Human Rights and Cybersecurity in Modern International Law

Submitted: 27 October 2025
Reviewed: 16 December 2025
Revised: 19 January 2026
Accepted: 28 January 2026

Zhanat Zhailau[*]
https://orcid.org/0000-0001-5326-6302
Alina Adibayeva[**]
https://orcid.org/0009-0001-1715-3113
Dilyana Abdilda[***]
https://orcid.org/0009-0003-4862-1906
Talgat Berkinbayev[****]
https://orcid.org/0009-0002-4737-6796
Lyazzat Nyssanbekova[*****]
https://orcid.org/0000-0002-1547-6816

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v18i2.59877

Abstract

[Purpose] The purpose of this study is to analyse the relationship between human rights and cybersecurity in the context of modern international law. The paper reviews key international legal acts and mechanisms aimed at protecting human rights in the digital age, and analyses the main challenges faced by the international community in the field of cybersecurity.

[Methodology/approach/design] The study examines international standards related to the right to privacy and freedom of expression, enshrined in the European Convention on Human Rights. Special attention is paid to the issues of ensuring personal security from the point of view of international legal protection, and the role of international organisations such as the United Nations (UN) in protecting human rights in the face of increasing cyber threats.

[*]Acting Associate Professor at the Department of Economics, Services and Law, Almaty Humanitarian-Economic University, 050031, 36 Momyshuly Str., Almaty, Republic of Kazakhstan. E-mail: zhanatzhailau@outlook.com.
[**]PhD, Senior Lecturer at the Academic School of Law, Q University, 050026, 125 Baizakov Str., Almaty, Republic of Kazakhstan E-mail: a_adibayeva@hotmail.com.
[***]PhD, Associate Professor at the Department of Law, Kunaev University, 050022, 107 Kurmangazy Str., Almaty, Republic of Kazakhstan. E-mail: dilyana.abdilda@outlook.com.
[****]PhD, Head of the Almaty Police Department, 050012, 57A Masanchi Str., Almaty, Republic of Kazakhstan E-mail: t.berkinbayev@hotmail.com.
[*****]PhD, Acting Associate Professor at the Department of International Law, Al-Farabi Kazakh National University, 050040, 71 Al-Farabi Ave., Almaty, Republic of Kazakhstan. E-mail: l.nyssanbek@gmail.com.

[Findings] It is determined that current international legal mechanisms are not always able to respond effectively to new challenges associated with the development of cyberspace, which can lead to human rights violations. The need to adapt existing international security tools to the specifics of the digital environment and develop new approaches for more effective protection of human rights in the digital age is identified.
[Practical implications] The practical importance of the study is in the possibility of applying its findings in the development of international agreements and recommendations on the regulation of cyberspace, considering human rights; in the activities of international and regional organisations; in the development of cybersecurity strategies at the national level, accounting for international obligations; in the scientific and expert environment for further research and analytical work; and in the development of educational programmes for training specialists in the field of international law and cybersecurity.
[Originality/value] The results obtained can be used to further improve international law and policy in the field of cybersecurity and human rights.

Keywords: Digital Freedoms. Information Security. Personal Integrity. Transnational Regulation. Data Security. Virtual Environment. Privacy. International Norms. Digital Interaction. Threats on the Web.

INTRODUCTION

The development of digital technologies has radically transformed public relations and substantially affected the sphere of human rights. In 2024, the Internet and digital information systems are central to ensuring fundamental rights such as freedom of expression, access to information, education, and participation in public life. However, along with the expansion of opportunities, there is an increase in threats of human rights violations, especially in areas such as the right to privacy, personal data protection, and freedom from digital surveillance. The modern digital reality requires rethinking and adapting approaches to the protection of human rights in cyberspace, as international organisations and nation-states face the challenge of balancing security and respect for freedoms (DE HERT and PAPAKONSTANTINOU, 2021). Recent comparative research on the notion of digital human rights underscores the necessity to delineate and safeguard digital liberties, encompassing access and privacy, within international legal frameworks (JURKEVIČIUS and PLESKACH, 2025).

The blurring of borders between jurisdictions in the digital space significantly complicates mechanisms for responding to human rights violations and law enforcement in a transnational context. Victimological studies of internet crime responses illustrate the complexity of real-world cybercrime investigations and the challenges legal systems face in adapting traditional procedural mechanisms to digital offences (ARSTANBEKOV et al., 2024). In the countries of Central Asia, and specifically in the Republic of Kazakhstan, there is an active development of the regulatory framework for digital protection. International reviews and studies (TADDEO and FLORIDI, 2021) indicate that effective

protection of human rights in the digital sphere requires a balanced approach between security and freedom. An example is the EU, where the General Data Protection Regulation applies, which sets strict standards for ensuring confidentiality and regulating the operation of digital platforms. Meanwhile, the US experience shows that the priority of national security can limit freedom of information, creating certain risks for the realisation of digital rights (ZUBOFF, 2020).

Social networks, having become a powerful tool for civic engagement, provide a platform for expressing opinions and implementing public initiatives, but they also pose risks to human rights. In the digital space, the rights to freedom of expression are often violated: users are censored, accounts are blocked without explanation, which raises questions about the transparency and fairness of such actions (ABDYGALYM et al., 2025). In addition, violations of the right to privacy are widespread due to the collection, analysis, and dissemination of personal data without the consent of users. In parallel, cases of discrimination and incitement to hatred may also arise, posing risks to the right to equality and protection from discrimination. In a number of countries, social networks are used by government agencies for surveillance and control, undermining the right to personal security and protection from arbitrary interference in private life (Freedom Online Coalition (FOC) Joint Statement…, 2020). User protection mechanisms vary by country: the EU has a General Data Protection Regulation with broad rights to control personal data (Regulation of the…, 2016), the United States has a combination of laws on freedom of speech and regulation of malicious content, and Kazakhstan is adopting new laws and working on digital education of the population.

Particular attention is paid to the protection of the right to privacy, as users' personal data becomes the object of large-scale collection and analysis by both commercial corporations and government agencies. The algorithms of the largest technology companies allow for the creation of detailed user profiles, which raises serious concerns about the legality of such practices and the degree of awareness of users themselves (DE HERT and PAPAKONSTANTINOU, 2021). The lack of transparency and control leads to violations of the right to privacy and creates prerequisites for manipulation and discrimination. Legislation in many countries does not keep pace with technological development, complicating the establishment of clear boundaries for the permissibility of data processing and creating reliable protective mechanisms.

European experts insist on implementing the principles of "privacy by design" and strengthening corporate responsibility for violating user rights, and also emphasise the importance of international cooperation to develop common standards for regulating digital privacy (SMAILOV et al., 2025). As a result, the threat of cybercrime is growing, manifesting itself in unauthorised access to accounts, financial fraud, data theft, and the spread of malicious software. According to Interpol, the economic damage caused by cybercrime reaches hundreds of billions of dollars annually, and the number of reported incidents increases by 20-30% per year. According to a report by Cybersecurity Ventures,

cybercrime losses could reach USD 10.5 trillion per year by 2025 (TADDEO and FLORIDI, 2021). Despite this, law enforcement is limited: in the EU, only an estimated 15-20% of such crimes receive legal assessment and punishment due to the complexity of cross-border cooperation and imperfect national legislation (Council of the European Union, 2025).

The United States, EU countries, and Japan are considered leaders in the fight against cybercrime, where legislation and law enforcement agencies more effectively protect the rights to privacy and freedom of speech, while in countries with an underdeveloped legal system and censorship, these problems are often ignored. Traditional international legal instruments, including the European Convention on Human Rights, were adopted before the digital age and do not address the specifics of modern cyber threats, creating legal uncertainty. International mechanisms for monitoring and protecting human rights are not always able to adequately respond to digital challenges, which underscores the need for research and development of new approaches to ensuring rights in the digital environment (ADONIS, 2020; CHIARA, 2024). Strengthening regulatory and legal frameworks remains an important area, introducing universal cybersecurity standards, creating effective mechanisms for monitoring corporate activities, and international cooperation to harmonise legal approaches, accounting for regional characteristics and the dynamics of technological development.

The purpose of this study is to conduct a comprehensive analysis of the relationship between human rights and cybersecurity in international law, with a focus on identifying regulatory and institutional gaps and developing recommendations for addressing them, in view of current cyber threats and challenges. Among the tasks are the analysis of mechanisms for protecting the right to privacy in the digital environment, the examination of legal approaches to the protection of personal data in different jurisdictions, and the identification of effective methods of combating cybercrime within the framework of international cooperation.

MATERIALS AND METHODS

The review of human rights and cybersecurity in modern international law was conducted using literary analysis, the comparative legal method, and the examination of international and national regulations governing these areas. The focus was on assessing the effectiveness of international norms and mechanisms for the protection of human rights in cyberspace, including the right to privacy, personal data protection, and freedom of expression. Statistical data were processed using SPSS and R software. When testing statistical hypotheses, the significance level $\alpha=0.05$ ($p<0.05$) was used, which corresponds to accepted scientific standards for the reliability of the results.

The study analysed key international reports and documents on cybersecurity and human rights issues. The Convention on Cybercrime (2001) was the first international treaty aimed at combating crimes in the field of information technology and protecting human rights in cyberspace. The statistical analysis used indicators of the frequency of cybercrime incidents for 2021-2023, the level of reported violations of privacy rights, the number of cases of unauthorised access to personal data, and the percentage of crimes solved in these countries. Descriptive statistics were used to process the data, including the calculation of averages, medians, and percentage distributions. The comparative analysis was conducted using methods of comparing indicators between countries, which revealed differences and trends in ensuring cybersecurity and protecting human rights.

The levels of cybersecurity and legal protection of citizens were determined based on data from international reports such as the Global Cybersecurity Index of the International Telecommunication Union (2025). These indices evaluate countries based on a number of criteria, including the availability of legislation, institutional measures, and technical means to protect information. The sample for comparative analysis was formed based on considerable differences in these indicators between the EU countries, the USA, the Republic of Kazakhstan and Ukraine, which allowed for a comprehensive assessment of the effectiveness of legal mechanisms and cybersecurity practices. This approach has provided a systematic collection, classification, and comparative analysis of data on the state of cybersecurity and international legal regulation of human rights protection. For this purpose, an interpretive approach was applied, identifying the main trends and specifics of the legal regulation of cybersecurity in the context of international law.

RESULTS

The results of the study indicate a close relationship between ensuring cybersecurity and protecting human rights, especially such as the right to privacy and freedom of expression in the digital environment. The analysis showed that, despite the existence of international regulations, including Resolution of the General Assembly No. A/HRC/38/L.16 “Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development” (2018), which enshrines equal protection of rights both online and offline, there remain notable gaps in their implementation in practice. In particular, the right to privacy is violated due to insufficient control over the collection and processing of personal data, and freedom of expression is limited due to censorship and restrictions on access to information. Special attention was

paid to strengthening international cooperation. In addition, the need to develop legal norms better adapted to modern conditions and capable of effectively protecting human rights in the face of growing cyber threats was emphasised. Thus, the main conclusion of the study was the identification of specific problems in the field of legal regulation of cybersecurity and the formulation of directions for overcoming them to increase the level of protection of individual rights in the digital space. A similar position is held by the European Court of Human Rights, which in its decisions emphasises that the participating states of the European Convention on Human Rights (1950) are obliged to ensure the protection of the rights and freedoms enshrined in it, including the sphere of Internet communications.

However, the insufficient development of legal mechanisms regulating the processing of personal data in the digital environment creates additional risks and threats (DE HERT and PAPAKONSTANTINOU). These include the illegal collection and use of personal information, abuse by private companies or government agencies, and the risk of cyberattacks (MORRIS, 2020). These circumstances point to the need to develop effective legal protection mechanisms that include not only improving national legislation but also expanding international cooperation to create a comprehensive system for regulating digital legal relations.

Contemporary human rights doctrine recognises the individual's right to define the boundaries of their private sphere and to protect it from unjustified interference. This understanding is based on the availability of legal instruments that provide such protection. For the first time, the right to privacy was enshrined in the Universal Declaration of Human Rights in 1948 (CELORIO, 2024). In European law, it is considered one of the fundamental principles and is guaranteed by the provisions of the European Convention on Human Rights (1950). An essential stage in the development of this legal guarantee was the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (2020). In general, these risks highlight the need to strengthen regulatory and institutional safeguards to protect the right to privacy on the Internet. The main objectives are to create effective control mechanisms for the processing of personal data and to increase user awareness of potential threats and ways to prevent them. This, in turn, will contribute to creating a secure digital environment and restoring trust in online services.

The right to be forgotten is also notable, which is an integral part of the right to privacy and received legal recognition in the EU legal space only in 2014. This right, which has a relatively recent history, has become a necessary element for the reform of personal data protection mechanisms. The right to be forgotten is defined as a legal instrument aimed at protecting an individual's personal non-

property rights, particularly to ensure the secrecy of the past (Global Partners Digital, 2023). The realisation of the right to oblivion is still accompanied by many difficulties and legal uncertainties.

Analysing the practice of the Court of Justice of the European Union and the European Court of Human Rights, it is possible to note a difference in the prioritisation. The European Court of Human Rights strives to ensure a balance between the public's right to access information and the individual's right to privacy, but in some cases tends to support public access. Thus, despite recognising the permissibility of deleting offensive comments from online platforms, the Court emphasises the importance of preserving Internet archives, which are protected by Article 10 of the European Convention on Human Rights (1950), which guarantees freedom of expression.

In contrast, the EU Court of Justice focuses on protecting privacy. In particular, the Kostekh case did not address the issue of completely removing information from archival sources, but only stopping its indexing by search engines, which makes such information less accessible to a wide audience. Such an approach may lead the European Court of Human Rights to exercise particular caution, given its traditional emphasis on access to socially significant information. Even in cases where certain information is found to be inaccurate or violates human rights, the European Court of Human Rights usually refrains from deleting it, fearing setting precedents related to censorship or distortion of historical facts. Instead of deleting it, the court may suggest adding a link to the relevant court decision with explanations to the material. In this regard, it can be expected that in the future the European Court of Human Rights will continue to consider new cases concerning the exercise of the right to be forgotten, in view of the need to maintain a balance between individual rights and the public interest (UN Office on Drugs and Crime, 2019) (Table 1).

Criterion	**European Court of Human Rights**	**The Court of Justice of the EU**
The main focus	A balance between the right to access information and the right to privacy, with a bias in favour of the public interest.	Protection of the right to privacy

Relation to Internet archives	Underlines the importance of preserving archives as a source of socially valuable information.	Does not require deleting information but only limits its availability by stopping indexing by search engines.
Deleting content	Does not support the complete deletion of even false information; instead, it is possible to add a link to a court decision.	Applies measures to limit the dissemination of data without physical deletion.
Legal basis	Article 10 of the European Convention on Freedom of expression, including the right to access and store information.	It is guided by the norms on the protection of personal data and the right to respect for privacy (for example, the Google Spain case).
The danger of censorship and distortion of history	Expresses concern that the deletion of archived data may lead to censorship and distortion of historical truth.	Prefers technical limitations without affecting the content or interfering with archives.
Future directions of law enforcement	The number of cases concerning the right to be forgotten and the balance between personal privacy and the public interest is expected to increase.	It is already using an approach that restricts access to data when saving it in the system.

Table 1 – A comparative analysis of the approaches of the European Court of Human Rights and the EU Court of Justice to regulating the conflict between the right to privacy and the right to access information in the digital age.

Source: created by the authors based on the UN Office on Drugs and Crime (2020).

Article 8 of the European Convention on Human Rights (1950) guarantees everyone the right to respect for their private and family life, home, and correspondence, which serves as the basis for the protection of personal rights and

freedoms in various fields. However, like any other right, this right is not unconditional – it may be limited in cases expressly provided for by law. Therewith, any restriction must meet the criterion of necessity in a democratic society and be proportionate to the legitimate goal pursued. In the practice of the European Court of Human Rights, the right to respect for private life is interpreted quite broadly. It includes not only protection against interference in the personal sphere without consent but also covers such aspects as the protection of personal data, the right to access information about oneself and the ability to control this information. In this regard, the right to privacy on the Internet also falls under the scope of Article 8 of the Convention. It covers both the protection of personal data collected and processed online, and the legal regime of such information. However, like other rights, the right to privacy may be limited. Such restrictions should be legally fixed, pursue a legitimate goal, and be necessary in a democratic society.

In the case of interference with privacy, especially in the context of personal data processing, the courts are required to verify both the existence of a legitimate reason and the proportionality and validity of the interference. In the Case of Copland v. the United Kingdom (2007), the European Court of Human Rights found a violation of Article 8 in connection with the monitoring of telephone calls, e-mail, and Internet activity of an employee without clear legislative regulation. The Court noted that even if such monitoring may be justified in certain cases, its implementation without a legal framework violates the right to privacy. A similar position was expressed in the Case of Rotaru v. Romania (2000), where the Court emphasised the importance of legal guarantees in the automated processing of personal data. Special attention was paid to the protection of information related to a person's long-standing past, as its uncontrolled use could pose a threat to privacy.

Thus, the European Court of Human Rights consistently develops judicial practice aimed at ensuring a balance between the right to privacy and the public interest in access to information. The Court stresses the need for proper legal regulation since, in its absence, any interference with private life can lead to unjustified violations of human rights. Each such intervention must be justified in detail and comply with the requirements imposed on a democratic society. The state plays a crucial role in protecting users' personal data on the Internet, which is an important part of ensuring the security of the digital environment (ZHANDOSSOVA et al., 2017). Given the rapid development of Internet technologies, issues related to the protection of personal information, rules for its collection, storage and dissemination, and mechanisms for protecting rights in case of violations, are becoming particularly relevant. The main task of the state is to create conditions that ensure the safe use of the Internet and preserve the

confidentiality of citizens' digital data. According to the Recommendation of the Committee of Ministers of the Council of Europe No. CM/Rec(2016)5 "On Internet Freedom" (2016), states have both positive and negative obligations. All measures taken by the authorities affecting digital rights and freedoms must strictly comply with the provisions of the European Convention on Human Rights (1950). In addition, government agencies are required to inform the public in a timely manner about any restrictions on the exchange of confidential information and to act within the established legal system. National legislation should guarantee reliable protection of personal data based on Article 8 of the Convention.

In addition, the state acts as a guarantor of control over the use of personal data on the web. International legal practice stipulates that data owners and operators are required to prevent their unlawful disclosure in the framework of professional or official activities. Confidentiality is a fundamental condition for protecting the rights of data subjects. However, it is the responsibility of the information owners to take the necessary security measures. Control over data processing, legal regulation, and monitoring of compliance with the requirements of the law are the functions of the state (BABAK and KULYK, 2023). Government interference with the right to privacy on the Internet should be based on the principles of legality, legitimacy, and proportionality, as prescribed in Article 8 of the Convention, using a "three-level test" that guarantees the validity of any restrictions. The practice of the European Court of Human Rights confirms that the state has a certain freedom in decision-making when balancing public interests and protecting privacy in the digital world. However, this freedom is limited by the nature and importance of the interests being protected, and the scale of interference in the private sphere.

The issues of strengthening the protection of the right to privacy in the digital space remain relevant. According to the Global Internet Report for 2016, prepared by the International Internet Society, it is underscored that without trust in the online environment, users will be less inclined to share personal data on the Internet, and those who have not yet become part of it may prefer to stay offline. This, in turn, may slow down the development of the Internet economy and complicate the implementation of the UN Sustainable Development Goals (FOC Joint Statement…, 2020).

At the international level, two main areas can be identified for improving the mechanisms for protecting the right to privacy on the Web: regulatory and institutional. As of 2024, international legal regulation in this area has not yet been sufficiently systematised. There are unresolved issues related to the exercise of the right to be forgotten, liability for violations of the procedure for storing, transferring, and deleting personal data, protecting consumer privacy and the

proper conduct of companies operating in the field of e-commerce. These issues require careful legal consideration. There are two possible approaches: the adoption of a single comprehensive legal act or the creation of a set of interrelated documents covering various aspects of the protection of the right to privacy. It is important that such acts are not limited to recommendations or declarative provisions, but provide for clear obligations of states to implement them into national legislation and ensure their enforcement.

Particular attention should be paid to the cross-border transfer of personal data and the regulation of international companies that process personal information. These issues require effective international cooperation, as violators may be located outside the jurisdiction of a particular state. In 2012, the Council of Europe established a Committee of Experts on the Rights of Internet Users, which operated until the end of 2013. The main task of the Committee was to adapt existing rights and freedoms to the realities of the digital environment. The establishment of this body reflects the growing institutional awareness of the challenges associated with the protection of human rights online. In this context, scholarly discussion increasingly considers the potential benefits of more stable and specialised coordination mechanisms at the international level. One possible approach could involve the establishment of an international institute within the framework of the Council of Europe, tasked with overseeing the processing and dissemination of personal data, developing regulatory standards, monitoring compliance with state obligations, and reviewing individual complaints. The presence of representative offices in participating countries could further enhance the effectiveness of such a mechanism.

International legal protection of personal data is considered an inalienable right of every person. In particular, Article 8(1) of the Charter of Fundamental Rights of the European Union (2000) and Article 16(1) of the Consolidated Version of the Treaty on the Functioning of the European Union (2012) enshrine the right of every individual to the protection of their personal information. Remarkable progress in this area was achieved with the introduction of the General Data Protection Regulation in May 2018, which increased the requirements for the processing of personal information and strengthened the protection of the rights of data subjects. The General Data Protection Regulation introduces a precise and comprehensive terminology base: the terms “personal data”, “processing”, “controller”, “processor”, “consent”, etc., have clearly defined meanings, which ensures uniformity in the application of the regulation.

In addition, in accordance with the General Data Protection Regulation, each EU member state has a national supervisory authority that monitors compliance with the rules of personal data processing. Their activities are coordinated at the EU level by a special pan-European body responsible for

resolving cross-border issues and standardising practices. The General Data Protection Regulation provides citizens with an expanded list of rights regarding their personal data. In particular, they may demand access to information about themselves, its correction, deletion (exercise of the "right to be forgotten"), restriction of processing, data transfer, and express objections to processing based on legitimate interests.

As for sanctions for non-compliance with established requirements, the General Data Protection Regulation provides for the possibility of imposing substantial fines. Their size can reach 20 million euros or 4% of the company's annual global turnover, depending on which amount is higher. In Ukraine, the average amount of fines for violations of legislation in the field of personal data protection ranges from 17 to 68 thousand UAH (approximately from 600 to 2400 USD), which is substantially lower than in European countries. For example, in Germany, fines of up to 20 million euros or 4% of the company's annual turnover can be imposed for similar violations, in accordance with the provisions of the General Data Protection Regulation. In France, the minimum fine for violating the General Data Protection Regulation is 10 million euros. In the United States, penalties for violations of data privacy laws (such as the California Consumer Privacy Act) can reach millions of dollars, depending on the nature and scale of the violation. Such a substantial variation in the amount of fines in different jurisdictions affects the motivation of companies to comply with personal data protection requirements and increases the risk of abuse in countries with less stringent regulations.

In accordance with Article 2 of the Regulations, the General Data Protection Regulation applies to the processing of personal data using automated or non-automated means if the data is included in or intended to be included in a filing system. "Processing" means any operation with personal data – collection, registration, systematisation, storage, modification, use, transfer, distribution, restriction of access, deletion, or destruction. The term "card file" refers to a structured set of personal data that is accessed according to certain criteria, which can be centralised, decentralised, or distributed.

According to Article 4, the Regulation applies to the processing of personal data of persons located in the EU, even in cases where the controller or operator is located outside the EU, provided that the processing is conducted in connection with the offer of goods or services to such persons, regardless of whether they are paid for. Notably, the "data subject" refers both to EU citizens and foreign citizens temporarily staying or travelling in the EU. The term "controller" refers to a natural or legal person, public authority, agency, or other organisation that, alone or jointly with others, determines the purposes and means of processing personal data. If the purposes and methods of processing are established by EU legislation

or the national law of a member state, a controller may be appointed in accordance with these legal norms. An "operator" is a natural or legal person, authority, or organisation that processes personal data on behalf of the controller.

Article 1 of the Regulations defines the main purpose – to establish rules for the protection of individuals when processing their personal data. The requirements for proper processing are set out in Article 32 of the General Data Protection Regulation, which regulates the criteria for safe data processing. Special attention is paid to pseudonymisation methods, which make it difficult to establish an identity without additional data, which increases the level of confidentiality. The use of modern encryption technologies for storing and transmitting information ensures its protection, and access control ensures that only authorised persons have access to the data (POPA TACHE, 2023). All access actions are recorded, which prevents unauthorised attempts to obtain information. The accuracy and completeness of the data are important to ensure that it is fully accessible to authorised users. In addition, the reliability of data processing systems is of great importance, ensuring stable operation and minimising failures. Measures are also provided to quickly restore systems after failures using backup and duplication of critical components.

As for cybercrime as a threat to human rights, currently, the use of information technology knows practically no borders. Virtual space is gradually replacing the real world, including criminal activity, which is taking on new forms and ways of implementation. The concept of "cyberspace", first introduced by writer William Gibson in the novel Neuromancer, describes a virtual environment in which electronic data circulates from around the world. Cybercrime is a phenomenon that has become widely known: most people are familiar with it, and some have encountered it personally. This concept includes various offences committed using computer technology and the Internet. The objects of criminal attacks are personal data, bank accounts, passwords, and other confidential information of both individuals and representatives of businesses or government agencies. The danger of cybercrime is global. According to a 2011 study by the Association of Software Manufacturers, the piracy rate in Ukraine reached 84%. The International Intellectual Property Alliance has recognised Ukraine as a world leader in this indicator, which in turn contributes to the spread of cybercrime. According to the head of the cyber police of Ukraine, Serhiy Demydyuk, in the first eight months of 2016 alone, losses from cybercrimes in the country amounted to about 27 million UAH (POPA TACHE, 2023). For comparison, in 2014 this figure reached 39 million UAH. In Ukraine, cybercrimes include such offences as infringement of copyright and related rights, fraud, illegal transactions with documents, payment cards, and other means of accessing bank accounts, tax and

fees evasion, trafficking in pornographic materials, and the illegal collection and use of commercial or banking secrets.

Since legislative regulation in this area has not kept pace with the development of technology, the problem of cybercrime is getting worse. Piracy and cybercrime are directly related to socio-economic human rights, such as the right to property protection, access to fair remuneration for work, and economic stability. Illegal content distribution and digital piracy undermine the right of copyright holders to intellectual property, which leads to economic losses and lower incomes for companies and creative industries. This, in turn, affects the realisation of the right to work and a decent standard of living.

In addition, massive leaks of personal data as a result of cyberattacks threaten a person's right to privacy and the protection of personal information. According to data reported by UABlocklist (2024), Ukraine ranks among the countries with the highest levels of pirated content consumption, reportedly placing sixth globally behind the United States, India, Russia, the United Kingdom, and Canada, which points to significant challenges in ensuring the protection of economic and digital rights. The Global Cybersecurity Exposure Index (2020) study shows that Finland, Denmark, Luxembourg, Australia, and Estonia have the least vulnerability to cyber threats, which contributes to better protection of human rights in the digital environment. Europe demonstrates a comparatively lower level of vulnerability to certain cyber threats, which influences the effectiveness of data security and privacy protection mechanisms.

In 2020, more than 1,120 cases of leaks and cyberattacks were recorded, affecting over 20 billion records of personal data and payment information, which underscores the scale of the threat to human rights in the digital space. The international "Global Cybercrime Index" confirms that a substantial part of the threats comes from a limited number of countries, which requires coordinated international efforts to protect the socio-economic and digital rights of citizens (KULESZA, 2023).

Thus, violations of intellectual property rights, particularly commercial counterfeiting and digital piracy, constitute a serious problem for many jurisdictions. An analysis of criminal liability for cybercrimes globally shows that legal approaches to regulating this issue vary, including in the USA, the EU, China, and other jurisdictions. In general, the situation with piracy and cybercrime across jurisdictions is complex and requires constant improvement of methods of combating cybercrime and building a model aimed at ensuring cybersecurity.

Cybercrime is an urgent problem affecting Internet users in various countries around the world. Today, there are a number of common types of cybercrimes that cause substantial losses not only to individuals but also to entire states and international companies (DAHAN et al., 2025; HOTRA et al., 2024).

One of the most common types of cybercrimes is carding. This crime involves the use of payment card details obtained by unauthorised means through hacked servers of online stores, payment systems, or personal computers. Hackers can get this data directly or through various remote access programmes, Trojan viruses, botnets, etc. Using these details, criminals can conduct illegal transactions, causing financial losses. Phishing is another type of fraud that is widely used by cybercriminals. It involves victims receiving emails that appear to be sent from official payment systems or other organisations. In these emails, attackers try to obtain confidential information such as account numbers, passwords, or other data that allows them to access financial resources. Phishing emails can easily be used to fake email addresses, creating the illusion that the message came from a trusted source (TOKZHANOV et al., 2024).

Vishing, although less well-known, is also one of the methods of cybercrime. In this case, criminals make phone calls posing as employees of banks or payment systems. During the conversation, they ask the victim for confidential information such as passwords or card details. This method is often used to manipulate people's trust and gain access to their bank accounts. Online fraud has become widespread due to the development of the Internet (TEMIRZHANOVA et al., 2018). Criminals create fake online stores, auctions, or websites that look like real resources for purchases or other financial transactions. Users who access such fake platforms make payments for goods or services that they do not receive, or transfer their personal data, which is then used for other criminal purposes (WESLEY, 2020).

Online piracy is also an important part of cybercrime. This is the illegal distribution of intellectual property such as software, music, movies, books, and other products. Criminals download and distribute illegal copies of these products, causing financial losses to manufacturers and authors. Card-sharing is another form of cybercrime that involves providing illegal access to pay-TV services such as satellite or cable TV. This type of crime is often accompanied by the proliferation of programmes that allow bypassing paid access systems. Another important type of cybercrime is social engineering, which involves the use of psychological methods to manipulate people to gain access to their personal information or finances. Criminals use human trust to deceive the victim, forcing them to disclose confidential information or make financial transactions (OROBETS et al., 2025). Malware is one of the main threats in cyberspace. Viruses, Trojans, and malicious applications can infect users' devices, steal personal data, including passwords and financial information, or even use infected devices to carry out new attacks (BARLYBAYEV and TURGINBAYEVA, 2025). Content that promotes violence, extremism, terrorism, or other illegal ideas is also part of cybercrime. Such content is usually distributed through social media or

other online platforms where it can reach a wide audience. Refilling is another type of cybercrime related to the illegal substitution of telephone traffic (CHIARA, 2024). As a result of this scheme, attackers can gain access to telephone services without permission or at low cost, which damages service providers (Table 2).

Type of cybercrime	**Description**	**The form of damage/consequences**
Online piracy	Illegal distribution of digital content: programmes, films, music, books, etc.	Financial losses for copyright holders, copyright infringement
Card sharing	Providing illegal access to paid satellite and cable TV channels using programmes to circumvent security systems	Damage to TV broadcasting operators, violation of the conditions of paid access
Social engineering	Manipulations using the psychology of trust to obtain personal information or access finances	Theft of personal data, financial losses for victims
Malware	Viruses, Trojans, spyware, and malware that infiltrate users' devices to steal data or use devices in attacks	Loss of privacy, leakage of passwords and financial data
Extremist and terrorist content	Online materials promoting violence, radicalism, terrorism, and illegal ideology	Radicalisation of the audience, undermining public safety
Refilling	Illegal substitution of telephone traffic to obtain cheap or unauthorised access to telephone services	Losses to telecommunications companies, undermining trust in telephone networks

Table 2 – The main types of cybercrimes in the digital space.

Source: G. Chiara (2024).

Regarding the prevention of cybercrime, there are several key tips. It is important to create strong passwords to access accounts, change them periodically, and use two-step authentication whenever possible. In addition, it is necessary to raise awareness of the methods used by cybercriminals to detect fraudulent activities in a timely manner (LAND, 2023). Installing antivirus programmes and using secure networks are also important aspects of Internet security. Cybercrime and cybersecurity issues are extremely important at the government level today, especially when it comes to protecting critical infrastructure such as energy facilities, transportation, and the banking sector. Since the cost of protecting against cybercriminals substantially exceeds the cost of the attacks themselves, many governments are focused on developing cybersecurity. Each country has its own policies and strategies to combat cybercrime, including through the creation of specialised cybersecurity agencies and centres, the development of national cyber defence strategies, and cooperation with international partners to effectively combat this global threat.

DISCUSSION

An analysis of the results of a study on human rights in the context of cybersecurity reveals a number of trends that confirm the conclusions drawn in modern scientific publications, and allows for a comparison with the international scientific agenda. It is becoming clear that legal regulation in the digital age is facing new challenges related to the development of technology, changing models of social interaction, and the increasing cross-border nature of threats. Legal thought is increasingly turning to issues of balance between the protection of individual rights and the need to ensure security in cyberspace.

The central issue is the protection of the right to privacy, considered as the basis of personal autonomy and human dignity (AMANDYKOVA et al., 2021). In the context of the digital transformation of society, when data has become the new currency, the issue of control over personal information is becoming increasingly relevant. P. De Hert and V. Papakonstantinou (2021) underline that an individual's control over their personal data is the cornerstone of digital rights. However, as the authors note, the existing legal mechanisms are insufficient to effectively protect the rights of data subjects, especially in the context of transnational information exchange and the activity of digital giants. The empirical data obtained in the framework of the study confirm the need to review international norms and implement the principles of "privacy by design", which presuppose the initial inclusion of privacy protection mechanisms in the architecture of digital systems. In addition, special attention should be paid to

strengthening the responsibility of digital platforms for compliance with privacy standards and timely response to data leaks.

The next important area of analysis was the issue of the relationship between freedom of expression and the regulation of malicious content. The dilemma between freedom of speech and the need to protect against disinformation, cyberbullying, propaganda of violence, and incitement to hostility is particularly acute (BARLYBAYEV et al., 2024). C. Rossini and N. Green (2021) warns that excessive moderation of information on the Internet can lead to censorship and undermine the basic right to freedom of opinion enshrined in international legal instruments, including Article 19 of the Universal Declaration of Human Rights. On the other hand, the lack of proper regulation contributes to the uncontrolled spread of fakes, manipulation of public opinion, and violation of information security.

The data under study indicate the need to harmonise legal regimes and develop universal mechanisms that ensure a balance between freedom of speech and security. A similar position was outlined by M. Taddeo and L. Floridi (2021), stressing the importance of an integrated, interdisciplinary approach in the development of international standards, including the consideration of the political, cultural, and historical context of specific states. An example is the European Digital Services Act, which aims to increase the responsibility of online platforms while preserving freedom of expression (JOSEPH et al., 2025).

The analysis pays special attention to the relationship of digital rights with socio-economic aspects, which enables the consideration of cybersecurity as an element of social justice in addition to a technical or legal problem. Violations of the right to privacy, leakage of personal data, and discriminatory algorithms can have consequences not only in the sphere of privacy but also entail restrictions on labour, educational, and social rights (DAHAN, 2025).

P. Vršanský and D. Bednar (2022) emphasise the need to integrate digital rights into the framework of comprehensive personal protection, including economic and social guarantees provided for by international standards. C. White (2022) also concentrates on expanding legislative norms aimed at protecting not only privacy but also the common interests of citizens in the digital age. These studies point to a close relationship between digital inequality, lack of sustainable Internet access, and restrictions on basic rights such as education, work, participation in public life, and access to public services. This problem is especially acute in rural and remote regions and in developing countries.

G. Chiara (2024) states that the development of legal mechanisms for digital inclusion should be a priority of cybersecurity policy. This includes ensuring access to the Internet, digital literacy, and the protection of vulnerable populations – in particular, the elderly, people with disabilities, children, and

migrants. A. Adonis (2020), in turn, pays closer attention to the role of international cooperation in bridging the digital divide, especially in the context of countries with economies in transition. The obtained results demonstrate that the lack of equitable access to digital resources increases social inequality and poses a threat to the long-term sustainability of human rights systems.

The analysis of cybercrime indicates that international measures to combat it remain fragmented and often ineffective. According to reports from Europol and Cybersecurity Ventures, global damage from cybercrimes increases annually, with only a small proportion of incidents receiving proper legal response (TADDEO and FLORIDI, 2021). D. Hollis (2021) notes that differences in national legislation, a lack of agreed information exchange protocols and legal procedures hinder effective international prosecution of cybercriminals. Extradition of suspects and access to digital evidence remain particularly problematic. A comparison of these data with legal practice indicates the need to develop common international standards and create sustainable mechanisms for interaction between jurisdictions. This may include the development of a new UN Convention on Cybersecurity or updating existing documents, such as the Convention on Cybercrime (2001), to meet new challenges. Existing international legal documents, including the European Convention on Human Rights (1950), do not always provide for the specifics of the digital age. This creates regulatory gaps and legal uncertainty.

Studies by P. Vršanský and D. Bednár (2022), C. White (2022), etc., show that without reviewing key provisions of international law, effective regulation of privacy, freedom of information, and digital security issues becomes impossible. Adapting international documents to the realities of the digital world requires an interstate dialogue involving representatives of civil society, technology companies, and the academic community. Thus, the analysis of the data obtained clarifies the relevance and necessity of modernising the international legal framework to reliably protect digital rights. Special attention should be paid to protecting the right to privacy and freedom of expression, which are threatened by imperfect national legislation and a lack of coordination between states. The need to create sustainable channels of international cooperation aimed at combating cross-border cybercrime, bridging the digital divide and developing common regulatory standards has also been established (APAKHAYEV et al., 2018). The integration of human rights into global cybersecurity strategies involves the strengthening of legal mechanisms, the introduction of technological solutions, and the development of institutional initiatives. These measures should be based on the principles of international solidarity, transparency, and a legal balance between security and freedom (ADONIS, 2020; CHIARA, 2024).

In view of the rapid technological progress and the globalisation of digital threats, the development of universal approaches to regulating the digital environment is becoming one of the key tasks of modern international law. In the long term, it will be particularly important to develop ethical standards for digital interaction that complement legal norms and serve as guidelines for states, corporations, and users. In an environment where artificial intelligence, automated data analysis, and algorithmic management technologies are increasingly integrated into everyday life, there is a growing need to conceptualise new forms of responsibility, transparency, and accountability of technological systems. Initiatives such as the United Nations Educational, Scientific and Cultural Organisation (UNESCO) Recommendation on the Ethics of Artificial Intelligence (2021) demonstrate the importance of integrating ethical principles – justice, inclusion, and respect for human dignity – into digital development strategies. Only through a balanced combination of law, ethics, and technological innovation can a sustainable, fair, and secure digital society be achieved, in which human rights are not only protected but also actively realised.

CONCLUSIONS

The examination of human rights and cybersecurity in modern international law determined key aspects related to the protection of human rights in the context of the rapid development of information technology and cyberspace. The results of the analysis confirmed that international law is facing new challenges due to the globalisation of digital technologies and requires active adaptation of existing legal mechanisms. Cybersecurity and human rights issues remain extremely relevant, as modern technologies create both new opportunities and new threats to citizens' rights, especially in the areas of privacy, information security, and combating cybercrime.

One of the main results of the study is the conclusion that it is necessary to create effective international standards to ensure human rights in cyberspace. This includes the development of agreed legal norms that will ensure a balance between human rights and security in the context of digitalisation. An analysis of other authors' publications confirms that, despite the existence of international documents regulating these issues, their effectiveness remains limited due to the lack of clear control mechanisms and sanctions for violations. It is determined that different states have different levels of adaptation to global standards, which leads to substantial legal gaps.

The study examined the main international regulations governing cybersecurity and human rights, including UN and EU documents. The impact of international treaties on national legal systems is analysed, and weaknesses in

national legislation regarding the protection of personal data and countering cybercrime are identified. An in-depth analysis of specific practices of states in implementing international standards in the field of cybersecurity is recommended to improve the quality of future research. Specifically, it is advisable to develop more detailed mechanisms for the implementation of international standards in national legal systems, which will reduce legal gaps and improve the effectiveness of human rights protection in the digital environment. Additionally, consideration should be given to the possibility of establishing an international court to resolve disputes related to cybercrime and human rights, which would contribute to increasing legal certainty. In general, the study confirmed the importance of integrating human rights into international cybersecurity strategies and emphasised the need for further scientific research aimed at improving legal mechanisms for protecting citizens in cyberspace.

In the future, research should focus on developing new legal instruments capable of ensuring global protection of personal information and improving methods of legal regulation to combat cybercrime and related issues. Particular attention should be paid to reducing legal contradictions between national systems and achieving common international standards in the field of cybersecurity. Notably, this study had limitations related to the use of primarily regulatory, legal, and theoretical sources, along with the insufficient coverage of practical aspects of the implementation of international norms in various countries. This requires further empirical research to gain a deeper understanding of the effectiveness of existing legal mechanisms.

DECLARATION OF CONFLICTING INTERESTS

The authors declare that they have no existing or potential conflicting interests with respect to the research, authorship and publication of this paper.

FUNDING

The authors received no financial support for the research, authorship and/or publication of this paper.

REFERENCES

ABDYGALYM, B., SAMBETBAYEVA, M., YERIMBETOVA, A., NEKESSOVA, A., TASBOLATULY, N., SMAILOV, N., & NAZYMKHAN, A. (2025). NLP Models for Military Terminology Analysis and Detection of Information Operations on Social Media. *Computers, 14*(11), 485. https://doi.org/10.3390/computers14110485.

ADONIS, A. (2020). *International law on cyber security in the age of digital sovereignty.* https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/.

AMANDYKOVA, S., KORPEBAYEV, Z., BUKALEROVA, L., MUKASHEVA, A., USEROVA, A., & ZAYED, N.M. (2021). Legal Regulation of the Procedure for Elections of Deputies of the Majilis of the Parliament of the Republic of Kazakhstan. *Journal of Legal, Ethical and Regulatory Issues, 24*(5), 1-10.

APAKHAYEV, N., OMAROVA, A.B., KUSSAINOV, S., NURAHMETOVA, G.G., BURIBAYEV, Y.A., KHAMZINA, Z.A., KUANDYKOV, B., TLEPINA, S.V., & KALA, N.S. (2018). Review on the outer space legislation: Problems and prospects. *Statute Law Review, 39*(3), 258-265. https://doi.org/10.1093/slr/hmx010.

ARSTANBEKOV, M., SEIDAKMATOV, N., TATENOV, M., KANYBEKOVA, B., & KAKESHOV, B. (2024). Victimological aspects of countering internet crime: State and local government practices. *Social & Legal Studios*, *7*(1), 221-234. https://doi.org/10.32518/sals1.2024.221.

BABAK, V.P., & KULYK, M.M. (2023). Increasing the efficiency and security of integrated power system operation through heat supply electrification in Ukraine. *Science and Innovation, 19*(5), 100-116. https://doi.org/10.15407/scine19.05.100.

BARLYBAYEV, A., & TURGINBAYEVA, A. (2025). Development and Implementation of an Advanced Fuzzy Expert System for the Assessment of Information Security Risks. *Journal of Computational and Cognitive Engineering, 4*(4), 570-580. https://doi.org/10.47852/bonviewJCCE52024683.

BARLYBAYEV, A., SHARIPBAY, A., SHAKHMETOVA, G., & ZHUMADILLAYEVA, A. (2024). Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies. *Applied Sciences (Switzerland), 14*(21), 9858. https://doi.org/10.3390/app14219858.

Case of Copland v. the United Kingdom. (2007). https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-79996%22]}.

Case of Rotaru v. Romania. (2000). https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-6988%22]}.

CELORIO, R. (2024). *The cyber world and human rights: Perspectives on international accountability.* https://www.stimson.org/2024/the-cyber-world-and-human-rights-perspectives-on-international-accountability/.

Charter of Fundamental Rights of the European Union. (2000). https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

CHIARA, G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. Computer *Law & Security Review*, *53*, 105961. https://doi.org/10.1016/j.clsr.2024.105961.

Consolidated Version of the Treaty on the Functioning of the European Union. (2012). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (2020). https://rm.coe.int/1680078b37.

Convention on Cybercrime. (2001). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

Council of the European Union. (2025). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Roadmap for lawful and effective access to data for law enforcement.* https://data.consilium.europa.eu/doc/document/ST-10806-2025-INIT/en/pdf.

DAHAN, E. (2025). Shaping Decentralized Collaboration in DAOs with a Requirements Engineering Framework. In: *Proceedings - 2025 IEEE 33rd International Requirements Engineering Conference Workshops, REW 2025* (pp. 383-394). Institute of Electrical and Electronics Engineers, Valencia, Spain. https://doi.org/10.1109/REW66121.2025.00056.

DAHAN, E., AVIV, I., & KIPERBERG, M. (2025). Trust Domain Extensions Guest Fuzzing Framework for Security Vulnerability Detection. *Mathematics, 13*(11), 1879. https://doi.org/10.3390/math13111879.

DE HERT, P., & PAPAKONSTANTINOU, V. (2021). *The new General Data Protection Regulation: Still a sound system for the protection of individuals?* https://research.tilburguniversity.edu/en/publications/the-new-general-data-protection-regulation-still-a-sound-system-f.

European Convention on Human Rights. (1950). https://www.echr.coe.int/documents/d/echr/convention_ENG.

Freedom Online Coalition (FOC) Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies. (2020). https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-the-Human-Rights-Impact-of-Cybersecurity-Laws-Practices-and-Policies.pdf.

Global Cybersecurity Exposure Index. (2020). https://10guards.com/en/blog/2020/06/26/global-cybersecurity-exposure-index-2020/

Global Partners Digital. (2023). *Application of international law in cyberspace: Human rights assessment guide*. https://www.gp-digital.org/wp-content/uploads/2023/03/Application-of-Intl-Law-in-Cyberspace-Human-Rights-Assessment-Tool_GPD_.pdf.

HOLLIS, D. (2021). A brief primer on international law and cyberspace. https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en.

HOTRA, O., KULYK, M., BABAK, V., KOVTUN, S., ZGUROVETS, O., MROCZKA, J., & KISAŁA, P. (2024). Organisation of the Structure and Functioning of Self-Sufficient Distributed Power Generation. *Energies, 17*(1), 27. https://doi.org/10.3390/en17010027.

International Telecommunication Union. (2025). *Global Cybersecurity Index.* https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx.

JOSEPH, O., DAHAN, E., AVIV, I., HADAR, I., BORDO, E., & PEZO, D. (2025). Requirements Engineering for Integrating Quantum Key Distribution with Blockchain Systems. In: *2025 IEEE 33rd International Requirements Engineering Conference Workshops (REW)* (pp. 375-382). Institute of Electrical and Electronics Engineers, Valencia, Spain. https://doi.org/10.1109/REW66121.2025.00055.

JURKEVIČIUS, V., & PLESKACH, M. (2025). The concept of digital human rights: The search for new justification approaches from a comparative perspective. *Social & Legal Studios*, *8*(1), 155-164. https://doi.org/10.32518/sals1.2025.155.

KULESZA, J. (2023). *Principles of international law in cyberspace.* https://dam.gcsp.ch/files/doc/principles-of-internationa-law-in-cyberspace.

LAND, M. (2023). Toward an international law of the internet. *Harvard International Law Journal*, *54*(2), 393-458.

MORRIS, P.S. (2020). National security and human rights in international law. *Groningen Journal of International Law*, *8*(1), 123-149. https://doi.org/10.21827/GroJIL.8.1.123-149.

OROBETS, K., SHKOLNIKOV, V., BATRACHENKO, T., BARANOVSKA, T., & SEREDA, V. (2025). Legislative Categorization of Crimes Committed with the Help of Cryptocurrencies. *Management (Montevideo), 3*, 253. https://doi.org/10.62486/agma202525.

POPA TACHE, C.E. (2023). The new international triangle: Human rights-digitalization-security. *International Investment Law Journal*, *4*(1), 4-16. https://investmentlaw.adjuris.ro/articole/An4v1/1.%20Cristina%20Popa%20Tache.pdf.

Recommendation of the Committee of Ministers of the Council of Europe No. CM/Rec(2016)5 "On Internet Freedom". (2016). https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2016-5-of-the-committee-of-ministers-to-member-states-on-internet-freedom.

Regulation of the European Parliament and of the Council No. 2016/679 "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive

95/46/EC (General Data Protection Regulation)". (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

Resolution of the General Assembly No. A/HRC/38/L.16 "Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development". (2018). https://digitallibrary.un.org/record/1640460?ln=en&v=pdf.

ROSSINI, C., & GREEN, N. (2021). *Cybersecurity and human rights.* https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf.

SMAILOV, N., KADYROVA, R., ABDULINA, K., URALOVA, F., KUBANOVA, N., & SABIBOLDA, A. (2025). Application of facial recognition technologies for enhancing control in information security systems. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska, 15*(3), 55-58. https://doi.org/10.35784/iapgos.7073.

TADDEO, M., & FLORIDI, L. (2021). The ethics of digital well-being: A thematic review. *Science and Engineering Ethics*, *26*, 2313-2343. https://doi.org/10.1007/s11948-020-00175-8.

TEMIRZHANOVA, L.A., IMANGALIEV, N.K., SYZDYKOV, A.Z., ESHNAZAROV, A.A., & SAGYMBEKOV, B.Z. (2018). Improving the mechanism of countering certain types of fraud in the Republic of Kazakhstan. *Journal of Advanced Research in Law and Economics, 9*(5), 1776-1788. https://doi.org/10.14505//jarle.v9.5(35).33.

TOKZHANOV, Y., KALMAGANBETOVA, D., KUSSAINOVA, A., BAIMOLDINA, S., & SARYBEKOVA, S. (2024). Steganographic Technologies in the Identification of Convicted Persons. *Pakistan Journal of Criminology, 16*(3), 275-294. https://doi.org/10.62271/pjc.16.3.275.294.

UABlocklist. (2024). *At the level of "digital Somalia": Statistics of internet piracy in Ukraine*. https://uablocklist.com/news/na-rivni-tsyfrovoho-somali-statystyka-internet-piratstva-v-ukraini.

United Nations Educational, Scientific and Cultural Organisation (UNESCO). 2024. *Recommendation on the ethics of artificial intelligence.* https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

United Nations Office on Drugs and Crime. (2019). *International human rights and cybercrime law*. https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-human-rights-and-cybercrime-law.html.

VRŠANSKÝ, P., & BEDNÁR, D. (2022). Cyber security and the international law. *Bratislava Law Review*, *1*(2), 38-49. https://doi.org/10.46282/blr.2017.1.2.74.

WESLEY, C. (2020). *The evolving challenge of applying international human rights law to cyberspace.* https://www.mosaicinstitute.ca/evolving-challenge-of-applying-human-rights-law-to-cyberspace.

WHITE, C. (2022). *Cyber security and international law.* https://chriswhitelawyer.com/humanrights-2/.

ZHANDOSSOVA, S.M., SHAUKENOVA, Z.K., KONOVALOV, S.A., KUCHINSKAYA, Y.V., & MUKANOVA, A.Z. (2017). Kazakh and us cooperation in counteracting religious extremism. *Man in India, 97*(6), 171-179.

ZUBOFF, S. (2020). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. https://www.hbs.edu/faculty/Pages/item.aspx?num=56791.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET