Personal data protection in Ukraine via the prism of european judicial institutions' practise

Personal data protection in Ukraine via the prism of european judicial institutions' practise

Mykola Kotenko
https://orcid.org/0009-0003-8010-7069
Taras Shevchenko National University of Kyiv. Ukraine
E-mail: mykola_kotenko@edu-knu.com

Ruslan Karagioz
https://orcid.org/0000-0002-6753-6155
Odesa State University of Internal Affairs. Ukraine
E-mail: Ruslan-19761@ukr.net

Iryna Sopilko
https://orcid.org/0000-0002-9594-9280
National Aviation University. Ukraine
E-mail: sopilko8182@edu-knu.com

Valerii Andrusiv
https://orcid.org/0009-0004-9464-2094
Kyiv University of Law of the National Academy of Science of Ukraine. Ukraine
E-mail: vgandrusiv@gmail.com

Hanna Yermakova
Interregional Academy of Personnel Management
03039, 2 Frometivska Str., Kyiv. Ukraine
E-mail: yermakova_hanna@neu.com.de

Recepción: 29 de marzo de 2024
Aceptación: 24 de agosto de 2024

DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

Abstract: The current paper intends to examine the issue of information protection, particularly personal data, based on positive international experience, aiming to revise and improve personal information protection provisions in Ukraine. Since conventional norms necessitate the use of the evolutionary interpretation approach in the context of the dynamic development of societal life, the study's materials were international legal regulations and the European Court of Human Rights and the Court of Justice of the European Union case law. Thus, notable cases were examined in order to shed light on the developing comprehension of sensitive data and the need for enhanced security. The analysis of the court practises regarding personal data protection was conducted using a combination of general scientific and specific legal methods, namely dialectical, analytical, formal-dogmatic, comparative-legal, systemic and predictive methods. As a result of the research, key standards for personal data protection were identified, and recommendations for improving Ukrainian legislation, particularly in terms of clarity and certainty, were developed. Recognising potential implementation challenges, the article advocates for ongoing research in this field to refine and strengthen personal data protection mechanisms in Ukraine.
Keywords: personal data protection; European Union practices; sensitive data protection; European Court of Human Rights; European Court of Justice; Ukrainian legislation.

Abstract: The current paper intends to examine the issue of information protection, particularly personal data, based on positive international experience, aiming to revise and improve personal information protection provisions in Ukraine. Since conventional norms necessitate the use of the evolutionary interpretation approach in the context of the dynamic development of societal life, the study's materials were international legal regulations and the European Court of Human Rights and the Court of Justice of the European Union case law. Thus, notable cases were examined in order to shed light on the developing comprehension of sensitive data and the need for enhanced security. The analysis of the court practises regarding personal data protection was conducted using a combination of general scientific and specific legal methods, namely dialectical, analytical, formal-dogmatic, comparative-legal, systemic and predictive methods. As a result of the research, key standards for personal data protection were identified, and recommendations for improving Ukrainian legislation, particularly in terms of clarity and certainty, were developed. Recognising potential implementation challenges, the article advocates for ongoing research in this field to refine and strengthen personal data protection mechanisms in Ukraine.
Keywords: personal data protection; European Union practices; sensitive data protection; European Court of Human Rights; European Court of Justice; Ukrainian legislation.

I. Introduction

In the context of the information society's active development, introducing new, in particular, informational technologies can be viewed as promising for some institutions. The digitalization of the national apparatus's work, reduction of bureaucracy, ensuring transparency in the provision of administrative services and performing other functions of the country with the use of electronic technologies, etc., are examples of such improvements. As Ukraine continues to develop in the information society, the introduction of new information technologies opens up significant opportunities to improve the efficiency of public administration. Digitalization of public administration, reduction of bureaucracy, and increased transparency of administrative services are some of the key benefits expected from these advances. However, along with these improvements, new challenges have emerged. These include increased risks of unauthorized access to personal data by governments and private organizations, increased threats of cyberattacks, and the possibility of foreign organizations obtaining confidential national security information or personal data of Ukrainian citizens.

However, in addition to the benefits mentioned, new problems have arisen, such as increased possibilities for obtaining information about a person, including unauthorised means by governments and private entities, an increase in the risks of cyber-attacks, as a result of which one country can acquire information containing national security secrets or personal data of citizens from another country, etc.

Due to the diversity of information, an extensive framework of informational law sources has been developed to establish the legal regime for its various blocks (Commission declaration, 2009; European Declaration, 2022; Recommendation, 2012). As an instance, the use and protection of public information, such as data obtained during the performance of governmental powers by entities or other information under their control, are regulated by the Law of Ukraine "On Access to Public Information" (2011). At the same time, information pertaining to science, technology, and production is recognised as a key subject of regulation under the special Law of Ukraine "On Scientific and Technical Information" (1993). Similarly, specific regulation has been applied to issues related to the use, provision of access to, and protection of personal information – at the level of the Law of Ukraine "On Personal Data Protection" (2010). These attests, on the one hand, to the specificity of relations governed by this law, aimed at ensuring the individual's right to non-interference in private life, and on the other hand, emphasises the fundamental importance for each subject of the matter of protecting their personal data.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

Individual international legal norms attest to the critical importance of private information protection at the global scale, particularly within the European community. For the first time at the international legal level, in 1948, Article 12 of the Universal Declaration of Human Rights recognised the right of everyone to privacy (Melnyk, 2013). To ensure this right, the government must fulfil its duties by: creating the necessary conditions to prevent unlawful and unjustified interference in private life by both private entities, responding appropriately to violations of the right to respect for private and family life, and investigating instances of such unauthorised interference. The listed duties apply to governments and public entities in the country (Universal Declaration of Human Rights, 1948). Those norms laid the foundation for promoting the right to privacy, an essential element of which is personal data security. Today, the right to personal information protection should be considered a component of the right to respect for private, family life, home, and correspondence guaranteed by Article 8 of the European Convention on Human Rights (1950). Since conventional norms necessitate the application of the evolutionary interpretation approach in the context of the dynamic development of societal life, including information relations, the European Court of Human Rights (hereinafter – ECtHR) plays an exceptional role in shaping and revising European standards for personal data protection. The Strasbourg Court has established consistent legal positions on the protection of individuals from unjustified and prolonged retention of personal data by a country`s authorities (e.g., the ECtHR decision in the case of "S. and Marper v. The United Kingdom", Nos. 30562/04 and 30566/04, dated December 4, 2008 (ECHR Decision, 2008)). In addition, the ECtHR has repeatedly examined the relationship between the right to privacy and the use of various forms of surveillance on individuals (e.g., the ECtHR decision in the case of "Uzun v. Germany", No. 35623/05, dated September 2, 2010 (ECHR Decision, 2010)).

A distinct layer of the ECtHRs' jurisprudence has developed the concept of "sensitive" personal data. This term encompasses the part of an individual's information that, if disclosed or negligently stored, has the potential to cause significant harm to a person. Consequently, such information necessitates extra security precautions by the country or other authorized entities. This is demonstrated, for example, by the ECtHR decision in the case of Aycaguer v. France, Case No. 8806/12, dated June 22, 2017 (ECHR Decision, 2017), and the case of Catt v. United Kingdom, Case No. 43514/15, issued on January 24, 2019 (ECHR Decision, 2019).

Article 15 of the Association Agreement between Ukraine and the European Union (hereinafter – EU) requires Ukraine to incorporate the best Euro-

pean and international standards for personal data protection into its national legal system (Association Agreement, 2014). Given the growing interaction between national economic entities and European participants in civil turnover against the backdrop of European integration in Ukraine, this requirement is entirely logical and justified. The EU is committed to protecting its citizens and residents within and outside its borders. The right to privacy is fundamental in EU legislation. Personal data protection is included in the system of fundamental rights under Article 8 of the EU Charter of Fundamental Rights (hereinafter – the Charter) (Charter, 2009). In this context, the Court of Justice of the European Union (hereinafter – CJEU; European Court of Justice) has considered the issue of personal information protection according to the EU law principles. The case "Volker and Markus Schek", in which the CJEU concluded that the requirement to disclose personal information about each individual who received assistance from funds, including details about the period, frequency, and amount of such assistance, does not meet the criterion of proportionality in restricting individuals' right to protect their personal data (Decision, 2010), is an example of this.

Summarizing the foregoing, the relevance of present research is determined by the following factors: a) the development of the information society, in which information, including personal data, is recognised as a distinct value and subject to legal regulation and protection; b) the appearance of new information technologies that expand the possibilities of obtaining information, including unauthorized means; c) recodification processes in the civil legislation of Ukraine allow for the possibility of revising and improving provisions on the protection of information, including personal data, based on positive foreign experience; d) a significant number of violations of the right to respect for private life guaranteed by Article 8 of the the European Convention on Human Rights, one of which is personal data protection, in Ukraine; e) the Eurointegration processes in Ukraine necessitated an examination of European standards for personal data protection as reflected in ECtHR and CJEU case law; f) due to the high dynamism of information technology, particularly in the processing and preservation of personal data, judicial practise is an especially useful source of legal regulation, as it evolves more rapidly in response to new societal challenges and standards than legislation and international treaties.

This sets the following objectives: to examine the ECtHR and the CJEU case law in terms of personal data protection; to clarify the state of legal provision and legal enforcement regarding personal data protection in Ukraine; identify its major shortcomings in light of the standards established in European judicial case law; and determine how Ukraine can improve its legal provisions and law enforcement practices on personal data protection to be in

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

line with European standards, in particular those set by the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union.

II. Materials and Methods

Hence, the current paper intends to examine the issue of information protection, including personal data, based on positive international experience, with the aim of revising and improving information protection provisions in Ukraine.

Since conventional norms necessitate the use of the evolutionary interpretation approach in the context of the dynamic development of societal life, including information relations, the study's materials were international legal regulations and also ECtHR and CJEU case law. The analysis of the ECtHR practises is crucial in this research especially due to specific decisions of the ECtHR and the Court of Justice of the EU, as well as key legal positions of these European courts, allowed for the identification of European standards for personal data protection and the formulation of proposals to Ukrainian legislators on their basis.

The analysis of the ECtHR and CJEU practises regarding personal data protection was performed on the basis of a methodological foundation that presented as a combination of both general scientific and specific legal methods of scientific cognition, namely:

The dialectical method was used to analyze the interaction and differences between European and Ukrainian personal data protection mechanisms. This method helped understand the broader context in which data protection laws operated, highlighting connections and disagreements that may facilitate personal data protection.

The analytical method was used to examine specific legal positions of the ECtHR and the CJEU regarding the issue of protecting personal data, as well as domestic legal provisions and legal enforcement practices in this field. Examining specific legal positions and national legislative provisions, the specifics of data protection mechanisms with the European legal space were assessed with a view of implementing best practices in the Ukrainian context.

The formal-dogmatic method was implemented to study the content of specific legal norms governing personal data protection in Ukraine and the EU. The comparative-legal method was employed to compare national legal provision and legal enforcement practises with the ones of European judicial institutions in the field of personal data protection, identifying shortcomings at the national level in the legal provision and data protection.

The systemic method allowed the organisation of a vast array of the ECtHR and CJEU case law on personal data protection by key problematic issues. The predictive method was employed to develop proposals for improving national legal framework of Ukraine for personal data protection in accordance with European standards in this area.

III. Results and discussion

1. European regulations for personal data protection

The history of the development of personal data protection legislation and case law in Europe is closely linked to the growing importance of privacy and personal rights in the context of digitalization and globalization. The origin of the idea of personal data protection can be traced back to the 1970s, when the first European countries, such as Germany and Sweden, began to adopt laws on personal information protection.

Gradually, with the development of information technology, these issues have become particularly relevant. In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which laid the foundation for the further development of European legislation in this area. This document was the first international treaty to establish common standards for the protection of personal data.

Based on Convention 108 and taking into account further technological changes, in 1995 the EU adopted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This directive became the basis for national laws of the EU member states, in particular, it required compliance with the principles of lawfulness, fairness and transparency in the processing of personal data.

The most significant milestone was the adoption of the General Data Protection Regulation (GDPR) in 2016, which entered into force in 2018. The GDPR was a response to the challenges posed by globalization and digitalization and established new, stricter data protection standards that must be met not only in the EU but also outside of it if the data of EU citizens are processed.

Article 16 of the Treaty on the Functioning of the European Union empowers the European Parliament and the Council, as regional legislative bodies, to formulate standards of protection the private entities' personal data. Furthermore, the mentioned Treaty allows the establishment of not only rec-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

ommendatory but also mandatory acts in this sphere, which are obligatory for compliance by all EU member countries without the need for separate consent from each country. Rules for the protection of individuals in the processing of their personal data by EU institutions, bodies, offices, and agencies, as well as by member countries during activities within the scope of EU legislation, are established following the ordinary legislative procedure, along with regulations regarding the free movements of such data. Compliance with these rules is monitored by independent authorities (Consolidated versions, 1992). In this regard, it may be beneficial to provide a brief overview and define the functional purpose of each of the specialised sources of legal protection for personal information protection in the EU, some of which have global significance as international agreements while others have been developed in accordance with Article 16 of the Treaty on the Functioning of the European Union and serve a purely regional purpose (Korniienko et al., 2020).

The occurrence of opportunities for cross-border personal information processing compelled countries to collaborate and establish collective international rules for the protection of personal data in a cross-border context. As a result, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (hereinafter – CETS No. 108) was established. This international treaty was ratified in order to ensure consistent and high-quality conditions for protecting each individual's right to privacy during the processing of their personal information across every participating jurisdiction (Convention, 1981).

European personal data protection standards, in particular those set by the GDPR, are based on several key principles, such as legality, transparency, data minimization, and accountability. These principles reflect the desire to ensure a high level of protection of individuals' privacy and data in response to the challenges posed by the development of technology. Fundamental principles for ensuring personal information protection were defined at the level of CETS No. 108's general provisions, and were later incorporated into the national legislation of most European countries, including Ukraine. Among these general principles, the following should be specified:

a) the principle of lawfulness and fairness in personal data collection and processing;
b) the legality and clarity of the purpose for storing personal information;
c) the sufficiency and proportionality of measures for storing and/or processing personal data;
d) the accuracy of the obtained personal information and the ability to review and update it at reasonable intervals;

e) the storing and displaying format of the personal information should allow subjects to be identified for no longer than the time required to satisfy the legitimate motive of processing personal data.

Furthermore, while CETS No. 108 does not explicitly use the term "sensitive data", it prohibits processing the "special categories of data" in the absence of adequate legal guarantees in national legislation. These are pieces of information which disclosure or careless storage may have particularly negative consequences for the data subject. Such information could pertain to a person's health, genetic information, religious beliefs, or circumstances surrounding criminal proceedings against them. In Ukrainian legislation, the "sensitive data" concept is legally regulated under Article 7 "On the Protection of Personal Data". Specific mechanisms for enhanced protection, such as increased legal liability for their disclosure or careless storage, are not provided in Ukrainian legislation, which may be considered a shortcoming.

Within the EU, the provisions of CETS No. 108 were continued in Directive 95/46/EC of October 24, 1995 (hereinafter – Data Protection Directive). The adoption of the Data Protection Directive was prompted by the challenge of disparate national standards and legislative approaches to personal information processing in various European countries, which resulted in inconvenient differentiation in data protection legal regulation as cross-border use of such data increased. This regional international act aims to establish a uniformly high level of protection for individuals across all European countries when it comes to the processing of their personal information. This uniformity is expected to be achieved through the full harmonisation of national legislative rules in this area. The importance of the Data Protection Directive was highlighted by the CJEU (ECJ Decision, 2011).

The Regulation of the European Parliament and the Council (EU) 2016/679 (hereinafter – General Regulation; GDPR) of April 27, 2016, on the protection of physical subjects concerning the processing of personal data and the free movement of such data (Regulation, 2016) is the next significant source of European law in the field of personal data. Cross-border exchange of personal data is unavoidable as a result of globalisation processes in the economy and politics aimed at expanding international trade and cooperation. However, according to Article 110 of the General Regulation, if personal data is transferred from the Union to third countries, the level of protection for individuals ensured by this Regulation in the Union should not be weakened. Thus, the implementation of the provisions of this EU legislative act in Ukraine is not only required for successful European integration but also to support commercial relations with EU countries. Unlike the previ-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

ous Data Protection Directive, the General Regulation establishes more stringent "game rules". The minimum amount of the fine set by Article 83 of the General Regulation on the protection of personal data, in particular, reaches 10,000,000 euros.

2. European experience in personal data protection

The analysis of established ECtHR practices is of special importance in our study. This is due to a significant number of cases reviewed by the Strasbourg Court concerning violations of Article 8 of the European Convention on Human Rights during the processing of personal information, unauthorised access to it by private entities, abuse of authority by country`s officials regarding access to the personal data of citizens, foreigners, and others (Granada Ministerial Declaration, 2010).

If we summarise the content of the EU courts and the ECtHR practise in the area of personal information protection, we can conclude that the entire ECtHR practice is based on the "three-part test" of the lawfulness of interference with personal data, specifically: compliance with the law, pursuit of legitimate objectives, and the usage of proportionate means. Generally, the history of the ECtHR's practise regarding personal data protection began with the court's decision following the substantive consideration of the case "Leander v. Sweden". The ECtHR drew the attention of European Convention on Human Rights participants, for the first time, in this decision, to the fact that disclosure of personal life information by representatives of a country's authorities, in the absence of a legal basis or legitimate purpose (or both elements simultaneously), may constitute a violation of Article 8 of the European Convention on Human Rights (Decision, 1987). Then, in its decision in "Amann v. Switzerland", the Strasbourg Court defined personal data as "information about an individual's private life that should be interpreted dynamically in light of the specific circumstances of the case and the principles of social life in a particular country" (Decision, 2000).

A distinct aspect of the ECtHR's practice is devoted to the issues of personal data protection in law enforcement activities, particularly the collection and storage of personal information in national registers (Recommendation, 1997). The Strasbourg Court has repeatedly emphasised the importance of adequate safeguards in national law to prevent the use of personal information inconsistent with international guarantees (ECtHR Decision, 1997). We believe that when automated processing involves personal data while performing police duties, officials may abuse their positions to obtain involuntary consent from the data subject, engage in unauthorised access to personal information,

etc. Hence, we fully agree with the ECtHR's conclusion in the case "Gardel v. France", which emphasised that legislation at the national level should function as a layer against the abuse of access to personal information (ECtHR Decision, 2009). Concurrently, the Strasbourg Court affirmed the admissibility of including personal information, including "sensitive data," in the state register of individuals convicted of crimes against sexual freedom in the same case. Given this ECtHR precedent, we consider the passage of Ukrainian Law No. 409-IX on December 19, 2019, creating a Unified Register of Persons Convicted of Crimes Against Sexual Freedom and Sexual Integrity of Minors, to be entirely permissible ("On Amendments…", 2020).

At the same time, when entering data into national databases, it is critical to consider the ECtHR's practice regarding the unjustified use of personal information. According to the decision of the Strasbourg Court in the case "Khelili v. Switzerland," police officers discovered a business card with a phone number and an ambiguous note during a raid: "A lovely woman, a little over thirty years old, looking for a man for occasional meetings". The police used this single business card to enter information about the applicant as a prostitute. While retaining personal information due to the high probability that the person is involved in criminal activity may be justified and proportionate when the allegations are not supported by sufficient evidence, are not legally defined, and are too general, such interference with a person's private life has no legitimate purpose and is not proportionate (ECtHR Decision, 2011). The European Court of Human Rights reached a similar conclusion in the case "S. and Marper v. the United Kingdom", where the application concerned violations of Articles 8 and 14 of the European Convention on Human Rights by law enforcement agencies. Despite the court's approval of two applicants, the police kept their biometric data, including DNA profiles containing an unusual amount of genetic information. According to the legislation at the time, this retention could occur indefinitely for the purpose of further identifying criminals, pursuing the legitimate purpose of detecting and preventing crimes (ECtHR Decision, 2008a).

In this case, the ECHR also classified the personal data, including biometric data, of minors as "sensitive data", the dissemination and negligent storage of which can cause particular harm due to the vulnerability of the data subject, who is on the path of social integration and personal development. The ECHR's unanimous decision in this case regarding the violation of Article 8 of the European Convention on Human Rights was also based on the "vague" formulation of law enforcement agencies' powers regarding the use and indefinite retention of suspects' personal data, regardless of the nature and severity of the offence.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

A dedicated part of the Court of Justice's practise, particularly its decision in the case "Gubert v. Germany", addresses the issues of the government maintaining registers with personal information about its citizens or foreigners through the lens of protecting the right to respect for private life. In this case, the applicant requested that his personal information be removed from the national database of citizens of foreign European countries who stayed in the territory of the FRG for more than three months. The main reason for keeping this register was to aid in statistical, law enforcement, and judicial activities. According to the CJEU, Article 7 (e) of Directive 95/46/EC requires the national authorities to process personal data solely on legal grounds in the interest of society. Furthermore, in ruling on this case, the EU Court emphasised the need for all EU countries to develop a unified concept of the necessity of intervention in personal data. This concept has autonomous significance throughout the EU territory and is based on the Data Protection Directive's overarching purpose, as stated in Article 1 (Derective, 1995)).

The Court of Justice emphasised the possibility of restricting an individual's right to free movement within an EU member country, a provision granted to the member countries by the Treaty on the Functioning of the European Union. As a result, when establishing a national register of information on foreigners' residence (stay), authorities should only use personal information to the extent justified by the legitimate purpose of granting them such powers at the official level. Only by complying with such requirements will the administration of those registers and databases be able to meet EU standards in this area. Otherwise, retaining personal information in specified statistical registers would not satisfy the necessity criterion (ECtHR Decision, 1997b).

In the case of "Guber v. Germany", the applicant drew attention to the purpose of keeping a centralised data register for foreigners - preventing crime on the territory of the Federal Republic of Germany (FRG). The court agreed that accomplishing this purpose requires effective pre-trial investigation and judicial review of criminal offences committed by citizens of any country, including German citizens. In this regard, there are grounds to believe that, in this case, the collection and processing of personal information solely for foreigners, considering the lack of a comparable database for FRG citizens, contains obvious signs of nationality discrimination, which is unacceptable under EU standards (ECtHR Decision, 1997b).

Finding a fair balance between respect for private and family life and the freedom of expression guaranteed by Article 10 of the European Convention on Human Rights is an important task that the ECtHR faces in addressing the issue of personal data protection. The Strasbourg Court has developed criteria for determining the priority of freedom of expression over respect for private

life over the years. These criteria, according to the ECtHR's conclusions in cases such as "Von Hannover v. Germany" (ECtHR Decision, 2004) and "Axel Springer AG v. Germany" (ECtHR Decision, 2012), include:

- the existence of public debate in which personal data about an individual is used to support such discourse;
- individuals` publicity and the content of publications about them;
- the individual's actions prior to acquiring and disseminating their personal information;
- the method of collecting information;
- the publication's format, content, and consequences;
- the rigour of the resulting responsibility.

A separate category of decisions made by European judicial institutions is dedicated to the issue of obtaining voluntary consent for processing personal data. In European law, consent characteristics are primarily defined in Article 5(2) of the Amended CETS No. 108. Specific provisions related to the granting of consent for personal information processing are also addressed in the Committee of Ministers Recommendation CM/Rec(2010)13 to member countries on the protection of individuals concerning automatic personal data processing in the context of profiling, dated November 23, 2010, and also in Articles 4, 6, 7, 8, and 9 of the General Data Protection Regulation. Following these documents, consent must be voluntary, informed, specific, and unambiguous. The CJEU has a compelling practice regarding the necessity of renewing previously obtained consent. For instance, in the case of "Deutsche Telekom AG", the EU Court considered the issue of renewing a subject's consent to processing their personal information. In this case, the CJEU recognised the relevance and validity of the consent to the processing of personal data as an additional characteristic. In the case of a change in at least one of the conditions of processing (a data recipient or the scope of the personal data being processed change), consent is required to be renewed to inform the provider of personal information about the new processing conditions (ECJ Decision, 2011).

Additionally, the modern concept of personal data protection incorporates the right to be forgotten, which has already been considered by the ECHR and the Court of Justice in a number of cases (Obukhovska). The right to be forgotten is primarily exercised on the Internet by contacting an online platform and requesting that specific information or accounts be removed from search engines if the information is outdated, inaccurate or no longer relevant. The implementation of the right to be forgotten, which is situated at the

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

"crossroads" of two fundamental rights (the right to privacy and the freedom of expression), was thoroughly examined by the Court of Justice of the European Union in the cases of "Google Spain SL, Google Inc. v Agencia Española de Protecciónde Datos, Mario Costeja González" (ECJ Decision, 2014) and "Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés" (CNIL) (ECJ Decision, 2019).

3. European personal data protection experience and the possibilities for Ukrainian legislation improvement

Today, personal data protection in Ukraine is one of the most pressing areas requiring significant attention from both legislators and law enforcement agencies. The state of legislation and judicial practice in this area reflects both achievements and certain shortcomings in the implementation of European personal data protection standards.

In Ukraine, personal data protection is regulated by a set of laws and regulations, as well as practical measures aimed at ensuring the confidentiality and security of personal information. The national data protection legislation of Ukraine is based on several key acts. The most important is the Law of Ukraine "On Personal Data Protection" (2010), which defines the rules for processing personal data, the rights of data subjects and the obligations of data processors. This law was an important step in creating a legal environment for the protection of personal information. In addition, the Law of Ukraine "On Electronic Trust Services" (2017), which regulates the issues of electronic signatures, seals and other electronic trust services that also affect data protection. The Law of Ukraine "On Cybersecurity" (2017) complements the regulation in this area, covering electronic signatures and general cybersecurity.

However, given the constant development of technology and growing threats, there are certain shortcomings in Ukrainian legislation that require attention. First, despite efforts to harmonize with international standards, Ukrainian regulations do not always meet the most up-to-date requirements of the European Union, in particular the General Data Protection Regulation (GDPR). This can create legal uncertainties for companies operating internationally. As of 2024, Ukraine has not yet fully implemented all the provisions of the GDPR, although certain steps have already been taken in this direction. For example, the Law of Ukraine "On Personal Data Protection" was amended to expand the rights of data subjects and oblige data controllers to ensure transparency in their processing. At the same time, Ukrainian legislation does not yet contain such important concepts as "confidential data" and

does not regulate some specific aspects, such as the processing of children's data or data transfers abroad.

Secondly, the lack of clarity of certain definitions and procedures in the legislation may complicate its practical application. The case law in Ukraine in the area of personal data protection is still being formed and is characterized by a lack of uniformity. National courts often rely on international standards, but there are not enough precedents that would clearly establish mechanisms for personal data protection in accordance with European standards. Problems with the implementation and enforcement of regulations, as well as irregular application of law enforcement practice, reduce the effectiveness of data protection

Thirdly, the need to constantly update legislation to meet rapid technological changes and new threats is a significant challenge.

Thus, although Ukraine has made important steps in the field of personal data protection, there are still many aspects that need to be improved to achieve a level of protection that meets international standards. One of them is the need to improve the mechanisms for monitoring compliance with the law, including enhancing the role of the Ukrainian Parliament Commissioner for Human Rights. In addition, the principles and standards laid down in the practice of European judicial institutions should be more actively implemented to ensure an adequate level of personal data protection.

In the context of European integration, Ukrainian legal scholars, such as Bem et al. (2015), Golovin et al. (2022), Kovalova et al. (2019), Melnyk et al. (2014), Onishchenko, Rogova (2011), Smokov et al. (2022), Tyshchenko, Yesimov (2013) etc., and Ukrainian society as a whole agree on the critical importance of adhering to Article 17 of Ukraine's Law titled "On the Execution of Decisions and the Application of the European Court of Human Rights Practise" (2006), which officially recognises the ECtHR's practise as a legitimate source of law in Ukraine. Consequently, a thorough examination of the established practices of the ECtHR can be recognized as imperative. Specifically, the analysis of distinct decisions provided by the ECtHR and the CJEU and the pivotal legal stances articulated by these European judicial entities allow the formulation of recommendations for Ukrainian legislators.

Considering the above, analysis of the ECtHR and the CJEU decisions was conducted and key legal positions of these European judicial bodies were defined and proposals for the Ukrainian legislator was formulated in this paper. These results have been organised in Table 1 for ease of comprehension.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

Table 1. The European Court of Human Rights and the European Union's Court of Justice decisions and opportunities for improving Ukrainian legislation

European Court of Human Rights and the Court of Justice of the European Union decisions	The content of the practise	Ways to improve personal data protection mechanism in Ukraine
The ECtHR decision in the case Aycaguer v. France No. 8806/12 dated June 22, 2017 (ECHR Decision, 2017), Catt v. United Kingdom No. 43514/15 dated January 24, 2019, Decision of the ECJ, C-101/01 "Bodil Lindqvist" dated November 6, 2003, S. & Marper v. United Kingdom dated December 4, 2008.	Those decisions establish a distinction between "sensitive" and "non-sensitive data", examine the legal basis for processing sensitive data and emphasise that violations of sensitive data integrity should result in increased liability. This is due to the fact that their security is more stringent, and the consequences of their dissemination are more dangerous and harmful to the data subject.	– to provide a legal definition of "sensitive data" as a type of personal data whose processing, storage, or dissemination causes a high risk to the data subject. therefore, a special regime of confidentiality and enhanced protection from both the country and authorised entities is required; – the list of sensitive data in the legislation of Ukraine needs to be expanded (including personal data of minors, conducting administrative offence proceedings against an individual, etc.), and a non-exhaustive list of the main types of sensitive data needs to be established. This would allow law enforcement authorities to classify certain personal data as sensitive based on the specific circumstances of each case within the limits of the discretion provided; – the increasing of administrative fines for the dissemination of sensitive data;

		– it is necessary to legislate the requirement for enhanced protection of information containing sensitive personal data. An example could be the employer storing such information in a safe in sealed envelopes or on electronic media with enhanced protection against information leakage, accessible only to a limited number of individuals (only those employees required to process sensitive data according to their direct official (labour) duties).
The ECtHR decision in the cases of "Fushman v. Germany" dated October 19, 2017, "Von Hannover v. Germany" dated June 24, 2004, and "Axel Springer AG v. Germany" dated February 7, 2012.	To effectively protect personal data, it is necessary to find a balance between the right to privacy and the freedom of expression in each case.	– to avoid ambiguous and contradictory practises by national judicial authorities on this subject, it is necessary to establish general criteria for balancing the right to respect for private life and the right to freedom of expression in a special law: 1) the existence of public debate in which personal data about an individual is used to support such discourse; 2) individuals` publicity and the content of publications about them; 3) the individual's actions prior to acquiring and disseminating their personal information; 4) the publication's form, content, and consequences; 5) the rigour of the resulting responsibility.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

The CJEU decision in the case of C-131/12, "Google Spain v. AEPD and Mario Costeja González" dated May 13, 2014, and case C-507/17, "Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés" (CNIL), dated September 24, 2019.	Regarding the right to be forgotten through the removal of information from internet search engines.	– it is necessary to establish a mechanism for implementing the right to be forgotten on the Internet at the level of a separate Article in a special law, taking into account a number of aspects, including the form and addressee of the request for information removal. It should also govern the various options that consider requests, such as administrative and judicial procedures, with or without the involvement of the country`s authorities; – it is necessary to establish the main criteria to be considered for the fulfilment of a "right to be forgotten" request (the outdated or irrelevant nature of the information, the inaccuracy of the data, the low degree of societal significance of the relevant information, and the non-public nature of the subject, etc.).

Thus, there is an urgent need for a legal definition of "sensitive data", and an expansion of the list of such data and in other improvements of Ukrainian legislation to introduce clarity and certainty. Addressing these issues will contribute to improving the protection of citizens' privacy. It is also clear that certain aspects of our proposal may pose challenges in practice due to a wide range of circumstances, indicating the need for further research in this area.

IV. Conclusions

A summary of the practices of the CJEU and the ECtHR regarding the protection of personal data leads to the conclusion that the entire jurisprudence of the ECtHR in this area emphasises the importance of adhering to the "three-part test" of the legitimacy of interference with personal data: 1) in accordance with the law; 2) in pursuit of a legitimate purpose; 3) by proportionate means. Additionally, it has been identified that European judicial instances

adhere to the following key standards of personal data protection in their decisions, which should be implemented into Ukrainian legislation:

- establish specific legitimate purposes for processing personal information, ensuring compliance with the lawfulness principle;
- enhance the legal definition of the "personal data" concept in accordance with the General Data Protection Regulation;
- formulate at the level of a separate norm of the principles for the protection of personal data based on the practices of European judicial institutions;
- establish a legal basis and regulation of each operation with personal information at the level of special legislation and regulations, following the principle of the rule of law, including the formal expression of a qualitative law for the legal processing of personal data;
- the country should only use adequate measures for the processing and protecting personal data that are proportionate to their legitimate purpose. In particular, the duration of operations involving personal information should not exceed the reasonable time required to achieve the legitimate purposes of such operations;
- establish, at the national legislative level, the option to review the relevance of personal data on a regular basis and, if necessary, lawfully update them at the request of the data subject;
- the concept of "sensitive data" necessitates separate special regulations for their protection due to the potential increased harm from their dissemination or negligent storage. At the same time, it is essential to remember that the risk of harm resulting from the processing of such information is determined not by its content but by the context in which it is used;
- confirm the priority of personal data protection over the subject's interest in providing services.

V. References

"On Access to Public Information". (2011). Verkhovna Rada of Ukraine. Law No. 2939-VI dated January 13, 2011. Verkhovna Rada of Ukraine Gazette (VVR), 2011, No. 32, Art. 314. https://zakon.rada.gov.ua/laws/show/2939-17#Text

"On Amendments to Certain Legislative Acts of Ukraine Regarding the Introduction of a Unified Register of Persons Convicted of Crimes against

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

Sexual Freedom and Sexual Integrity of a Minor, and Strengthening Responsibility for Crimes Committed against Sexual Freedom and Sexual Integrity of a Minor". (2020). Law of Ukraine No. 409-IX of December 19, 2019. *Information of the Verkhovna Rada (VVR), 27*(175). https://zakon.rada.gov.ua/laws/show/409-20#Text

"On Protection of Personal Data". (2010). Verkhovna Rada of Ukraine. Law No. 2297-VI dated June 1, 2010. Verkhovna Rada of Ukraine Gazette (VVR), 2010, No. 34, Art. 481. https://zakon.rada.gov.ua/laws/show/2297-17#Text

"On Scientific and Technical Information". (1993). Verkhovna Rada of Ukraine. Law No. 3322-XII dated June 25, 1993. Verkhovna Rada of Ukraine Gazette (VVR), 1993, No. 33, Art. 345. https://zakon.rada.gov.ua/laws/show/3322-12#Tex

"On the Implementation of Decisions and Application of the Practice of the European Court of Human Rights". (2006, February 23). No. 3477-IV. Information of the Verkhovna Rada of Ukraine (VVR), 2006, No. 30, Art. 260. URL: https://zakon.rada.gov.ua/laws/show/3477-15#Text

Association Agreement between Ukraine and the European Union. (2014, June 27). URL: https://zakon.rada.gov.ua/laws/show/984_011#Text

Bem, M.V., Gorodinsky, I.M., Sutton, G., & Rodionenko, O.M. (2015). *Protection of Personal Data: Legal Regulation and Practical Aspects: Scientific and Practical Guide*. Kyiv: K.I.S. http://er.ucu.edu.ua/bitstream/handle/1/449/Protection%20of%20personal%20data.pdf?sequence=1&isAllowed=y

Charter of Fundamental Rights of the European Union. (2009, December 1). URL: https://ccl.org.ua/posts/2021/11/hartiya-osnovnyh-prav-yevropejskogo-soyuzu/

Commission declaration on net neutrality. (2009). 2009/C 308/02. Official Journal of the European Union. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:308:0002:0002:EN:PDF

Consolidated versions of the Treaty on European Union. (1992, February 7). https://zakon.rada.gov.ua/laws/show/994_b06#Text

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (1981, January 28). Council of Europe Convention. Strasbourg. https://zakon.rada.gov.ua/laws/show/994_326#Text

Decision of the Amann v. Switzerland, App. No. 27798/95. Judgment of February 16, 2000. (2000, February 16). https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22Amann%20v.%20Switzerland%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58497%22]}

Decision of the European Court of Justice in the joint cases C-92/09 and C-93/09, 'Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen' dated 9 November 2010. (2010, November 9). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092

Decision of the Leander v. Sweden, [1987] 9 EHRR 433. App. No. 9248/81, Judgment of March 26, 1987. (1987, March 26). URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}

Directive 95/46/EC of the European Parliament and of the Council. (1995, October 24). "On the protection of individuals with regard to the processing of personal data and on the free movement of such data" (Data Protection Directive). https://zakon.rada.gov.ua/laws/show/994_242#Text

ECHR Decision in the case of Aycaguer v. France [8806/12]. (2017, June 22). file:///C:/Users/C%D0%BD%D0%B8%D0%B6%D0%B0%D0%BD%D0%B0/Downloads/CASE%20OF%20AYCAGUER%20v.%20FRANCE%20(1).pdf

ECHR Decision in the case of Catt v. United Kingdom [43514/15]. (2019, January 24). URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-189424%22]}

ECHR Decision in the case of S. and Marper v. the United Kingdom [30562/04]. (2008, December 4). http://www.bailii.org/eu/cases/ECHR/2008/1581.html

ECHR Decision in the case of Uzun v. Germany [35623/05]. (2010, September 2). URL: https://ips.ligazakon.net/document/ES005935

ECJ Decision, C-131/12, "Google Spain v. AEPD and Mario Costeja González" dated May 13, 2014. (2014, May 13). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131

ECJ Decision, C-507/17, "Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)" dated September 24, 2019. (2019, September 24). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0507&qid=1698510544598

ECJ Decision, C-524/06, "Huber v. Germany" (Huber v. Germany) dated December 16, 2008. (2008b, December 16).

ECJ Decision, C-543/09, "Deutsche Telekom AG v. Germany" (Deutsche Telekom AG v. Germany), dated May 5, 2011. (2011, May 5).

ECJ Decision, joined cases C-468/10 and C-469/10. (2011, November 24). "National Association of Credit Financial Institutions (ASNEF) and

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

Electronic Commerce and Direct Marketing Federation (FECEMD) v. State Administration" (Asociacion Nacional de Establecimientos Financieros de Credito (ASNEF) and Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado)", paragraphs 28–290.

ECtHR Decision in the case of "Axel Springer Ag v. Germany", application No. 39954/08, dated February 7, 2012. (2012, February 7). https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-109034%22]}

ECtHR Decision in the case of "Khelili v. Switzerland", No. 16188/07, dated October 18, 2011. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-107032%22]}

ECtHR Decision in the case of "S. and Marper v. the United Kingdom", application No. 30562/04, dated December 4, 2008. (2008a, December 4). https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-117816%22]}

ECtHR Decision in the case of "Von Hannover v. Germany", application No. 59320/00, dated June 24, 2004. (2004, June 24). https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-61853%22]}

ECtHR Decision of December 17, 2009, in the case of "Gardel v. France", application No. 16428/05. (2009, December 17). https://hudoc.echr.coe.int/tkp197/view.asp#{%22fulltext%22:[%22\%22Gardel%20v.%20France\%22%22],%22itemid%22:[%22001-96457%22]}

ECtHR Decision of February 25, 1997, in the case of "Z v. Finland", application No. 22009/93. http://medicallaw.org.ua/fileadmin/user_upload/pdf/Z_against_Finland.pdf

European Convention on Human Rights. (1950). https://zakon.rada.gov.ua/laws/show/995_004#Text

European Declaration on Digital Rights and Principles for the Digital Decade. (2022, January 26). https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration

Golovin, D., Nazymko, Y., Koropatov, O., & Korniienko, M. (2022). Electronic evidence in proving crimes of drugs and psychotropic substances turnover. *Access to Justice in Eastern Europe,* 5(2): 156-166. https://doi.org/10.33327/ajee-18-5.2-n000217. URL

Granada Ministerial Declaration on the European Digital Agenda. (2010, April 19). URL: https://www.mincotur.gob.es/es-es/gabineteprensa/notasprensa/documents/declaration.pdf

Korniienko, M.V., Petrunenko, I.V., Yena, I.V., Pankratova, K.O., & Vozniakovska, K.A. (2020). Negative effects of corruption offenses for the country's economy. *International Journal of Management (IJM), 11*(5): 1072-1083. https://doi.org/10.34218/IJM.11.5.2020.09818569/

Kovalova, O., Korniienko, M., & Postol, O. (2019). Ensuring of child's dignity as a principle of modern education: Administrative and legal aspects. *Asia Life Sciences Supplement, 21*(2): 341-359. Publicado: jun 27, 2024 https://doi.org/ https://www2.scopus.com/record/display.uri?eid=2-s2.0-85077192885&origin=resultslist&sort=plf-f

Melnyk, K.S. Foreign and domestic experience in the formation of the personal data protection institute. (2013). *Information Security of the Individual, Society, State, 2*(12): 97–103.

Melnyk, K.S. Improvement of Regulatory and Legal Regulation of Personal Data Protection in Ukraine. (2014). *Legal Informatics, 1*(41): 30–44.

Obukhovska T. Classification of Personal Data and Access Regime to Them: Mechanisms of Public Administration. http://visnyk.academy.gov.ua/wp-content/uploads/2013/11/2013-1-13.pdf

Onishchenko, V.V. (n.d.). *Protection of Personal Data*. URL: http://jrnl.nau.edu.ua/index.php/UV/article/viewFile/6540/7311

Recommendation "Basic Directions for the Protection of the Rights of Individuals. (1997, December 9). Connection with the Processing of Personal Data on Information Superhighways". *Visn. NADU, 2011*(4): 119–126.

Recommendation CM/Rec(2012)4. (2012, April 4). Committee of Ministers on the protection of human rights with regard to social networking services. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016, April 27). On the protection of individuals 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). https://zakon.rada.gov.ua/laws/show/984_008-16#Text

Rogova, O.G. *Protection of personal data in the legislation of the European Union and Ukraine*. (2011). Kharkiv: Kharkiv Regional Institute of Public Administration of the National Academy of Public Administration under the President of Ukraine 'Magistr', Issue 3 (34), 512 p.

Smokov, S.M., Horoshko, V.V., Korniienko, M.V., & Medvedenko, S.V. (2022). Rule of Law as a Principle of Criminal Procedure (on materials

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2025.19.19032

of the European Court of Human Rights). *Pakistan Journal of Criminology, 14*(3): 37-46.

Tyshchenko, K. (n.d.). GDPR – New Challenges for Personal Data Processors. *Legal Newspaper Online*. http://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/gdpr-novi-vikliki-dlya-obrobnikiv-personalnih-danih-vukrayini.html

Universal Declaration of Human Rights. (1948). https://zakon.rada.gov.ua/laws/show/995_015#Text

Yesimov, S.S. (2013). Protection of Personal Data in the Context of the Development of Dynamic Systems. *Scientific Bulletin of the State University of Internal Affairs,* 3: 198–207. http://www2.lvduvs.edu.ua/documents_pdf/visnyky/nvsy/03_2013/13yessdis.pdf

Cómo citar

Sistema IIJ

Kotenko, Mykola, Ruslan, Karagioz, Sopilko, Iryna, Andrusiv, Valerii, y Yermakova, Hanna, "Personal data protection in Ukraine via the prism of european judicial institutions' practise", *Estudios en derecho a la información*, México, vol. 10, núm. 19, enero-junio de 2025, pp. 151-173. https://doi.org/10.22201/iij.25940082e.2025.19.19032

APA

Kotenko, M., Ruslan, K., Sopilko, I., Andrusiv, V., y Yermakova, H. (2025). Personal data protection in Ukraine via the prism of european judicial institutions' practise. *Estudios en derecho a la información*, *10*(19), 151-173. https://doi.org/10.22201/iij.25940082e.2025.19.19032