAL ASPECTS

Veronika Horielova[1]

DOI: https://doi.org/10.30525/978-9934-26-602-7-29

Abstract. Biometric technologies are currently among the most significant and, at the same time, most controversial tools of digital transformation, changing the ways of identification, verification, and control of individuals in many areas of public life. The subject of this study is biometrics not only as a technical means of authentication, but as a complex interdisciplinary phenomenon at the intersection of law, ethics, and information technology. The peculiarity of this technology is that it makes the human body and its unique characteristics a central element in identity management processes. As a result, a new paradigm is emerging, in which the individual is effectively merged with their biological data, thus giving rise to far-reaching social consequences. The aim of the study is to analyse the legal and ethical challenges associated with the use of biometrics, as well as to outline the tension between innovative development, security requirements, and respect for fundamental human rights. Particular attention is paid to issues of privacy, the preservation of autonomy, and threats of discrimination caused by algorithmic bias. The study also explores the vulnerability of biometric infrastructures – particularly the irreversibility of biometric template compromise – and its broader implications for democracy, digital trust, and social justice. The methodological framework is based on several complementary approaches. First, an overview of international legal instruments has been conducted, including the European Union's General Data Protection Regulation (GDPR) and the Council of Europe's Convention 108+. Second, a comparative analysis has been applied, taking into account the experiences of various countries: from the widespread use of biometric surveillance in China, to border control practices in the United

[1] PhD in Law, Associate Professor,
Associate Professor of the Department of State Law and Humanities,
V.I. Vernadsky Taurida National University,
Educational and Scientific Institute of Humanities,
Department of State Law and Humanities, Ukraine

States, and the implementation of biometrics in e-governance systems in Ukraine. Third, the method of theoretical generalisation has been employed to develop a conceptual framework for the ethical and legal debates surrounding biometrics. The findings indicate that biometrics presents a wide range of risks. These include restrictions on privacy and autonomy, the dangers of mass surveillance – which leads to a "chilling effect" on civil liberties – and the reproduction of social inequality through algorithmic bias. Legal analysis demonstrates that, despite the existence of international standards, gaps remain in ensuring proportionality, informed consent, and accountability of stakeholders. Technical solutions such as encryption, hashing, or multibiometrics offer partial protection mechanisms; however, they do not eliminate the fundamental problem of irreversibility in the event of data compromise. The conclusion of the study highlights the urgent need to maintain a balance between security and human rights in the context of the rapid expansion of biometric technologies. Biometrics can enhance efficiency and increase trust in digital services only when embedded within clear ethical frameworks, transparent governance mechanisms, and internationally recognised legal standards. Without such a balance, biometrics risks shifting from a tool of protection to a means of control, potentially undermining the foundations of democratic society.

1. Introduction

In the era of digital transformation, biometric technologies are increasingly shaping the architecture of information security, identification processes, and human interaction with governmental and commercial structures. Whereas identity verification was previously based on documents, passwords, or codes, today the leading tool is the use of an individual's physical and behavioural characteristics. Fingerprints, voice, facial geometry, gait, or even typing dynamics are becoming universal 'access keys' to financial, administrative, and social services [1]. This entails not only an increase in the effectiveness of identification systems but also the emergence of qualitatively new ethical and legal challenges that require comprehensive investigation.

The relevance of this issue is determined by several factors. First, biometrics concerns the most sensitive area, namely the physiological and behavioural identity of an individual, which is unique and remains

unchanged throughout life. Secondly, the widespread introduction of technologies in public administration, transport, finance, and healthcare creates risks of mass surveillance and the loss of anonymity in public spaces [2]. Thirdly, the insufficient development of the regulatory framework, which lags behind the pace of technological innovation, exacerbates the problem of legal uncertainty and thereby increases the risk of violations of fundamental human rights and freedoms [3].

The purpose of this chapter is to examine biometric technologies through the prism of their legal and ethical dimensions, with an emphasis on achieving a balance between innovative security measures and the protection of privacy and human dignity. The objectives of the study are to systematise the key characteristics of biometric data, analyse the principal ethical risks, review international standards of legal regulation [4], and substantiate the concept of the digital ethics of biometrics as a new framework for public understanding.

The methodological basis consists of the provisions of international and European law in the field of personal data protection (the General Data Protection Regulation (GDPR) [5], the Council of Europe Convention 108+ [4]), as well as an interdisciplinary approach combining legal analysis, ethical reflection, socio-philosophical generalisations, and the findings of contemporary research in the field of cybersecurity. The structure of the presentation is based on clarifying the essence of biometrics and its key properties, addressing ethical and legal challenges, and identifying optimal mechanisms for their regulation.

The scientific novelty of the study lies in its comprehensive interdisciplinary analysis of biometric technologies, integrating legal, ethical, technical, and social dimensions. The study emphasises that biometrics extends beyond the traditional legal regulation of personal data and constitutes a new paradigm of identification, which significantly transforms the relationship between security and fundamental human rights.

The novelty is manifested in several key provisions. First, the concept of the "chain vulnerability of biometrics" is introduced, denoting the risk of multiple compromises of an individual resulting from the leakage of a single biometric parameter. Secondly, the problem of the loss of anonymity in public space, caused by the spread of remote facial recognition systems and behavioural profiling, is examined, and its consequences for democratic

practices are analysed. Thirdly, an interpretation of algorithmic bias is proposed as a new form of digital discrimination, which may reproduce social inequality in access to services.

The study proposes an author's approach to evaluating biometric technologies, which combines technical performance indicators – FAR (False Acceptance Rate), FRR (False Rejection Rate), and EER (Equal Error Rate) [6] – with ethical and legal criteria for the protection of privacy, autonomy, and human dignity [7]. This integrated approach allows for moving beyond traditional technical metrics and developing a concept of digital ethics in biometrics, which, by analogy with bioethics in medicine, delineates the limits of acceptable use of identification technologies.

Thus, the novelty of the study lies in the development of a comprehensive framework for analysing biometrics as a tool that simultaneously provides innovative security and generates profound ethical and legal challenges, which require new regulatory and scholarly consideration.

2. Theoretical and methodological foundations of biometrics

In contemporary scholarly discourse, biometrics emerges as a multilayered phenomenon that integrates elements of biology, cybernetics, mathematics, engineering, psychology, and law. [8]. Its subject matter is the identification of individuals based on unique physiological or behavioural characteristics, which are subject to digital encoding and subsequent algorithmic analysis [9]. At the same time, biometrics is not limited to the technological domain: it increasingly assumes the status of a socio-legal institution that defines the boundaries of privacy, freedom, and security in the digital age.

The key methodological principle of biometrics is the algorithmisation of human uniqueness, whereby a physical or behavioural characteristic is transformed into a digital template [10]. This implies that identity ceases to be merely a social or legal category and acquires a new technical and mathematical dimension. A defining feature of biometric data is its inalienability: unlike a password or document, an individual cannot change or transfer their fingerprints or facial geometry [11]. This immutability ensures high identification accuracy but also gives rise to fundamental risks in the event of compromise.

Among other characteristics, it is important to highlight uniqueness, which guarantees the exceptional distinctiveness of each individual's biometric parameters, and stability, which ensures the persistence of traits over an extended period. Equally significant is measurability, that is, the capacity of biometric characteristics to be digitally represented through sensors and software algorithms. The category of acceptability also remains important, as the level of societal acceptance of biometrics depends on cultural, psychological, and social factors. Finally, resistance to falsification and scalability determine the reliability and performance of biometric systems in large-scale applications [12].

A methodological understanding of biometrics requires its consideration within the broader context of human rights. While in the classical approach personal data were regarded as attributes that could be changed or restored, biometric characteristics constitute irreplaceable markers that accompany an individual throughout their life. This fundamentally alters approaches to their legal regulation: under international law, they are recognised as a "particularly sensitive category", requiring additional safeguards for confidentiality and minimisation of the risks of misuse.

From a scientific and methodological perspective, biometrics is not only a technological process but also a new paradigm of identity. Individuals no longer have full control over their personal data, as it becomes subject to algorithmic analysis, is stored in centralised or cloud-based repositories, and may potentially be used for purposes other than those declared. This underscores the need for a multidimensional study of biometrics, which must take into account the technical characteristics of systems, legal standards, ethical principles, and social consequences.

Thus, the theoretical and methodological foundations of biometrics can be summarised as the combination of two interrelated dimensions: the technological, which determines the algorithms for collecting and processing unique traits, and the socio-legal, which delineates the boundaries of their permissible use. It is precisely this duality that renders biometrics a phenomenon that simultaneously opens new horizons for security and generates profound challenges to individual autonomy, privacy, and human dignity.

3. Ethical Risks of Using Biometrics

The introduction of biometric technologies is accompanied not only by technical and organisational challenges but also by profound ethical issues that directly impact fundamental human rights and freedoms. While biometrics is designed at the technological level to enhance the convenience and reliability of identification, it poses, in the social dimension, a range of threats that could transform the very nature of the relationship between individuals and institutions.

One of the most prominent ethical challenges is the risk of privacy loss. Biometric features (fingerprints, facial features, voice, gait) are intrinsic characteristics of an individual that cannot be altered if compromised. While a leaked password or digital code can be neutralised by changing it, a leaked biometric template creates a lifelong vulnerability that accompanies the individual throughout their life [10]. Consequently, the individual is effectively deprived of the ability to regain control over their own identity, which contravenes the fundamental principle of autonomy.

Equally concerning is the phenomenon of mass and remote surveillance, made possible by the development of video analytics systems and facial recognition algorithms. Biometrics transforms public space into a zone of potential control, where an individual's whereabouts are constantly recorded and analysed [13]. Under such conditions, the right to anonymity in the social environment, which has historically served as a guarantee of freedom of movement and expression, is gradually being eroded. Aware of the constant possibility of identification, individuals tend to alter their behaviour, self-censor their actions, and avoid open forms of communication. This effect, recognised in legal doctrine as the 'chilling effect', poses a serious threat to democratic practices [14].

The third ethical challenge is coercion and the formalisation of consent. Although international standards, in particular the GDPR, require voluntary and informed consent for the processing of biometric data, in practice participation in such procedures is often a prerequisite for access to public services, banking transactions, or digital platforms [15]. Under such circumstances, consent becomes more a formality than an expression of free will. Individuals are effectively deprived of any alternative, as refusing to provide biometric samples entails losing access to essential services.

Such covert coercion undermines the principle of personal autonomy and diminishes the ethical significance of consent.

The issue of algorithmic bias is also significant. Biometric systems operate on the basis of mathematical models developed using training data samples. If these data are unrepresentative, the algorithms reproduce hidden social barriers and may exhibit varying degrees of accuracy depending on the gender, age, or ethnicity of users [16]. In such instances, identification errors go beyond technical malfunctions and become a factor of discrimination with tangible socio-legal consequences. Thus, biometrics can reinforce existing inequalities by generating new forms of digital injustice.

The phenomenon of biometric profiling warrants particular attention. It involves not only the use of biometric characteristics for authentication but also their application for analytical and commercial purposes – ranging from marketing to the monitoring of emotional states [17]. The collection and integration of various biometric parameters enables the creation of comprehensive digital profiles that may contain information about health, psychological traits, or even political preferences [18]. This gives rise to opportunities for manipulation and covert control, which are incompatible with the principles of transparency and integrity.

From an ethical perspective, the issue of vulnerability to abuse by the state or corporations is also highly sensitive. The centralisation of vast amounts of biometric data in state registers or cloud storage creates conditions for the development of a total surveillance infrastructure. When combined with artificial intelligence technologies, such infrastructure can operate invisibly, transforming society into a space of covert control. In this context, the concern extends beyond technical security to the preservation of fundamental democratic values.

Thus, the ethical risks of biometrics extend beyond privacy concerns or technical failures. They pertain to fundamental aspects of human dignity, freedom, and autonomy. By transforming physical characteristics into a digital identifier, biometrics presents individuals with new challenges: how to maintain control over their own data, how to avoid becoming the subject of constant surveillance, and how to prevent algorithmic discrimination. Addressing these questions goes beyond technological efficiency and necessitates the establishment of an ethical and legal framework capable of balancing security interests with inalienable human rights.

4. Legal Foundations for the Processing of Biometric Data

The legal regulation of biometric technologies in the contemporary world is characterised by a combination of international standards, regional instruments, and national legislation aimed at ensuring a balance between the use of innovation and the protection of human rights. Biometric data are recognised as a particularly sensitive category of personal information, as their processing is directly associated with risks of privacy loss and breaches of the principle of personal autonomy.

The most developed legal framework in the field of biometrics is that of the European Union, where the General Data Protection Regulation (GDPR, 2016/679) establishes a special regime for data that enables the identification of individuals based on physiological or behavioural characteristics. Article 9 of the Regulation explicitly classifies biometrics as a 'special category of personal data,' the processing of which is prohibited except in specific cases (notably, with the explicit consent of the data subject, in the field of healthcare, within the context of employment relationships, or to protect the public interest) [12]. This framework exemplifies the principles of purpose limitation and proportionality, according to which the processing of biometric data is permitted only to the extent that it is necessary and justified.

In view of technological developments, the Council of Europe also places considerable emphasis on biometrics. The revised Convention No. 108+ "Convention for the Protection of Individuals with regard to the Automated Processing of Personal Data" underscores the need to provide special legal protection for data relating to the unique characteristics of individuals [5]. The document emphasises the principle of data minimisation, according to which only information necessary to achieve a specific and lawful purpose may be processed.

In a number of countries, including the United States, China, India, and Canada, specific legislative approaches to biometrics have also been developed. In the United States, regulation is fragmented: in certain states, such as Illinois and Texas, specific acts – namely the Biometric Information Privacy Act (BIPA) and the Capture or Use of Biometric Identifier Act (CUBI) – require the obtaining of written consent and provide the right to legal action in the event of violations [19]. China and India, by contrast, are moving towards the creation of large-scale state biometric registries,

which has attracted criticism due to the risks of total surveillance [20]. This illustrates the absence of universal standards and underscores the need for international harmonisation.

A key legal concept in the field of biometrics is informed consent. Its essence lies in an individual providing voluntary permission for the processing of their data after receiving complete and comprehensible information regarding the purpose, scope, retention period, and potential consequences of its use [15]. However, in practice, consent often assumes a merely declarative character: citizens sign standard agreements without fully understanding the scale and risks associated with biometric processing. As a result, the issue of formalised consent arises, undermining the notion of genuine expression of will [21].

The law also establishes a number of principles aimed at limiting arbitrariness in the processing of biometric data. These include:

– Legality and fairness – any operation involving data must be conducted on the basis of a legal norm and in the interest of the individual;

– Transparency – data subjects must be aware of who processes their data, how it is processed, and for what purpose;

– Purpose limitation – the use of biometrics only for predefined objectives;

– Storage limitation – destruction of data once the purpose for which it was collected has been achieved;

– Security – implementation of technical and organisational measures to protect against unauthorised access;

– Accountability – the organisation processing biometric data is responsible for ensuring compliance with these principles.

The issue of proportionality is of particular significance. The use of biometrics must be justified in each specific case and should not constitute excessive intrusion into private life. For example, the use of fingerprints for access to a bank account may be considered justified, whereas their collection in kindergartens or schools raises questions regarding necessity and proportionality. In this context, the principle of proportionality is regarded as a key mechanism for balancing a legitimate objective with the degree of intrusion into an individual's private sphere [22].

Scientific discussions are increasingly focusing on the concept of human rights to bodily integrity and informational self-determination, which

are becoming foundational for assessing the permissibility of biometric practices [23]. These rights emphasise that individuals should have control not only over their physical characteristics but also over their digital representations [24]. In the long term, this approach may contribute to the development of new legal standards, particularly in the domains of digital ethics and future-oriented law.

In conclusion, the legal foundations for the processing of biometric data are built on a combination of general principles for the protection of privacy and specific regulatory mechanisms recognising their particular sensitivity. Nevertheless, even in the most developed regulatory systems, there remain "grey areas" that require further consideration: the issue of formal consent, the risks associated with the centralisation of databases, and the absence of international harmonisation. This underscores the need to develop global standards that integrate legal, ethical, and technical approaches to the use of biometrics.

5. Practical domains of application

Biometric technologies are gradually extending beyond highly specialised fields and are becoming a universal tool of identification across a wide range of contexts. Their expansion is driven by the demand for rapid and reliable identity verification that cannot be substituted or transferred to another individual. At the same time, each domain of application offers particular advantages while simultaneously generating specific risks.

One of the most significant domains of biometric application is public administration and security. Many countries are actively developing national biometric registries containing citizens' fingerprints, photographs, and other personal data [12]. Biometrics are employed in the issuance of passports, identity cards, visas, and even electoral documents. In the context of border control, facial recognition and fingerprint technologies facilitate faster border crossings while enhancing security [4]. Nevertheless, this also entails the risk of establishing an infrastructure for mass state surveillance, in which citizens effectively forfeit their right to privacy in public spaces [19].

Biometrics are being integrated into law enforcement with equal intensity. Video surveillance systems equipped with facial recognition are employed to identify suspects, manage public events, and monitor crime

rates [20]. Biometric analysis enables the identification of individuals even on the basis of fragmentary data, such as fingerprints or voiceprints. However, the deployment of such technologies carries a significant risk of abuse, particularly in the context of political protests or the activities of opposition groups. The core problem lies in the absence of adequate safeguards against malicious use and the insufficiency of societal oversight.

An important sphere of development is banking and finance. Biometrics are increasingly employed to authenticate customers when making payments, accessing personal accounts, or using mobile applications [24]. Such systems substantially enhance convenience, as they replace passwords, which users may forget or inadvertently disclose to third parties. At the same time, there is a significant threat of cyberattacks and leaks of biometric templates, which may result in large-scale financial fraud. This problem is further compounded by the fact that, unlike passwords, biometric data cannot be altered once compromised, creating an irreversible loss effect.

The application of biometrics in transport infrastructure is acquiring particular significance. In many airports worldwide, automated passenger control systems operate on the basis of fingerprint and facial geometry analysis. These systems minimise the human factor, reduce waiting times, and enhance the efficiency of border-control procedures. However, in the event of technical failures or identification errors, passengers may be subjected to discrimination or unwarranted delays, highlighting the importance of combining technological solutions with effective mechanisms of appeal and oversight.

The use of biometrics in the medical sphere is of considerable interest. Biometric data may be applied for patient identification, for securing access to electronic medical records, or even for the diagnosis of health conditions. For instance, voice analysis can reveal indicators of certain diseases, while the monitoring of micro-expressions may provide insights into an individual's psycho-emotional state. At the same time, however, concerns arise regarding the confidentiality of medical data, which belong to a particularly sensitive category, and the risk of their misuse.

Biometrics are also spreading into the spheres of education and private business. In educational institutions, biometric systems are sometimes employed to monitor attendance, while in corporate environments they are used to regulate access to office premises or secured computer systems.

Such practices may enhance discipline and security, but they also pose the risk of excessive intrusion into the lives of students and employees, fostering an atmosphere of distrust and constant surveillance.

All of the above examples illustrate the dual nature of biometrics as a tool: on the one hand, it enhances convenience and security, while on the other, it generates opportunities for potential abuse. The absence of a unified ethical and legal framework to standardise permissible areas of application and restrict excessive control remains a key challenge. In conclusion, the practical implementation of biometrics may be regarded not merely as a technical or organisational task, but also as a process that reshapes the quality of relations between the individual, the state, and society.

6. Technical and security aspects

The security dimension of biometric technologies represents one of the most complex and, at the same time, least obvious aspects when compared with ethical or legal considerations. While ethical debates often focus on issues of privacy and human autonomy, the technical sphere concerns how to ensure the reliability and durability of systems handling biometric data. In other words, this pertains to the infrastructure of trust: without effective protection measures, any legal norms or ethical protocols remain merely declarative.

Modern methods for protecting biometric templates are grounded in cryptographic techniques, including encryption, hashing, and combinatorial models of multibiometrics [25]. Encryption allows data to be transformed into a form that is unreadable by third parties, with the key retained by the identifying authority. In practice, however, the challenge lies in key management, since the loss or compromise of keys can provide mass access to vulnerable data [26]. Hashing, meanwhile, prevents the recovery of the original biometric characteristics from the template, but simultaneously carries the risk of so-called ‘matching attacks,’ whereby the same hash can be used across different databases to identify an individual.

In Ukraine, this debate has become particularly prominent following the introduction of the Diia system, which actively employs biometric identification to verify identity in public services. The concern is not so much one of functionality as of confidence that protection measures are correctly implemented and will prevent data leaks [27].

Multibiometrics, as a method of integrating several independent parameters (e.g., fingerprint and facial geometry), substantially reduces the risk of system compromise [28]. If a single template is stolen or compromised, it does not automatically provide access to the system, as additional verification using another parameter is required. However, multibiometrics introduces another challenge: it necessitates the creation of more complex databases containing even greater volumes of confidential information. Thus, reducing the risk of hacking at the level of a single technology is accompanied by an increased potential scale of damage in the event of a data breach.

This is the paradox facing modern security engineers: by strengthening the system in one dimension, they render it more vulnerable in another.

The problem of compromising biometric data differs fundamentally from the leakage of passwords or conventional identification keys. While a password can be changed and a card blocked, biometric characteristics are irreversible. Individuals cannot alter their fingerprints or irises, even if such data falls into the hands of malicious actors. In this respect, biometrics imposes an entirely new level of responsibility on database operators and identification systems. As Shoshana Zuboff observes in her work, "biometric technologies do not simply collect information, they make the body an integral component of the digital market" [28]. In other words, the compromise of biometric data effectively constitutes a lifelong risk for an individual who loses control over their own physical uniqueness.

The consequences of such breaches are already evident in practice. For instance, in 2019, it was revealed that the Biostar 2 system, which provided biometric access for numerous European companies, contained serious vulnerabilities, resulting in millions of fingerprints and facial scans being exposed publicly [29; 30]. The experience of this incident prompted international bodies to review data storage and encryption standards. Similarly, in the United States, following the compromise of federal officials' biometric templates in 2015, the government was compelled to develop new security protocols for employees who had lost control over their identifiers [31]. This demonstrates that the issue is neither theoretical nor hypothetical, but carries tangible social and legal consequences.

International trends in the security of biometric systems demonstrate a clear commitment to enhancing resilience through the development of

standards and advanced technological solutions. At the European Union level, the concept of "privacy by design" is being actively implemented, which entails embedding protective mechanisms into the system's architecture from the very stage of its creation [32]. This involves minimising the volume of data collected, distributing storage, and regularly updating encryption algorithms.

In Japan, research is ongoing to integrate biometric technologies with artificial intelligence methods capable of detecting anomalies in real time [33]. Such systems not only identify users but also detect suspicious behavioural patterns or technical malfunctions, thereby enhancing preventive security.

In Germany, emphasis is placed on the importance of establishing independent cybersecurity audit centres, which are tasked with evaluating systems not only prior to deployment but also during their operational use [34]. An example of this is the establishment of the Biometric Evaluation Center, developed in collaboration with the Federal Office for Information Security (BSI) and Bonn-Rhein-Sieg University of Applied Sciences.

Ukraine, in its efforts to integrate into the European digital space, must also consider these approaches, particularly in the context of e-government implementation and the development of national registries [35; 36]. Initiatives such as Diia, Trembita, and the GovTech Alliance UA illustrate the state's commitment to embedding the principles of 'digital trust' and personal data protection at the system architecture level.

The overarching conclusion is that the technical and security aspects of biometrics cannot be considered in isolation from ethical and legal dimensions. Even the most sophisticated technology always carries a human element, and the extent to which developers and legislators are able to integrate innovative solutions with security principles determines trust in the system as a whole. In other words, biometrics is not solely a matter of science and technology, but also a question of the social contract regarding the degree to which we are willing to entrust our own bodies to the digital infrastructure.

7. Biometrics as a societal challenge

The current development of biometric technologies increasingly demonstrates that this is not merely a matter of technical progress or the

optimisation of identification procedures. Biometrics is emerging as a multidimensional societal challenge, raising fundamental questions about the balance between freedom and security, between personal privacy and the needs of the state, and between technological innovation and the preservation of human dignity. In other words, it concerns the formation of a new social contract in the digital age, in which the body and biological characteristics become central to participation in economic, political, and legal relations.

The issue of balancing security and human rights lies at the heart of the current debate on biometrics. On the one hand, the use of biometric technologies considerably enhances the effectiveness of efforts to combat terrorism, fraud, and illegal migration. The experience of the United States following the terrorist attacks of 11 September 2001 has demonstrated convincingly that biometric border control systems have become a crucial component of national security [37].

On the other hand, the intensification of control inevitably leads to restrictions on privacy, creating an atmosphere of pervasive surveillance in which every action of the individual is recorded and analysed. In countries with underdeveloped democratic institutions, such technologies may be employed as instruments of political pressure and social segregation. The Chinese example of the "social credit" system, in which biometric identifiers are integrated into a framework for evaluating citizens' behaviour, raises a critical question for the world: can a security technology become a technology of discipline? [38; 39].

The European tradition of a human-rights-based approach seeks to find a balance between these poles. Within the framework of the General Data Protection Regulation (GDPR) and the Council of Europe's Convention 108+, emphasis is placed on the principle of proportionality: the use of biometrics is permissible only when the objective cannot be achieved by other, less invasive means [15; 40]. However, even this principle does not always prevent misuse. In Ukraine, for example, discussions regarding the implementation of facial recognition video surveillance systems in major cities immediately raised questions about who would have access to the data, under what conditions it would be stored, and how citizens' rights to challenge governmental actions would be ensured [41].

Thus, this balance is not static – it requires continuous review and societal oversight.

In this context, the concept of digital ethics assumes particular significance. Biometrics is not merely a set of technical solutions, but a tool that transforms the way individuals interact with the state and society. As Luciano Floridi notes in his work The Ethics of Information (2013), in the digital age, 'ethical dilemmas unfold not around things, but around flows of information' [42]. Biometric data constitute precisely such flows, serving both as information and as a physical marker of the individual. They form a bridge between the physical and digital realms, and therefore demand careful ethical consideration.

On the one hand, biometrics can enhance human capabilities by providing faster access to services, safeguarding against fraud, and creating a more user-friendly digital environment. On the other hand, it may generate new power asymmetries, whereby technological corporations and state institutions gain excessive control over individuals' lives. This raises the question of trust. If citizens are not confident in the security and fairness of biometric systems, their use is likely to provoke resistance. This can already be observed in numerous European countries, where local communities have protested against the installation of facial recognition cameras in public spaces. In 2020, several French municipalities officially abandoned such projects, citing the protection of civil rights [43]. In particular, the Administrative Court of Marseille ruled that the facial recognition experiment in schools was disproportionate and failed to ensure voluntary consent [44]. Similar debates are occurring in Ukraine, where digital trust in state services is critical for the further development of e-government. In 2025, regulations for building national digital systems were updated, with an emphasis on openness, avoidance of vendor lock-in, and alignment with international ISO/IEEE standards [45]. However, trust is built not only through technical solutions but also through transparency, auditing, and societal dialogue. In other words, biometrics without public dialogue risks becoming a tool of division rather than unity.

Public dialogue in this domain is not only desirable but essential. It should involve not only legal and technological experts but also the general public, who directly experience the consequences of biometric

system implementation. Such discussions can help shape a new framework of responsibility and establish acceptable limits of control. Notably, the experience of Germany, where the establishment of dedicated ethical councils under the government has enabled the inclusion of representatives from academia, industry, civil society, and the media in the development of digital policy, offers a valuable model. This approach could serve as a benchmark for Ukraine, which is currently undergoing large-scale digital transformation.

In conclusion, biometrics as a societal challenge is not merely a matter of technical efficiency or legal compliance. Above all, it represents a challenge for democracy, for the culture of trust, and for society's capacity to negotiate the boundaries of acceptability. Technologies can make our lives safer, but only on the condition that they do not undermine human freedom and dignity. For this reason, the future of biometrics will be determined less by engineering solutions than by our ability to foster an honest and open dialogue about its role in our lives. In other words, the question is not whether to use biometrics, but how to make it a tool for development rather than for control.

8. Conclusions

The final chapter of the study summarises the key findings derived from the analysis of biometric technologies as a multidimensional phenomenon of contemporary society. Biometrics is simultaneously a technical innovation, an identity management tool, and a significant societal challenge that engages the fundamental foundations of legal, ethical, and democratic culture. On the basis of this analysis, several strategically important conclusions can be drawn.

Firstly, the uniqueness and immutability of biometric data create a qualitatively new level of risk. Unlike passwords or access codes, which can be changed in the event of a breach, biometric characteristics are inseparable from the individual. Loss of control over such data entails lifelong vulnerability and generates the potential for abuses on an unprecedented scale. For this reason, biometrics requires a distinct legal framework that differentiates it from ordinary personal data and provides additional security safeguards. This necessitates the development of specialised protocols by legislators that take into account the irreversible nature of such data.

Otherwise, any compromise could give rise to a problem that is impossible to rectify.

Secondly, the ethical risks associated with the use of biometrics pose a serious challenge to democratic societies. Issues of privacy, autonomy, and non-discrimination extend beyond technical considerations and touch upon the fundamental foundations of individual freedom. The widespread implementation of surveillance technologies produces a "chilling effect", whereby citizens alter their behaviour due to the awareness of constant monitoring. This undermines trust in institutions and transforms the culture of public spaces. Democracy without trust is merely a formal shell, and biometrics may become the point at which freedom and control enter their sharpest conflict.

Thirdly, the legal regulation of biometric technologies is today largely shaped by international standards. The General Data Protection Regulation (GDPR), the Council of Europe's Convention 108+, and other instruments serve as benchmarks for national legal systems. They establish a framework in which the principles of proportionality, data minimisation, and protection against excessive interference are central. For Ukraine and other states undergoing digital transformation, compliance with these standards is not only a legal obligation but also a prerequisite for integration into the international community. Where common rules are absent, disorder arises, which invariably benefits the more powerful actor – whether the state or a corporation.

Fourthly, the pursuit of a balance between innovation and human rights is a necessary condition for the development of biometrics. Technologies can significantly enhance security, governance efficiency, and everyday convenience, but their implementation without consideration of value-based principles can alienate individuals from their own corporeality and undermine the concept of human dignity. A flexible approach implies that innovations are neither rejected nor treated as an end in themselves. They are integrated into society only to the extent that they align with democratic principles and a culture of trust. In other words, technology should serve humanity, not the reverse.

Fifthly, the future development of biometric systems is linked to the implementation of multibiometrics, the strengthening of cybersecurity mechanisms, and the establishment of new ethical frameworks.

Multibiometric solutions can reduce the risk of data compromise, but at the same time increase the volume of information that requires more robust protection. Therefore, the future depends not only on technical improvements but also on new models of accountability and transparency. It is crucial to establish mechanisms for continuous auditing and independent oversight of biometric system use, so that society can influence the development of these technologies. Otherwise, innovations risk remaining in the hands of a narrow group of actors who make decisions without regard for the public interest.

Ultimately, the main conclusion is that biometrics is not merely an identification tool, but also a mirror of social processes. It exposes the tension between security and freedom, between innovation and dignity, and between the state and the individual. The future of this technology will depend less on technical solutions than on society's ability to establish rules for coexistence in a world where digital identity becomes an integral part of human existence. Biometrics will neither disappear nor halt its development. Yet we still have the opportunity to determine its trajectory: as a tool of trust and progress, or as a mechanism of control and subordination.

References:

1. Maeko, M. E., van der Haar, D. (2022) A model for biometric selection in public services sector. In: *Artificial Intelligence Research*, pp. 323–334. Springer.

2. Wen, Y., Zhang, L., Kim, H. (2024) Facial recognition technology and the privacy risks. In: *Face De-identification: Safeguarding Identities in the Digital Era*, pp. 15–20. Springer.

3. Wang, X., Lee, J., Kumar, R. (2024) Algorithmic discrimination: Examining its types and regulatory measures. *Frontiers in Artificial Intelligence*, vol. 7. https://doi.org/10.3389/frai.2024.1320277

4. Council of Europe (2018) *Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108), as amended by Protocol CETS No. 223.* Strasbourg: Council of Europe.

5. European Parliament and Council (2016) *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.* Official Journal of the European Union, L 119, 88.

6. Cook, J. (2018) *Biometric security jargon: CER, EER, FRR, FAR.* DZone. https://dzone.com/articles/biometric-security-jargon-cer-eer-frr-far (accessed August 30, 2025).

7. New York University (2023) *Ethics and privacy concerns in biometric authentication: A literature review.* https://ultraviolet.library.nyu.edu/records/exvxc-xqn29/files/exvxc-xqn29.pdf (accessed August 30, 2025).

8. Tambe-Jagtap, S., Patel, R., Singh, A. (2024) The use of biometrics in digital identity: Legal implications for governments. *Biometric Technology Today*, vol. 6. https://biometrictechnologytoday.com/index.php/journal/article/view/4 (accessed August 30, 2025).

9. TrustCloud (2025) *Biometric data protection: Trends and best practices 2025.* https://community.trustcloud.ai/docs/grc-launchpad/grc-101/governance/biometric-data-protection-emerging-technologies-and-privacy-concerns-in-2024/ (accessed August 30, 2025).

10. Hendrickson, L. (2025) *Privacy concerns with biometric data collection.* Identity.com. https://www.identity.com/privacy-concerns-with-biometric-data-collection/ (accessed August 30, 2025).

11. European Commission (2025) *What personal data is considered sensitive?* https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en (accessed August 30, 2025).

12. GDPR (n.d.) *Article 9 – Processing of special categories of personal data.* https://gdpr-info.eu/art-9-gdpr/ (accessed August 30, 2025).

13. Equality and Human Rights Commission (2025) *Met Police's live facial recognition policy is 'unlawful'.* Daily Mail. https://www.dailymail.co.uk/news/article-15018715 (accessed August 30, 2025).

14. Penney, J. (2021) *Understanding chilling effects. Berkman Klein Center*. https://cyber.harvard.edu/story/2021-06/understanding-chilling-effects (accessed August 30, 2025).

15. Information Commissioner's Office (ICO) (2025) *How do we process biometric data lawfully? UK GDPR Guidance.* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/ (accessed August 30, 2025).

16. Valdivia, A., Singh, R., Chen, M. (2021) *Fairness in biometrics.* arXiv.org. https://arxiv.org/pdf/2112.11193 (accessed August 30, 2025).

17. McStay, A. (2020) *Emotional AI, soft biometrics and the surveillance of emotional life.* Big Data & Society. https://journals.sagepub.com/doi/pdf/10.1177/2053951720904386 (accessed August 30, 2025).

18. Barker, D., Nguyen, T., Ali, S. (2025) Ethical considerations in emotion recognition research. *Psychology International*, vol. 7, no. 2, p. 43. https://doi.org/10.3390/psycholint7020043 (accessed August 30, 2025).

19. Turner, J. (2024) BIPA vs. CUBI: Comparative analysis of major biometric privacy acts in Illinois and Texas. *Illinois Business Law Journal.* https://publish.illinois.edu/illinoisblj/2024/08/20/bipa-vs-cubi-comparative-analysis-of-major-biometric-privacy-acts-in-illinois-and-texas/ (accessed August 30, 2025).

20. Gurram, A. (2024) *Biometric (data) governance and digital surveillance: A comparative analysis of biopolitics in India and China.* In: Policing and Intelligence in the Global Big Data Era. Springer. https://link.springer.com/chapter/10.1007/978-3-031-68298-8_11 (accessed August 30, 2025).

21. The Legallo (2024) *Understanding consent challenges in biometric systems*. https://thelegallo.com/consent-challenges-in-biometric-systems/ (accessed August 30, 2025).

22. Troncoso Reigada, A. (2012) The principle of proportionality and the fundamental right to personal data protection: The biometric data processing. *Lex Electronica*, vol. 17, no. 2. https://www.lex-electronica.org/en/s/159 (accessed August 30, 2025).

23. Lagerkvist, A., Nilsson, M., Sundström, P. (2022) *Body stakes: An existential ethics of care in living with biometrics and AI. AI & Society.* https://mau.diva-portal.org/smash/get/diva2:1977576/FULLTEXT01.pdf (accessed August 30, 2025).

24. Buitelaar, J. C. (2017) Post-mortem privacy and informational self-determination. *Ethics and Information Technology,* vol. 19, no. 2, pp. 129–142. https://doi.org/10.1007/s10676-017-9421-9 (accessed August 30, 2025).

25. Sangeetha, P., Revathy, B. (n.d.) Secure multibiometric cryptosystems using biohashing. *International Journal of Engineering Research & Technology.* https://www.ijert.org/research/secure-multibiometric-cryptosystems-using-biohashing-IJERTCONV1IS06047.pdf (accessed August 30, 2025).

26. Tidmarsh, D. (n.d.) *Biometric data risks and how to mitigate them.* Preventive Approach. https://preventiveapproach.com/biometric-data-risks/ (accessed August 30, 2025).

27. Suprun, K., Piskun, A. (2024) *Digital credentials in Diia: The case of Ukraine.* Finnish National Agency for Education. https://www.oph.fi/sites/default/files/documents/2024-05-08%20DS_052024_Kateryna_Suprun_Andrii_Piskun.pdf (accessed August 30, 2025).

28. Zuboff, Sh. (2019) *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* London: Profile Books.

29. Fogden, T. (2019) *Breach exposes biometric data of 2.8 million users.* Tech.co. https://tech.co/news/suprema-biostar-2-leak-2019-08 (accessed August 30,2025).

30. O'Neill, P. H. (2019) *Data leak exposes unchangeable biometric data of over 1 million people*. MIT Technology Review. https://www.technologyreview.com/2019/08/14/133723/data-leak-exposes-unchangeable-biometric-data-of-over-1-million-people/ (accessed August 30, 2025).

31. Khandelwal, S. (2015) *5.6 million federal employees' fingerprints stolen in OPM hack.* The Hacker News. https://thehackernews.com/2015/09/opm-hack-fingerprint.html (accessed August 30, 2025).

32. CORDIS, European Commission (n.d.) *Putting privacy at the heart of biometric systems.* https://cordis.europa.eu/article/id/86916-feature-stories-putting-privacy-at-the-heart-of-biometric-systems (accessed August 30, 2025).

33. Toshiba Global (2021) *Toshiba introduces new anomaly detection AI for large-scale industrial plant*s. https://www.global.toshiba/ww/technology/corporate/rdc/rd/topics/21/2112-01.html (accessed August 30, 2025).

34. B2B Cyber Security (n.d.) *BSI: New biometric evaluation center opened.* https://b2b-cyber-security.de/en/bsi-opened-a-new-biometric-evaluation-center/ (accessed August 30, 2025).

35. VoxUkraine (n.d.) *State digital transformation in Ukraine: 2019–2024 review.* https://voxukraine.org/en/state-digital-transformation-in-ukraine-2019-2024-review (accessed August 30, 2025).

36. Digital State of Ukraine (2025) *Ukraine launches GovTech Alliance*. https://digitalstate.gov.ua/news/govtech/ukraine-launches-govtech-alliance (accessed August 30, 2025).

37. Djanegara, D. T. (2021) *How 9/11 sparked the rise of America's biometrics security empire.* Fast Company. https://www.fastcompany.com/90674661 (accessed August 30, 2025).

38. Hoffman, S. (2017) *Managing the state: Social credit, surveillance and the CCP's plan for China. Jamestown Foundation.* https://jamestown.org/program/managing-the-state-social-credit-surveillance-and-the-ccps-plan-for-china (accessed August 30, 2025).

39. Lin, L. Y.-H., Milhaupt, C. J. (2023) China's corporate social credit system: The dawn of surveillance state capitalism? *The China Quarterly,* no. 256, pp. 835–853. https://doi.org/10.1017/S030574102300067X (accessed August 30, 2025).

40. Information Commissioner's Office (n.d.) *How do we process biometric data lawfully?* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition (accessed August 30, 2025).

41. Laboratoriia tsyfrovoi bezpeky (2023) *How "clear" is the legality of Clearview AI in Ukraine?* https://dslua.org/publications/how-clear-is-the-legality-of-clearview-ai-in-ukraine (accessed August 30, 2025).

42. Floridi, L. (2013) *The ethics of information. Oxford: Oxford University Press.* https://books.google.com/books/about/The_Ethics_of_Information.html?id=_XHcAAAAQBAJ (accessed August 30, 2025).

43. Kayali, L. (2019) *How facial recognition is taking over a French city. Politico.* https://www.politico.eu/article/how-facial-recognition-is-taking-over-a-french-riviera-city (accessed August 30, 2025).

44. Hogan Lovells (2020) *Facial recognition challenged by French administrative court.* https://www.hoganlovells.com/en/publications/facial-recognition-challenged-by-french-administrative-court (accessed August 30, 2025).

45. GovTech Alliance of Ukraine (2025) *No vendor lock-in, full digitalization: Ukraine resets its GovTech rules.* https://digitalstate.gov.ua/news/govtech/ukrayina-onovyla-pravyla-dlia-derzavnykh-tsyfrovykh-system-i-tse-spravzniy-heymchendzer-dlia-govtech (accessed August 30, 2025).