UDC 342.7:004.9
DOI: 10.32518/sals2.2025.248

Соціально-правові студії. 2025. Т. 8, № 2
Social & Legal Studios. 2025. Vol. 8, No. 2

Theoretical grounds for defining the criteria to distinguish between digital and traditional human rights: An international legal analysis

Mariia Pleskach*
PhD in Law, Researcher
Mykolas Romeris University
LT-08303, 20 Ateities Str., Vilnius, Lithuania
https://orcid.org/0000-0003-3296-5475

Abstract. The growing influence of digital technologies and the internet on legal systems has raised the urgent need to clearly distinguish between traditional and digital human rights. The purpose of this study was to define theoretical criteria for differentiating these rights within the framework of international legal analysis. The research was based on methods of legal analysis, comparative methodology, and content analysis of scholarly literature, international documents and national legal acts. The study examined the evolution of human rights in the digital age and analysed legal gaps in international and national frameworks. It was found that digital rights differ from traditional rights due to their technological dependence, dynamic content, and the multi-stakeholder structure of legal relations. Key features such as the context of emergence, subject composition, regulatory mechanisms, and objects of protection were identified as criteria for differentiation. It was also revealed that most digital rights emerge from private-law relations and involve actors beyond the state, including transnational corporations and algorithmic systems. The research concluded that current legal doctrine lacks a unified standard for digital rights and that the distinction between digital and traditional rights requires a systematic theoretical basis. It was generalised that new legal standards must be developed to adequately address threats to digital rights, especially in the context of AI, data privacy, and content regulation. The findings of this study can be applied by international organisations, national lawmakers, human rights defenders and academic researchers in the development of coherent and adaptive legal policies for safeguarding rights in digital environments

Keywords: digital rights; online freedoms; international legal standards; digital transformation; cybersecurity; privacy in the digital era

Introduction

As of 2025, the increasing entrenchment of digital technologies across all areas of human life has fundamentally transformed communication, data access, civic participation, and interaction with state authorities. Against this background, the issue of safeguarding human rights in the digital environment has become significantly more complex. The importance of this topic lies not only in the need to adapt existing legal instruments but also in the rethinking of the conceptual foundations of human rights in an age of digital omnipresence. A distinction must now be drawn between those rights that emerged as a response to new digital threats and opportunities, and classical rights formulated in the physical reality of human experience. On the one hand, traditional rights are increasingly being extended into the digital sphere; on the other, a new set of phenomena has arisen that demands separate legal recognition. Therefore, establishing criteria that enable the identification of digital rights as a distinct category is both theoretically significant and practically urgent for the development of effective human rights protection mechanisms in the 21st century.

The issue of human rights transformation in the digital era has become the focus of numerous international and national academic studies. According to N. Ahmad *et al.* (2025), the main challenges in the age of artificial intelligence (AI) include the erosion of privacy, the expansion of surveillance mechanisms, and the discriminatory effects of algorithmic systems, which complicate the exercise of classical rights. The normative differentiation between rights in digital contexts has been addressed by W. Benedek (2025), who proposed a three-stage typology of digital rights development: adaptation of existing rights, emergence of new digital rights, and the introduction of the digital legal subject. From an institutional perspective, A. Brantly (2022) underscored those digital technologies do not merely transform the exercise of rights but also generate new threat vectors, including those related to disinformation and opaque platform governance.

Suggested Citation

Article's History: Received: 08.03.2025 Revised: 15.05.2025 Accepted: 25.06.2025

Pleskach, M. (2025). Theoretical grounds for defining the criteria to distinguish between digital and traditional human rights: An international legal analysis. *Social & Legal Studios*, 8(2), 248-261. doi: 10.32518/sals2.2025.248.

*Corresponding author

E. Celeste *et al.* (2023) examined how platforms increasingly regulate communication through so-called "platform law", a normative system that operates independently of public legal institutions. A. Bon *et al.* (2023) focused on the "digital divide" and introduced the concept of a "digital censor" – the phenomenon where individuals without access to technology are de facto excluded from exercising basic rights. In the studies of M. Baumgärtel and S. Ganty (2024), national frameworks for electronic communications and e-commerce were identified as critical for enabling the realisation of digital rights. Provisions of the Civil Code of Lithuania (2000) and the Civil Code of the Republic of Estonia (2002) show an attempt to integrate digital realities into civil law, but in the absence of coherent theoretical underpinnings, such integration remains fragmented.

The aim of this study was to substantiate the theoretical foundations and to formulate concrete criteria for distinguishing between traditional and digital human rights in the context of international legal frameworks. The objectives included:

1) identifying the core features of digital rights as an autonomous legal phenomenon;

2) systematising scholarly approaches to the classification of human rights in the digital era; and

3) analysing the practical consequences of legal ambiguity surrounding digital rights for national and international human rights mechanisms.

Literature review

Recent legal scholarship has increasingly addressed the evolving relationship between digital transformation and the existing framework of human rights. Scholars have sought to define the limits of traditional legal systems in responding to rapidly advancing technologies that impact individuals' rights in ways previously unanticipated by international law. A significant contribution to this discourse is the work of A. Mantelero (2024), who introduced the concept of the Fundamental Rights Impact Assessment in the context of the EU's Artificial Intelligence Act (2024). Author contends that any high-risk AI system must undergo legal scrutiny to assess its potential human rights implications before implementation. This model emphasizes proactive governance, arguing for the transition from reactive protection to anticipatory legal safeguards. The Fundamental Rights Impact Assessment concept is not only a procedural innovation but also a philosophical shift in the understanding of risk, legitimacy, and responsibility within digital ecosystems. Another foundational perspective is offered by M.K. Land (2019), who analysed the emergence of what she terms "platform law" – a form of pluralistic legal ordering governed not by states but by the internal rules of social media platforms. Researcher argues that these platforms construct their own quasi-legal systems, frequently operating independently of and, at times, in opposition to national and international human rights standards. This raises fundamental questions about legal authority and accountability, as these private actors increasingly mediate access to freedom of expression, privacy, and due process in the digital realm. The tension between public law and corporate rule-making is at the heart of debates concerning the legitimacy and enforceability of digital rights. The multinational report by T. Pajuste (2022) contributes further nuance by mapping out the core threats posed by digital technologies to the existing human rights regime. These include algorithmic opacity, mass data surveillance, manipulation of information through AI-driven tools, and the erosion of legal certainty. The authors argue that existing legal instruments, including the Universal Declaration of Human Rights (1948) and the European Convention on Human Rights (1950), offer only limited guidance in addressing these challenges. Their work calls for a new legal architecture capable of navigating cross-border governance, platform responsibility, and evolving conceptions of identity and autonomy in the digital space. In particular, they advocate for the establishment of transnational monitoring mechanisms to identify digital rights violations and ensure cross-jurisdictional accountability.

In a more practical and technical vein, P. Pathak (2025) investigated the covert installation of Android's SafetyCore application on millions of mobile devices. The incident, involving no prior user consent or notification, highlighted a regulatory vacuum in addressing corporate actions that affect users' privacy and autonomy. Author's analysis revealed the ways in which digital platforms bypass traditional consent models, exploiting terms of service to implement surveillance technologies. The SafetyCore case stands as a paradigm of how legal norms surrounding notice, consent, and control are insufficiently adapted to the digital environment. It also raises important questions about the private origins of digital normativity, often divorced from democratic deliberation or legal accountability. C.E. Popa Tache and C.S. Săraru (2024) broaden this discussion by examining the triangulated relationship between digital transformation, corporate governance, and international law. Their analysis highlights those digital rights are increasingly shaped not only by states but by transnational corporate entities that participate in global norm-setting. They emphasise that legal scholars and regulators must account for the hybrid character of digital regulation, where private companies, international organisations, and national legal systems interact in complex and often asymmetrical ways.

B. Farrand (2025) explored how digital rights are reshaping intellectual property regimes, arguing that digitalisation blurs the boundaries between private and public rights and renders existing classifications obsolete. The study highlights how digital rights challenge established legal categories, requiring a reconfiguration of concepts such as ownership, authorship, and usage rights in the age of blockchain, streaming, and algorithmic distribution. In a complementary approach, C.H. Kan (2024) examined the dual legal nature of digital human rights, distinguishing between those rights that have emerged directly due to technological advancements and those that are digital extensions of traditional rights. The study calls for a differentiated typology of digital rights and argues that failure to distinguish between these categories creates confusion in legislative and judicial interpretation.

Materials and methods

This study was grounded in a purely theoretical legal framework and does not involve empirical data collection, case law analysis, or legislative application. The methodology draws upon doctrinal legal research, conceptual reasoning, and a critical review of contemporary academic and normative sources related to the classification of digital rights. The study relied on a systematic review of 48 academic, normative, and institutional sources published primarily between 2019 and 2025. The literature included peer-reviewed articles, international legal documents, and analytical reports issued by

academic institutions and intergovernmental organisations. A purposive sampling approach was applied to ensure conceptual rigor and temporal relevance. Sources that offered descriptive overviews without analytical depth were excluded.

The study applied a range of theoretical methods. The hermeneutic method was used to interpret transformations in core legal concepts such as rule of law and human dignity in the digital context. Logical and semantic analysis allowed for the distinction of interrelated legal categories, such as legality and legitimacy. Comparative doctrinal analysis was employed to contrast theoretical perspectives across legal traditions and jurisdictions. Content analysis was used to identify recurring themes and structural patterns in legal doctrine and theory. Discourse analysis enabled the identification of normative and rhetorical strategies shaping the field of digital constitutionalism. The research also relied on typologisation and conceptual modelling, particularly in constructing the taxonomy of digital rights and their legal characteristics.

In addition to scholarly publications, a range of normative instruments was consulted as conceptual baselines. These included the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), the European Convention on Human Rights (1950), and the Convention on the Rights of the Child (1989). Special attention was also given to regional legislative instruments that address digital governance and personal data protection, such as the General Data Protection Regulation (2016), the Artificial Intelligence Act (2024). The legislation of the client's country was analysed, in particular the Law of the Republic of Lithuania No. XIII-1120 "On Electronic Identification and Trust Services for Electronic Transactions" (2018), which regulates the legal framework for digital identity and electronic commerce. These were not examined as normative rules for application but as illustrative frameworks that reflect the evolution of legal thinking. Institutional and policy-based declarations were likewise integrated, including the European Declaration on Digital Rights and Principles for the Digital Decade (2022) and the Global Digital Compact (2023) and the decisions provided in cases Getty Images v. Stability AI (2025) and Mata v. Avianca, Inc. (2023), which illustrate new legal dilemmas in the application of traditional doctrines to AI-generated outputs. These documents provided insight into emerging consensus on digital rights at the international level, even in the absence of binding legal definitions.

Results and Discussion

Specific features of the legal nature of digital human rights. Traditional human rights and digital rights share a common goal – securing the opportunities and extent of individual freedom – yet they differ considerably in terms of the spheres of their application and the methods via which they are realised in the modern world. Traditional human rights, enshrined in international instruments such as the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966), focus on the protection and safeguarding of human rights in the material world, particularly the right to life, liberty, equality before the law and personal inviolability. These rights have historically formed the foundation of legal systems and cover the most crucial aspects of human existence, without which the physical functioning of a democratic society would be impossible.

However, the rapid development of digital technologies and the globalisation of the virtual environment have compelled human rights organisations, governments and international institutions to address new challenges related to the emerging legal phenomenon of digital human rights. Digital rights, such as the right to access the internet, the protection of personal data and freedom of expression in the digital environment, have already become essential for ensuring legal protection for citizens in the modern world, which is particularly relevant in the context of the rapid digitisation of the banking sector. For example, as the O. Kolodiziev *et al.* (2021) shows, the introduction of digital innovations not only determines the competitiveness of banks, but also leads to the active use of personal data and online platforms, which in turn increases the importance of digital rights in the legal regulation of banking activities. Thus, the transformation of banks into digital ecosystems creates a need for a balance between the efficiency of digital services and the observance of basic user rights in the digital environment. However, these rights are not clearly defined in international law and often remain outside the scope of traditional legal norms. This is due to the fact that international legal documents, such as the Universal Declaration of Human Rights, were created in an era when the internet and other digital technologies did not yet exist in the form that familiar with today.

A distinctive feature of digital rights is their dependence on and relation to emerging technologies, which have the potential to radically alter the ways in which people interact with information. Currently, legal systems in different countries face challenges in ensuring the protection of digital rights. In some countries, particularly countries that are members of the EU, progressive legal mechanisms such as the General Data Protection Regulation (2016) have already been established to regulate the protection of personal data and ensure users' rights to privacy in the digital space. In contrast, there are many other countries that lack clear laws aimed at protecting human rights on the Internet. This creates legal uncertainty, which consequently makes users vulnerable to abuses such as unauthorised surveillance, data collection without consent and violations of privacy.

Currently, legal doctrine offers no direct guidance on how to distinguish between digital and traditional rights. Instead, it emphasises the principles of universality and non-discrimination in terms of human rights, which should apply to all forms of their realisation, including digital rights. International law does not yet have clearly defined and universally accepted standards for distinguishing digital and traditional rights, although some developments have occurred. For example, the European Declaration on Digital Rights and Principles for the Digital Decade (2022) attempts to address the new digital reality by enshrining within it the key principle that "what is illegal offline is illegal online". However, the question arises as to whether the approach of applying the "doctrine of the equivalence of human rights in online and offline space" is justified and sufficiently grounded. Currently, most international treaties and legal acts still focus on the material aspects of human rights, rather than their digital manifestations. This highlights the importance of amending existing legal norms and developing specific international standards for the protection of digital rights, as only in this way can harmony be ensured between the observance of human rights and technological progress. In the context of the need to develop digital rights that would

effectively protect the interests and needs of citizens in the digital age, it should be noted that the protection of human rights in cyberspace cannot be ensured solely through existing international human rights law. Existing rights require adaptation and supplementation with new digital rights to ensure the effective protection of individual rights in the digital world. The recognition of emerging digital human rights is evidenced by the formalisation of specific guarantees such as the right to access the Internet and the right not to be subject to automated decision-making. The United Nations Human Rights Council (2021) has affirmed that the same rights people enjoy offline must be protected online, explicitly emphasising Internet access as a prerequisite for exercising freedom of expression and participation in modern society. Complementing this, Article 22 of the General Data Protection Regulation (2016) establishes the individual's right not to be subject to decisions based solely on automated processing, including profiling, when such decisions have legal or significant effects. Further normative developments have been articulated by the Y. Shany (2022), which conceptualises a human-centric digital rights framework, advocating for the legal recognition of a "right to a human decision-maker" to ensure transparency, accountability, and fairness in algorithmically governed processes. This situation is primarily due to the fact that the criteria for distinguishing digital rights from traditional human rights remain unclear. As a result, this negatively impacts the development of a more practical mechanism for their protection.

A study by S. Demeke (2024) is insightful, stating that digital technologies directly or indirectly influence almost all aspects of private and public life. Human rights face new challenges and threats, and their content, scope and understanding are changing considerably in the digital age. The conceptual changes involve the fact that the scope of recognised fundamental rights is changing in unpredictable ways, the boundaries between physical and digital actions are gradually blurring and, as a result, the application of traditional criteria to such activities ceases to be relevant. Human rights are no longer embedded in existing theoretical structures and legal doctrines, and "digital rights" are gaining increasing salience.

Analysis of doctrinal sources and scholarly works demonstrates that many researchers focus on developing their own lists or classifications of digital rights without providing sufficient justification for why specific rights should be categorised as digital. Scholars who have attempted to catalogue digital rights offer heterogeneous and often mutually inconsistent taxonomies. A. Mantelero (2024) anchors his list in the risk-based logic of the Fundamental Rights Impact Assessment, dividing rights into those threatened by "high-risk" and "limited-risk" AI systems. Although the model is technologically sensitive, it conflates the source of risk with the nature of the right: access-to-internet, data-portability and transparency appear side by side without a shared doctrinal denominator, making the catalogue hard to transpose beyond the AI-governance context. W. Benedek (2025) distinguish three "generations" of digital rights – adapted, new and prospective – yet leave the transition thresholds undefined. Because the same right (for instance, data protection) may be "adapted" in one jurisdiction and "new" in another, their matrix reproduces the very boundary problem it seeks to solve. G. Malgieri and C. Santos (2025) proposes a pragmatic checklist – right to digital identity, right to cybersecurity, right to digital heritage and so on – but offers no criteria for inclusion beyond empirical salience. The resulting inventory is exhaustive in appearance yet conceptually eclectic; several entries (e.g., digital education) describe policy goals rather than rights in the strict legal sense. M.K. Land (2019) groups rights around the notion of "platform law", treating content governance rules as sui generis digital rights. This platform-centric lens illuminates private-ordering problems but obscures public-law obligations; it also labels corporate terms of service as "rights", thereby blurring the line between contractual privileges and universal entitlements. E. Celeste *et al.* (2023) frames digital rights within "digital constitutionalism", differentiating participatory, informational and procedural clusters. Yet the scheme rests on constitutional rhetoric without clarifying whether the clusters are distinct rights, principles or interpretive canons, which weakens its normative precision. Finally, B. Farrand (2025) treats digital rights as a subsection of intellectual-property law, carving out "digital authorship" and "algorithmic creativity". While this sectoral focus reveals important collisions, it neglects non-proprietary dimensions such as autonomy or equality, resulting in a partial and discipline-bound taxonomy. Taken together, these classifications illustrate the field's terminological dispersion, the absence of shared inclusion criteria and the tendency to merge technological descriptors with legal categories – shortcomings that continue to hinder the formation of a coherent, standardized catalogue of digital human rights.

A similar observation was made by G. Malgieri and C. Santos (2025), who described "new rights" (both new in essence and new manifestations of fundamental human rights): the right to access the Internet, the right to digital education and the development of digital skills, the right to digital identity, the right to cybersecurity, the right to protection from misinformation, the right to the protection of personal data, the right to access digital public services, the right to freedom of content creation and protection and the right to digital heritage (the right to digital freedom and the right to be forgotten). However, the criteria for classifying this list of rights as "new" are not entirely clear.

These discussions lead to the conclusion that to classify a specific right as digital, it is necessary to determine not only how this right differs from classical (traditional) rights but also its legal nature and why it should receive special status in the legal world. This question is crucial for establishing a clear legal framework that will allow these rights to be protected at the international level, as different jurisdictions may approach the regulation of digital rights differently. Scholars should focus not only on creating a list of digital rights but also on a deeper exploration of the theoretical foundations that allow a particular right to be classified as digital. This approach will help foster a clearer understanding of digital rights and ensure their correct application in different legal systems. To achieve a consistent and enforceable system of digital human rights, it is essential to analyse the current state of national legal systems that continue to rely on traditional legal instruments to regulate digital relations. Many states have not yet developed autonomous legal frameworks for digital rights and instead attempt to extend classical civil or administrative law norms into the digital environment, which is particularly noticeable during the transformation of the public administration system in the current crisis conditions. As noted by O. Krasivskyy (2023),

the digitisation of public services has accelerated significantly, but this institutional modernisation has not been accompanied by a corresponding update of legal approaches to the protection of digital rights. Therefore, legal practice often involves the mechanical transfer of traditional civil or administrative law norms to new digital realities without proper adaptation to the specifics of digital environments. This approach creates risks of legal uncertainty for citizens and requires a conceptual understanding of digital rights as an independent area of regulation.

This approach leads to legal uncertainty and insufficient protection of rights specific to cyberspace. One example is the Civil Code of Ukraine (2003). Despite the emergence of multiple legal relations in the digital sphere – such as digital identity verification, algorithmic decision-making, and personal data governance – the Code still defines the grounds for civil rights and obligations based solely on traditional notions: transactions, law-prescribed acts, and general legal principles. Article 11 of the Code establishes a closed list of grounds for legal relations, including contracts and events, but fails to recognise digital interaction or automated decision-making systems as independent legal phenomena. This omission becomes critical in cases involving the misuse of algorithms or the breach of platform-based obligations, where the parties' digital conduct does not fully align with established contractual or delictual models. Similarly, the Civil Code of the Republic of Lithuania (2000), while progressive in certain civil matters, also lacks clear provisions on digital rights. Article 1.136 provides a list of sources for the emergence of civil obligations, such as contracts, law, or custom. However, it does not mention digital consent, algorithmic processing, or terms-of-service-based interactions that are now widespread in online communication and commerce. In practice, this forces courts to interpret internet-related disputes through analogies with classical civil obligations, which may not adequately reflect the nature of decentralised or automated digital conduct. Another illustrative case is Public Information Act of the Republic of Estonia (2000), which governs access to public data but lacks a dedicated section on the rights of individuals to digital privacy, digital literacy, or algorithmic transparency. Estonia is often praised for its digital governance model, yet its foundational legislation remains focused on access, not control or accountability in digital interactions. As a result, while digital infrastructure is advanced, the legal system has not caught up in terms of individual rights within the algorithmically mediated public domain.

These examples reflect a broader trend in which national legal systems extend existing analog-world doctrines into the digital space rather than developing new normative categories. This results in several consequences: rights are often defined in material rather than informational terms; enforcement mechanisms are reactive and poorly adapted to the speed of digital harm; and individuals lack effective redress for violations that originate in automated, transnational or platform-governed environments. Therefore, the absence of direct recognition of digital rights – such as the right to algorithmic transparency, the right to be forgotten, or the right to fair platform governance – in foundational legal acts of civil law systems underscores the need for explicit codification and doctrinal innovation. Without this, the regulation of digital relations remains fragmented, relying on analogical reasoning and subject to the interpretive discretion of courts, rather than grounded in proactive, rights-based legislative design. This indicates that, although digital rights are gaining increasing importance, most legal systems still lack clearly defined provisions specifically addressing digital rights and continue to adapt existing civil law norms to the new conditions.

Currently, in European countries, most types of human activity in cyberspace are primarily regulated by traditional civil law norms, which have been adapted to regulate this type of activity. A high proportion of legal relations in cyberspace falls under civil law regulation, including online contract formation for purchasing goods in e-commerce stores, protection of intellectual property rights, information security, protection of personal data, provision of software services and development, legal protection of websites and content, and registration and protection of copyrights and trademarks online (Urtaiev, 2022).

The grounds for the emergence of rights and obligations of subjects of civil legal relations are established at the level of national legislation (civil codes). For example, in Lithuania, Article 1.136 of the Civil Code of the Republic of Lithuania (2000) sets out the grounds for the emergence of civil rights and duties. It states that rights and duties shall emerge from the grounds established by this Code and other laws, in addition to actions performed by persons and organisations which, although not determined by laws, create civil rights and duties within the general principles and the meaning of the civil laws. Article 5 of the Civil Code of the Republic of Estonia (2002) established that civil rights and duties arise from transactions, events specified by law and other acts that the law links to the creation of civil rights and obligations, as well as from unlawful acts.

The ability of modern technologies to integrate data and provide prompt access to these data changes the usual models of interaction and transforms traditional tools for the realisation of subjective rights (Vachhani, 2024). In particular, most digital rights, interests and needs of today's individuals are realised in private-law relationships. For example, the right to access the Internet is implemented between the end user of electronic communication services and the electronic communication service provider. According to the Law of the Republic of Lithuania No. XIII-1120 (2018), contractual relations in the field of electronic services are based on the provider's obligation to ensure the availability and secure delivery of such services – particularly when it comes to the processing and transmission of data in digital environments. The user, in turn, is required to fulfil payment obligations and comply with the agreed conditions for service use. Digital rights, including the right to personal data protection in cyberspace, constitute a core component of these legal relationships and are embedded within broader contractual and regulatory frameworks. In the context of electronic commerce, the use of personal data is permissible only when the commercial actor implements effective measures to guarantee its protection, thereby ensuring lawful and transparent data processing in accordance with both national and EU legal requirements. As stipulated in Article 6 of the Law, parties engaged in electronic transactions are obliged to ensure the confidentiality and protection of personal data obtained through electronic means, in accordance with the requirements of relevant data protection legislation, including the General Data Protection Regulation (2016).

The private nature of digital human rights is also emphasised in a study by M. Susi (2019). He notes that a characteristic of digital rights is that they are ensured not only through the international normative architecture of human rights but also through norms created by electronic communication service providers (e.g., digital platforms and technology giants). He argues that in cases where a digital platform "reserves the right to ultimately determine whether its rules have been violated", this reflects a fundamental difference between digital and traditional rights. He refers to the possibility of using terms such as "Lex Facebook", which indicates the private nature of the origin of digital human rights.

Thus, digital human rights emerge as a response to the rapid development of technology and its penetration into all areas of life. They have specific aspects related to the interactions between humans and the digital environment and are predominantly characterised by a private-law nature of dual character: the digital rights themselves and the extension of traditional rights to the digital environment. Distinguishing between digital rights, traditional rights and rights that are extensions of traditional rights is crucial for understanding how human rights evolve in the context of technological advancements. Purely digital rights are rights that have emerged as a result of the development of digital technologies and would have no real meaning without the digital environment. They came about with the growing influence of the Internet, mobile technologies, big data and AI. Examples of these rights include the right to access the Internet, the right to access digital services, and the right to cybersecurity protection against cyber threats, such as hacking and malware. In other words, technological progress itself has created new types of threats that did not exist in the traditional physical world.

All other digital rights are an expansion of the scope of existing traditional rights into new conditions, where an increasing number of aspects of lives occur in the online space. For example, the right to freedom of expression on the Internet represents a reinterpretation of the traditional right to freedom of expression, as enshrined in Article 10 of the European Convention on Human Rights (1950). In the digital environment, this right extends to the ability to freely express one's views via the Internet, for example in blogs or on social networks.

It is clear that the criteria for defining digital rights need to be reconsidered in a legal context. The insights of W. Benedek (2025) are useful here. They observed that the development of digital human rights can be viewed through three conditional generations of evolution. The first generation of digital human rights focused on adapting existing human rights to the conditions of the digital age. The second generation involves the introduction of new digital rights that address specific needs and interests in the online space, which traditional rights cannot fully encompass. A potential third generation could introduce new right-holders and duty-bearers, including the concept of a digital persona, which would impose legal obligations on private technology companies. Together, these three generations could create a comprehensive human rights system capable of effectively protecting individual needs and interests in the online environment.

Criteria for distinguishing between digital and traditional human rights. To distinguish digital rights from traditional human rights in a meaningful and applicable way, it is necessary to define a coherent set of criteria that clarify the legal nature of each category. Such differentiation enables more precise interpretation and implementation of rights within contemporary legislative frameworks and enforcement practices. These criteria should reflect not only the origin and technological context of digital rights but also their functional divergence from classical rights in terms of protection mechanisms, subject scope, and normative objectives. By establishing clear parameters for comparison, the legal system can more effectively integrate emerging digital entitlements into existing human rights architecture without eroding the foundational principles of either.

The context of the emergence of the respective right is first and foremost among such criteria. Traditional human rights are fundamental, universal rights and freedoms that are integral to human dignity and provide protection against discrimination, violence and the abuse of power. These rights have been formulated and enshrined through the historical development and evolution of legal norms that apply to every individual, regardless of nationality, gender, age, religion or other characteristics. According to the Icelandic Human Rights Centre, they include civil, political, social and cultural human rights. The formation of international standards for traditional human rights has become a crucial process that ensures fundamental rights and freedoms for individuals at a global level. Thanks to numerous international agreements, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (1966), the Convention on the Rights of the Child (1989), the International Convention on the Elimination of All Forms of Racial Discrimination (1965), the Convention on the Elimination of All Forms of Discrimination against Women (1979), the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984) and other international agreements, human rights standards have become the foundation for the development of the modern global legal system. They guarantee that all individuals, regardless of nationality, race, religion or other characteristics, have the right to life, liberty and dignity.

In contrast, digital rights, in their own essence, emerged as a result of the development of digital technologies, prior to which they did not exist. These rights would have been meaningless or impossible without technological progress. An example of this is the right to access the Internet. The extension of traditional human rights into the digital environment refers to rights that are a direct consequence of adapting traditional human rights to the digital context. For example, the right to privacy, which was traditionally associated with physical spaces (such as the inviolability of the home and the confidentiality of correspondence), now extends to the protection of personal data in the online environment. Similarly, the right to freedom of expression has also undergone a major transformation in the digital space. As noted by R. Spano (2021), the Internet in its current form is unique in that it offers instant access to diverse content for anyone who can afford relatively low-cost connectivity. This allows individuals to share their views, ideas and opinions, creating equal opportunities for communication. These advances have had a profound impact on freedom of expression, which has been a fundamental element of international human rights since its inclusion in Article 19 of the Universal Declaration of Human Rights (1948). In other words, to practically apply the criterion of the context of the emergence of a right to determine whether a specific right is

traditional, purely digital or a digital extension of a traditional right, it is necessary to identify the period in which the right emerged and also to ascertain whether its creation (or transformation) is directly linked to technologies or innovations.

The dynamic nature of the content of rights, as a second criterion, is manifested as follows. Traditional rights are relatively stable, as they are formed based on widely accepted principles in the physical world. Their development occurs gradually within structured processes that depend on changes in social, political and economic conditions. The three generations of rights (civil, economic, and social and cultural rights), each of which developed based on the previous ones, reflect certain stages in the evolution of legal ideals.

Unlike traditional rights, digital rights develop much more rapidly and more unevenly as technologies are constantly changing. These are rights that emerge in conditions of rapid technological advancement and have no analogues in the traditional legal context. For example, the right to access Internet resources or the right to protection from manipulation through new technologies, such as fake news and automated bots. The emergence of digital technologies has triggered a wide range of legal, social and ethical issues that often lack definitive legal solutions. A notable example is the case of Mata v. Avianca, Inc. (2023), where a lawyer submitted a legal brief generated by ChatGPT that included fictitious judicial decisions. The court sanctioned the attorney for failing to verify the authenticity of the sources, thereby raising concerns about the professional responsibility of legal practitioners using generative AI tools. Another illustrative case is Getty Images v. Stability AI (2025), in which Getty accused Stability AI of unlawfully scraping millions of copyrighted images to train its Stable Diffusion model. The High Court of Justice in the UK allowed the case to proceed, indicating the judiciary's growing recognition of the complexities surrounding intellectual property and data use in AI training. These cases underscore the inadequacy of traditional legal frameworks in addressing the novel challenges posed by AI-generated content, authorship attribution, and data provenance in machine learning contexts. In other words, these rights can be a direct consequence of advances in new technologies, and at the time of their emergence, they did not exist in the traditional legal context. This includes the right to digital assets and the right to a digital identity, both of which are closely tied to the development of blockchain technologies. In general, if a right arises as a result of the need to adapt to rapidly occurring technological changes that have no analogues in traditional law, such a right can be considered a genuine digital right.

The specific subject structure of legal relations for the realisation of digital rights is the third criterion for differentiation. All individuals are equal in terms of their fundamental rights, meaning that every individual is a bearer of fundamental rights to an equal extent. This means that a person cannot be denied rights based on their gender, ethnicity, language, religion or other characteristics. Limitations based on these characteristics violate human rights and are considered discrimination. Traditional rights are natural, inalienable and non-transferable, meaning they cannot be taken away, and an individual cannot renounce them. A distinctive feature of participants in legal relations regarding the exercise of digital rights is that, in addition to their traditional legal capacity, which consists in the ability to possess civil rights and exercise them independently, elements of technical and educational preparedness are added, which directly correlates with the idea of legal paternalism in the regulation of digital rights. As shown in the study by I. Patricheeva (2025), modern European legislation, in particular the GDPR, introduces both hard and soft forms of paternalistic regulation, which are designed to protect individuals in conditions of limited digital competence. In other words, legal capacity in the field of digital rights increasingly depends not only on formal legal status, but also on the ability of the subject to act consciously in the information environment. In this context, technical ignorance and a lack of digital education serve as grounds for justified regulatory intervention aimed at protecting individuals from digital risks, even if this means restricting their autonomy. This approach demonstrates a conceptual shift towards paternalistic law, where the intellectual and technical capacity of the subject becomes the criterion for determining the limits of legal protection. This is because an individual who lacks basic knowledge about the functioning of the digital environment and the Internet will be unable to fully exercise their digital rights. In other words, modern technologies that integrate data and provide rapid access to it change traditional models of interaction, transforming familiar institutions and fundamental categories. Thus, when entering into private relations in the digital environment, participants face new challenges that did not exist in traditional models of legal relations before the digital era. In this sense, can speak of a "technological and educational censor" when exercising digital rights. This technological and educational censor effectively excludes from legal relations individuals who are unable to use the internet to meet certain needs and interests or to access digital services. This leads to what is known as the "digital divide", where in poorer regions or countries, many people lack access to digital services and content, which hinders their participation in the information society and impedes development (Bon *et al.*, 2023). This means that the inability to use digital technologies can limit an individual's access to many modern services and opportunities. This can significantly impact participation in contemporary economic, social and political life, as many essential functions today are carried out through digital channels: communication, shopping, medical services, online education and more. In this context, can even speak of a shift from "digital rights" to "digital duties", as requirements for citizens to make full use of digital technologies. This is reflected in their ability to protect their data, work with online resources and actively participate in digital civic processes, among other activities. Furthermore, this emphasises the importance of ensuring equal access to digital resources, education and support for those who lack sufficient experience or opportunities to use digital technologies, as well as the need to develop adequate legal standards for the protection of digital rights that meet today's requirements.

Another feature of the implementation of digital rights is that the legal relationships in this sphere are always characterised by multi-subjectivity. In addition to participants who interact directly (for example, users among themselves or users and electronic commerce entities), the realisation of digital rights also involves the presence of additional actors. These actors, although they do not initiate legal relations, exert both normative influences (as they establish the rules for usage) and technical influence, as they can control the network, change connection parameters and affect

technical aspects of a network. Such actors include, for example, providers of electronic communication services and moderators of digital online platforms. E. Celeste *et al.* (2023) argue that many such actors play a role in translating human rights norms – which comprise the "DNA" of modern constitutionalism – into rules that align with the context of managing digital rights, particularly online content. Today, transnational companies that own and manage social media platforms are becoming dominant actors alongside state authorities.

The fourth criterion refers to the objects of legal protection (the objects to which digital rights apply). Traditional human rights concern fundamental goods (values) that are guaranteed to individuals in the material world (environment), meaning they originated in the context of the physical world and aim to protect individuals in real life from physical infringements on their freedom, property, life and dignity. The objects of digital rights are fundamental goods with which individuals enter into legal relations specifically in the digital environment. While in traditional human rights the objects of rights include property, material things, actions, and both material and immaterial goods, in the context of digital rights, these objects can change due to technological advances, particularly the development of the Internet.

C.H. Kan (2024) found that the main object of digital rights is information, which can be accessed, shared, stored and more, but specifically due to the existence of the Internet. In other words, the focus is not only on information as such but also on information that is limited by the existence of the digital space. Information is the primary object of digital rights because it can be accessed, stored, transmitted and processed electronically using various technologies. This encompasses personal data, i.e., all information related to an individual, such as their name, address, email, phone number, search history, identification numbers, etc. The protection of personal data raises issues of confidentiality and the right to privacy. Content, in the form of all types of information that is created, transmitted, or processed in a digital format, is also included. This can include text, images, videos, audio, software, websites, e-books, databases, etc. This content is subject to protection by copyright, intellectual property rights and other norms. Digital identity is also a key object of digital rights, as it defines an individual's identity in the electronic environment. It includes various data that enable user identification in the digital world, ranging from usernames and passwords to biometric characteristics, such as fingerprints or features recognised by facial recognition systems. Digital identity not only provides access to various online services but also enables transactions and interactions with both government and private institutions and ensures the protection of personal data in the digital environment. Digital assets, also referred to as digital property, are another object of legal protection in the context of digital rights. These include cryptocurrencies and other forms of digital currencies and tokens, as well as intellectual property, which encompasses patents, software code, trademarks and other digital products. These assets can be subject to both civil and criminal legal protection, necessitating specialised legal regulation in this area. With the development of Web 2.0, cyberspace has become an environment where numerous threats to the security of both individual users and organisations are possible (Kharchenko *et al.*, 2017). Therefore, cybersecurity, as a non-material asset, can also be considered an object of digital rights. Digital services should also be included in the objects of legal regulation, as they encompass a wide range of activities conducted via the internet. These include Internet access services; Internet services, such as communication platforms including social networks, messenger services, email and cloud storage services; e-commerce services, including online stores, trading platforms, online banking services and financial services; and entertainment and media services, such as streaming platforms, online gaming platforms, e-books and educational courses.

The fifth criterion of distinction is the sphere of application (implementation) of rights. Traditional rights are directly related to the material aspects of an individual's life, including their interactions with other people, society and the state. In contrast, digital rights focus on the interactions of individuals with virtual spaces, digital resources, platforms and technologies, or interactions with other people, society and the state through the use of information technologies. These rights are implemented through specific types of social relations that arise, change and terminate within cyberspace (digital space). In other words, the development of digital technologies creates the conditions for the transformation of traditional private legal relations, which has led to the emergence of a system of digital rights that requires additional regulation and a review of the mechanisms for their protection.

A. Pandey and A. Mishra (2025) noted that the realisation of digital rights occurs in relationships that cannot be classified as purely legal or factual relationships. These are social connections of a special legal, informational and technical nature. The distinctive feature of the legal relationships in which digital rights are realised is that information exchange occurs in electronic form; the actors exercising their rights and obligations are distanced from each other in space; digital rights are realised with the use of software, technical standards and protocols. The social relations arising from the use of global computer networks are unique informational relations. The particularity of these relations lies in the presence of a technical component (the realisation of which takes place through digital technologies), the informational content of the objects of these relations and the unique composition of the actors involved.

The sources of threats that exist to a particular right comprise the next criterion for distinguishing the types of rights examined in this article. Violations of traditional rights are primarily carried out through physical violence, discrimination, unlawful detention or restrictions on human rights, among other means. A study by A. Brantly (2022) showed that digital technologies create new forms of human rights violations that are exclusively digital, as well as transferring old forms of violations from the physical world into the virtual one. It is important to note that these technologies are also capable of returning violations from the virtual space to the physical one, causing considerable harm to human rights. Violations of digital rights are often particularly dangerous, as they infiltrate individuals' personal spaces that were once free from surveillance mechanisms available to governments, companies or even other citizens. Rights that were once clearly protected are increasingly becoming subject to service terms, algorithmic design and new approaches to the protection of previously guaranteed rights. As a result, human autonomy in the digital environment is increasingly turning from a right into a privilege, secured either by financial payments for services provided by companies or

complex security practices implemented by individuals. Through algorithms, networks, and data collection and analysis, as well as platforms that alter the rules of the game, the situation is becoming increasingly complex.

Violations of digital rights may, at first glance, seem less obvious (e.g., without physical violence), but they can have serious consequences for individuals. The sources of threats to digital human rights are primarily linked to the technologies themselves, particularly the development of AI, as these technologies are not neutral. This manifests, for example, in cyberattacks, theft of personal data, illegal surveillance of internet users, censorship and information manipulation (for example, fake news and propaganda).

In general, any virtual interaction or legal relationship in the digital sphere cannot be considered secure due to potential inaccuracies in information, data breaches, malfunctions of digital services and other similar issues. Remote transactions within civil relationships require placing personal data and banking details on an online platform and sharing them with the platform owner and a potential counterparty, which creates conditions for the improper use of this information. Moreover, the possible anonymity of the counterparty and the inability to apply traditional methods of verifying their identity and the offered resources can raise doubts both about the actual existence of the counterparty and the authenticity of any information provided, as well as about the proper fulfilment of any arising obligations in the future. Essentially, when entering into legal relationships through digital technologies, individuals are often forced to rely on the accuracy of information and the good faith of the digital service provider who participates in establishing and implementing the legal ties (Urtaiev, 2022).

A study by T. Pajuste (2022) highlighted the real and potential dangers that technologies may pose, noting that technologies once thought to help ensure human rights can be used by both state and non-state actors to achieve the opposite. Technologies can be employed for the surveillance of citizens and the spread of disinformation, which could potentially diminish public trust in scientific data and knowledge, for example. AI is now used daily in various ways, including in decision-making within both public and private sectors, which could pose significant threats to human rights. Research has shown that AI can be biased and may not always ensure fair outcomes in all cases. AI can also conceal and diminish accountability for potential human rights violations, as it is not easily adaptable to traditional mechanisms of holding violators accountable. For example, in 2022, Russia launched an extensive disinformation network known as Pravda, which employed AI and chatbots to disseminate propaganda across 49 countries. According to a study conducted by NewsGuard, the network aggregated content from pro-Kremlin sources and used large language models to spread fabricated news narratives. This manipulation, referred to as "large language models grooming," significantly affected the reliability of chatbot outputs, with false claims generated by the network being reproduced in 33% of tested AI responses (Fried, 2025). Some large language models, such as ChatGPT, have started reproducing these manipulations, quoting fake materials and posing a threat to users who may receive false information. In Europe, the adoption of the European Artificial Intelligence Act (2024) has significantly improved the situation in this area. In particular, the requirements for data quality for high-risk AI systems are regulated in Article 10 of this law: "High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such data sets are used". However, the AI Act does not regulate issues related to the verification of information sources, detection of fake news or disinformation, or mechanisms for user reporting. These remain under the framework of other regulations, such as the Digital Services Act, which governs online platforms. In the future, the AI Act may be supplemented with requirements to combat the manipulation of information and the dissemination of fake news, particularly for platforms that generate content. This will necessitate increased transparency of AI models and clear mechanisms for monitoring the use of AI to detect any manipulations or unacceptable content.

The infringement of digital rights manifests in diverse and increasingly sophisticated forms that evolve in parallel with the rapid advancement of technology. These violations may involve unauthorized data collection, algorithmic discrimination, surveillance overreach, manipulation of digital identities, or unjustified content restrictions, each presenting unique legal and ethical challenges. Given the fluidity of digital environments and the pace at which new platforms and systems are introduced, the identification of threat sources cannot rely on static legal instruments. Instead, it requires a flexible and anticipatory legal framework that responds to emerging risks in real time. This, in turn, necessitates the continuous improvement of both regulatory standards and law enforcement practices, including the development of adaptive compliance mechanisms, cross-sectoral cooperation, and the incorporation of technological expertise into legal analysis. Without such a dynamic approach, legal systems risk falling behind the realities of digital transformation and becoming ineffective in upholding fundamental rights in the digital sphere.

The seventh criterion for distinguishing rights is normative regulation. Traditional human rights are regulated within traditional legal systems and have a well-established legislative framework (including national legislation and international treaties and conventions). The legal nature of the digital space and the legal relations in which digital rights are realised distinguishes them from the existing legal system, creating an autonomous system that requires the development of its own method and regulatory mechanism. Digital rights are heterogeneous in their legal nature; they are constantly evolving and becoming more complex, which directly impacts the nature of their legal regulation, which is particularly relevant in the field of information protection in electronic registers. As noted by N. Mentukh & O. Shevchuk (2023), legal regulation of information security cannot remain static, as the complexity of digital rights requires a dynamic approach to legal mechanisms for the protection of personal data and privacy. As of 2025, there is no unified legal standard that consolidates the rules establishing the key principles for ensuring digital human rights. Such a legal standard for digital human rights should be comprehensive, considering various aspects of the digital environment and technologies, as well as ensuring effective protection of human rights in an ever-changing world. Currently, certain digital rights are enshrined in various normative legal acts at the national and international levels. In

particular, the right to access the Internet is primarily regulated at the level of national legislation of individual countries. For example, Public Information Act of the Republic of Estonia (2000) regulates access to public information, including digital rights related to online content. In the EU, the General Data Protection Regulation (2016) ensures the protection of personal data in cyberspace, setting standards for privacy and data security. Laws such as the AI Act and the Digital Services Act regulate specific aspects of digital rights concerning protection from disinformation and manipulations in the digital space, ensuring transparency of algorithms (such as content moderation) and combating harmful digital practices.

Another distinctive feature of the legal regulations and legal sources in which digital human rights are enshrined is that they often have a "private character", as technology companies on the Internet set their own platform usage requirements, which they may interpret at their discretion in light of general human rights provisions. These are sometimes referred to as "platform policies", forming what is known as "platform law", which is defined as a system of norms governing communication on the Internet through private platforms rather than public authorities. Platforms such as social networks establish their own rules regarding content; these rules may be either publicly available or hidden. Even when these rules are not disclosed or are kept secret, platform law continues to operate, as platforms effectively act as intermediaries in regulating the Internet. An example of such "private regulation" can be seen in the case of Google's installation in 2025, without user consent, of the Android System SafetyCore app on millions of Android devices, which scans photos to filter 18+ content. While SafetyCore is intended to enhance user security by filtering sensitive content, its automatic installation and lack of transparency raised concerns. One of the most controversial aspects was that SafetyCore was installed without warning on devices running Android 9 and newer versions. This app was automatically installed on users' devices without their knowledge and has virtually unrestricted access to the entire system on such devices. This opens up the possibility that Google could gain access to almost everything on a user's phone without their knowledge or consent, creating a dangerous precedent. There are no guarantees that the app will not scan personal photos, videos or other files (Pathak, 2025).

Tech giants, by establishing content and usage policies based on their own values (primarily commercial), face criticism for unilaterally setting the rules for their virtual spaces, significantly deviating from international human rights law. However, even relying solely on existing laws is not an optimal solution, as social networks are global spaces with users from different countries, and the question of which national law should take precedence raises concerns about digital imperialism. International human rights law also does not provide the ultimate solution, as it requires further interpretation to be applied to online moderation and the digital space. For example, until 2018, Meta claimed that it was not bound by international human rights law (Weng, 2024). However, following major legislative changes in the EU, with the adoption of the Digital Services Act, it introduced a corporate human rights policy that includes a commitment to comply with international norms and discuss the balance between the platform's internal standards and external human rights standards. It is entirely reasonable to agree with the statement by E. Celeste *et al.* (2023) that there is an urgent need for the establishment of a more comprehensive human digital rights standard created by the international community and formalised into treaties through a multistakeholder process. This would help bridge the gap between companies that actively protect human rights in their operations and those that do considerably less.

At the same time, the networked nature of the Internet and the conflicting interests of states often diminish the importance of rights in digital matters. M.K. Land (2019) argues that one of the main problems in the legal regulation of digital human rights and the establishment of a universal standard will remain the issue of jurisdictional conflicts between countries. For example, France is attempting to force Google to comply with European data protection laws globally, while Canada's Supreme Court has deemed it necessary to unilaterally remove websites of intellectual property infringers. At the same time, US courts oppose such decisions, as they could contradict American laws that protect intermediaries from liability for content transmission. This situation creates challenges in regulating the Internet at the international level. The protection of digital rights and the regulation of the Internet largely depend on the political structures and models present in different countries. A. Brantly (2022) identified five distinct "Internets" that vary in terms of openness, control and regulation, depending on the country in which they developed. Among these are the Silicon Valley Open Internet, the Brussels Bourgeois Internet, the DC Commercial Internet, the Beijing Paternal Internet and the Moscow Spoiler Internet. In A. Brantly's (2022) analysis, each of the five visions of the internet presents a unique set of policy and regulatory challenges. All of this confirms the hypothesis about the specific nature and complexity of digital rights, which necessitates a combination of international and national legal regulation and imperative and dispositive norms, demonstrating the complex and fragmented nature of digital rights.

An equally important criterion for distinguishing rights is the mechanism (method) of protection of rights and methods of monitoring violations. Traditional human rights have a well-established model for challenging rights violations through legal and political mechanisms, for example, through national courts or international bodies. Traditional human rights are typically protected through state institutions (such as courts, the police and government bodies), as well as international human rights organisations (such as the UN and the European Court of Human Rights).

Monitoring is carried out through local and international bodies, but it often depends on national political will. In the offline sphere, human rights form an interconnected system, where the effectiveness of each component relies on other components. The changes arising from the division between offline and online raise concerns about the consistency of the offline system when applied to the Internet, casting doubt on whether offline tools are suitable for addressing legal issues in the digital environment (Susi, 2019). The implementation of digital human rights requires a special approach to protection through specific technological tools, such as encryption systems, anti-censorship technologies and data protection monitoring tools. It also involves the engagement of international human rights mechanisms, particularly the United Nations Human Rights Council (2021), which has adopted multiple resolutions affirming that the

rights protected offline must also be protected online, and the development of initiatives such as the Global Digital Compact, aimed at safeguarding human rights in the digital age. Challenging violations of rights in the digital environment can be much more complex than in the offline world due to various technical barriers. Access to legal protection mechanisms online is crucial, such as for combating censorship in cyberspace and ensuring access to fair mechanisms for personal data protection. As the digital environment is more complex and dynamic than the offline environment, protection mechanisms in this context are often not as clearly defined or accessible, which is particularly evident in the field of social networks, where the speed of personal data circulation and the volume of information processed significantly complicate privacy control. S. Yevseiev *et al.* (2021) show that the risks of data leakage or unauthorised use increase significantly due to the human factor, the vulnerability of IoT devices and the imperfection of cloud services. The effectiveness of personal data protection directly depends on the level of user trust in the information and the systems that process it. Thus, the vagueness of legal protection mechanisms in the digital environment is exacerbated by the fact that users themselves do not have sufficient guidance on the level of security and reliability of the digital platforms on which they operate. This indicates the need for not only technical but also legal modelling of protection mechanisms that would take into account the variable nature of trust and the complexity of digital social structures. In other words, the uncertainty regarding the criteria for what should be considered a violation of digital rights is an additional obstacle to improving the protection mechanisms for digital rights. In many cases, there are no clear standards for what constitutes a violation of digital rights. This can lead to situations where some violations go unnoticed or are ignored due to the lack of a clear legal framework, accountability and sanctions.

The specificity of implementing digital rights also lies in the fact that fundamental principles of traditional human rights, such as transparency, accessibility and predictability, lose their general functionality in relation to online human rights. While transparency in the offline environment means that individuals can understand why certain outcomes regarding their ability to exercise human rights are what they are, typically through the analysis of judicial decisions, regulations, laws or other documents related to their specific situation, in the digital rights context, problems can arise due to the lack of transparency, for example when online companies gain access to the moderation of user-generated content. Transparency in the protection of individual human rights is replaced by statistical data about the outcomes of similar online conflicts of rights or values. Accessibility includes both access to regulatory principles, which are positive rights, and the availability of legal protection in the event of a potential violation. However, when it comes to protecting rights in the online environment, individuals often do not know where to find the relevant regulations, if they even exist. In the case of traditional human rights protection, there are no such issues. However, the application of legal remedies in the online context remains highly debatable, whether through judicial proceedings or through a certain platform in an extrajudicial manner, and which norms should be applied. Furthermore, digital rights protection is characterised by "multistakeholderism", meaning that states "shift" some of their obligations for human rights protection onto private entities. Nevertheless, the question of how legal remedies should function in the online environment remains complex and unsettled. It is still unclear whether such remedies should be pursued through formal judicial systems, alternative dispute resolution mechanisms, or internal procedures established by digital platforms. As noted by M. Susi (2019), the protection of digital rights increasingly involves a multistakeholder model, where traditional state responsibilities are redistributed among various private actors, particularly technology companies. This redistribution not only redefines the allocation of duties in safeguarding human rights but also leads to a transformation in how standards are created and enforced – shifting normative authority away from public institutions and toward transnational corporate entities.

Conclusions

The distinction between digital and traditional human rights is rooted in their origin and the nature of the social and technological conditions that gave rise to them. Digital rights have emerged as a necessary legal response to the profound societal changes driven by the digitalisation of communication, the development of AI, and the algorithmisation of everyday interactions. These rights were not foreseen in the classical human rights paradigm, which was developed in response to threats existing in the material, institutionalised world. As a result, digital rights differ not only in their object of regulation but also in their structural characteristics, implementation conditions, and normative justification. Although digital rights often interact with and extend traditional rights, they represent a separate legal phenomenon that requires specific regulatory treatment. One of the fundamental differences is the technological dependency of digital rights. These rights arise and function only within the digital environment and have no relevance outside of it. Unlike traditional rights, which apply regardless of technological context, digital rights are inseparable from the infrastructures that enable them. Furthermore, digital rights are marked by high dynamism of content; their scope and meaning continuously evolve in response to technological shifts. This dynamic nature contrasts with the relative stability of traditional human rights, which have maintained core definitions over decades of international legal development. The implementation of digital rights also presupposes a particular structure of legal subjectivity. Realisation of such rights is possible only when individuals possess not only formal legal capacity but also a minimum level of technological competence and access. This introduces an additional dimension of inequality and highlights the need for considering the so-called digital divide in human rights discourse. Another crucial factor is the specificity of the legal objects protected. Digital rights focus on immaterial and data-driven assets such as personal information, digital identity, algorithmic transparency, and cybersecurity. These objects are not only novel in the legal sense but also volatile, often existing across jurisdictions and outside traditional state regulation. Accordingly, the legal mechanisms for protecting such rights are often fragmented, involving a mix of national laws, international frameworks, and internal policies of digital platforms.

In contrast, traditional rights are supported by constitutional guarantees and binding international treaties, with established enforcement mechanisms through national courts and international human rights bodies. The absence

of equivalent legal architecture in the digital sphere creates asymmetry between the recognition of digital rights and their practical enforceability. The nature of threats to digital rights also differs substantially. While traditional rights are typically endangered by physical coercion or legal restrictions imposed by the state, digital rights face threats from algorithmic bias, commercial surveillance, platform censorship, and the uncontrolled dissemination of personal data. These threats often remain invisible to the affected individuals and may originate from private actors rather than public authorities, thereby complicating the legal accountability framework. The normative regulation of digital rights remains largely underdeveloped. Many jurisdictions continue to address digital harms through analogical application of civil or administrative law without recognising the distinctive features of digital rights. Foundational legal documents such as civil codes and information laws often fail to define rights such as access to digital infrastructure, protection from algorithmic decision-making, or the right to transparency in data use, despite the growing importance of such issues in contemporary society.

In this context, it becomes clear that the development of effective legal standards for the protection of digital rights requires a conceptual framework capable of addressing these distinctions. Legal systems must move beyond treating digital rights as derivatives of classical categories and instead recognize them as a complex and evolving phenomenon shaped by the interaction of legal norms, technological affordances, and platform governance. The absence of such a framework risk reducing digital rights to discretionary privileges dependent on private regulation rather than enforceable legal entitlements. Consequently, the clarification and theoretical grounding of digital rights are not only a matter of academic interest but a prerequisite for ensuring justice, accountability, and human dignity in the digital era.

Acknowledgements

The author would like to thank the Research Council of Lithuania (Lietuvos mokslo taryba) for their financial support in this research and Mykolas Romeris University. This work was supported by the Research Council of Lithuania (Lietuvos mokslo taryba) (grant number P-PD-23-170).

Funding

The study was not funded.

Conflict of interest

None.

References

[1] Ahmad, N., Ali, A.W., & Yussof, M.H. (2025). The challenges of human rights in the era of artificial intelligence. *UUM Journal of Legal Studies*, 16(1), 150-169. doi: 10.32890/uumjls2025.16.1.9.

[2] Approved Judgment of the High Court of Justice Business and Property Courts of England and Wales Intellectdual Property in the Case No. IL-2023-000007 “Getty Images v. Stability AI”. (2025, January). Retrieved from https://www.judiciary.uk/wp-content/uploads/2025/01/Getty-Images-and-others-v-Stability-AI-14.01.25.pdf.

[3] Artificial Intelligence Act. (2024, July). Retrieved from https://artificialintelligenceact.eu/the-act/.

[4] Baumgärtel, M., & Ganty, S. (2024). On the basis of migratory vulnerability: Augmenting article 14 of the European Convention on Human Rights in the context of migration. *International Journal of Law in Context*, 20(1), 92-112. doi: 10.1017/S174455232300037X.

[5] Benedek, W. (2025). International organizations and digital human rights. In B. Wagner, M.C. Kettemann, K. Vieth-Ditlmann & S. Montgomery (Eds.), *Research Handbook on human rights and digital technology* (pp. 310-324). Cheltenham: Edward Elgar Publishing. doi: 10.4337/9781035308514.00025.

[6] Bon, A., Saa-Dittoh, F., & Akkermans, H. (2023). Bridging the digital divide. In H. Werthner, C. Ghezzi, J. Kramer, J. Nida-Rümelin, B. Nuseibeh, E. Prem & A. Stanger (Eds.), *Introduction to digital humanism* (pp. 283-298). Cham: Springer. doi: 10.1007/978-3-031-45304-5_19.

[7] Brantly, A. (2022). Utopia lost – human rights in a digital world. *Applied Cybersecurity & Internet Governance*, 1(1), 1-19. doi: 10.5604/01.3001.0016.1238.

[8] Celeste, E., Palladino, N., Redeker, D., & Yilma, K. (2023). *The content governance dilemma: Digital constitutionalism, social media and the search for a global standard.* Cham: Palgrave Macmillan. doi: 10.1007/978-3-031-32924-1.

[9] Civil Code of the Republic of Estonia. (2002, March). Retrieved from https://www.riigiteataja.ee/akt/106122010012.

[10] Civil Code of the Republic of Lithuania. (2000, July). Retrieved from https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.107687?positionInSearchResults=1&searchModelUUID=c68a6ba6-0c7a-44be-b440-d9c054eca329.

[11] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15#Text.

[12] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. (1984, December). Retrieved from https://surl.lu/qlnrem.

[13] Convention on the Elimination of All Forms of Discrimination against Women. (1979, December). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women.

[14] Convention on the Rights of the Child. (1989, November). Retrieved from https://surl.li/hcnwfs.

[15] Demeke, S. (2024). A human rights-based approach for effective criminal justice response to human trafficking. *Journal of International Humanitarian Action*, 9(1), article number 4. doi: 10.1186/s41018-023-00143-4.

[16] European Convention on Human Rights. (1950, November). Retrieved from https://www.echr.coe.int/documents/d/echr/convention_ENG.

[17] European Declaration on Digital Rights and Principles for the Digital Decade. (2022, January). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0028.

[18] Farrand, B. (2025). Online platforms, intermediary responsibility, and human rights: Digital copyright as a site of multiple contestations in the EU. In B. Wagner, M.C. Kettemann, K. Vieth-Ditlmann & S. Montgomery (Eds.), *Research handbook on human rights and digital technology* (pp. 54-68). Cheltenham: Edward Elgar Publishing. doi: 10.4337/9781035308514.00010.

[19] Fried, I. (2025). *Exclusive: Russian disinformation floods AI chatbots, study finds*. Retrieved from https://www.axios.com/2025/03/06/exclusive-russian-disinfo-floods-ai-chatbots-study-finds.
[20] General Data Protection Regulation. (2016, April). Retrieved from https://gdpr-info.eu/.
[21] Global Digital Compact. (2023). Retrieved from https://www.un.org/global-digital-compact/en.
[22] International Convention on the Elimination of All Forms of Racial Discrimination. (1965, December). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial.
[23] International Covenant on Civil and Political Rights. (1966, December). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
[24] Kan, C.H. (2024). Artificial intelligence (AI) in the age of democracy and human rights: Normative challenges and regulatory perspectives. *International Journal of Eurasian Education and Culture*, 9(25), 145-166. doi: 10.35826/ijoecc.1825.
[25] Kharchenko, V., Ponochovnyi, Y., Qahtan, A.-S.M., & Boyarchuk, A. (2017). Security and availability models for smart building automation systems. *International Journal of Computing*, 16(4), 194-202. https://doi.org/10.47839/ijc.16.4.907.
[26] Kolodiziev, O., Krupka, M., Shulga, N., Kulchytskyy, M., & Lozynska, O. (2021). The level of digital transformation affecting the competitiveness of banks. *Banks and Bank Systems*, 16(1), 81-91. doi: 10.21511/bbs.16(1).2021.08.
[27] Krasivskyy, O. (2023). Specific features of public involvement and digitalization of services when reforming public administration during the war. *Democratic Governance*, 16(1), 12-23. doi: 10.23939/dg2023.01.012.
[28] Land, M.K. (2019). The problem of platform law: Pluralistic legal ordering on social media. *SSRN*. doi: 10.2139/ssrn.3454222.
[29] Law of the Republic of Lithuania No. XIII-1120 "On Electronic Identification and Trust Services for Electronic Transactions". (2018, April). Retrieved from https://surl.li/ruwggx.
[30] Malgieri, G., & Santos, C. (2025). Assessing the (severity of) impacts on fundamental rights. *Computer Law & Security Review*, 56, article number 106113. doi: 10.1016/j.clsr.2025.106113.
[31] Mantelero, A. (2024). The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. *Computer Law & Security Review*, 54, article number 106020. doi: 10.1016/j.clsr.2024.106020.
[32] Mentukh, N., & Shevchuk, O. (2023). Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy and Security*, 1(1), 4-17.
[33] Opinion and Order on Sanctions of the United States District Courtsouthern District of New York in Case No. 1:22-cv-01461 "Mata v. Avianca, Inc.". (2023, June). Retrieved from https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1%3A2022cv01461/575368/54/.
[34] Pajuste, T. (2022). *Specific threats to human rights protection from the digital reality*. Tallinn: Tallinn University. doi: 10.13140/RG.2.2.17192.85760.
[35] Pandey, A., & Mishra, A. (2025). Conflict and coexistence of human rights: An exploratory study with reference to intellectual property rights. *Journal of Human Rights and Social Work*, 10, 43-54. doi: 10.1007/s41134-024-00361-9.
[36] Pathak, P. (2025). *What is Android System SafetyCore and why did it appear on your phone?* Retrieved from https://allthings.how/what-is-android-system-safetycore-and-why-did-it-appear-on-your-phone-2.
[37] Patricheev, I. (2025). Legal paternalism's influence on the balancing data protection and fundamental rights. *Law Journal of the National Academy of Internal Affairs*, 15(1), 48-58. doi: 10.63341/naia-chasopis/1.2025.48.
[38] Popa Tache, C.E., & Săraru, C.S. (2024). Evaluating today's multi-dependencies in digital transformation, corporate governance and public international law triad. *Cogent Social Sciences*, 10(1), article number 2370945. doi: 10.1080/23311886.2024.2370945.
[39] Public Information Act of the Republic of Estonia. (2000, November). Retrieved from https://www.fao.org/faolex/results/details/en/c/LEX-FAOC049697/.
[40] Shany, Y. (2022). *From digital rights to international human rights: The emerging right to a human decision maker*. Retrieved from https://www.oxford-aiethics.ox.ac.uk/blog/digital-rights-international-human-rights-emerging-right-human-decision-maker.
[41] Spano, R. (2021). *Freedom of expression and media freedom in the light of the case law of the ECHR*. Retrieved from https://www.echr.coe.int/documents/d/echr/Speech_20210618_Spano_ERA_conference_European_media_law_ENG.
[42] Susi, M. (2019). *Human rights, digital society and the law: A research companion*. London: Routledge. doi: 10.4324/9781351025386.
[43] United Nations Human Rights Council. (2021). *Resolution on the promotion, protection and enjoyment of human rights on the Internet*. Retrieved from https://www.article19.org/resources/un-human-rights-council-adopts-resolution-on-human-rights-on-the-internet/.
[44] Universal Declaration of Human Rights. (1948, December). Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights.
[45] Urtaiev, O. (2022). Peculiarities of regulation of legal relations in the field of IT law. *Law Herald*, 6, 233-239. doi: 10.32782/yuv.v6.2022.28.
[46] Vachhani, S.J. (2024). Networked feminism in a digital age – mobilizing vulnerability and reconfiguring feminist politics in digital activism. *Gender, Work & Organization*, 31(3), 1031-1048. doi: 10.1111/gwao.13097.
[47] Weng, Z. (2024). Digital human rights from the perspective of system theory – concept definition, social function, and constitutional basis. *Human Rights*, 4, 69-101.
[48] Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., & Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. *EUREKA, Physics and Engineering*, 2021(1), 24-31. doi: 10.21303/2461-4262.2021.001615.

Теоретичні засади визначення критеріїв розмежування цифрових і традиційних прав людини: міжнародно-правовий аналіз

Марія Плескач
Кандидат юридичних наук, науковий співробітник
Університет Миколаса Ромеріса
LT-08303, вул. Атейтіс, 20, м. Вільнюс, Литва
https://orcid.org/0000-0003-3296-5475

Анотація. Зростаючий вплив цифрових технологій та Інтернету на правові системи викликав нагальну потребу в чіткому розмежуванні традиційних і цифрових прав людини. Метою цього дослідження було визначення теоретичних критеріїв для розмежування цих прав у рамках міжнародно-правового аналізу. У дослідженні були використані методи правового аналізу, порівняльно-правового методу та контент-аналізу наукової літератури, міжнародних документів і національних правових актів. Було розглянуто еволюцію прав людини в цифрову епоху та проаналізовано правові прогалини в міжнародному та національному законодавстві. Було виявлено, що цифрові права відрізняються від традиційних прав через їхню технологічну залежність, динамічний зміст та багатосторонню структуру правовідносин. Критеріями диференціації визначено такі ключові ознаки, як контекст виникнення, суб'єктний склад, механізми регулювання та об'єкти захисту. Також було виявлено, що більшість цифрових прав виникають з приватноправових відносин і залучають суб'єктів поза межами держави, включаючи транснаціональні корпорації та алгоритмічні системи. Дослідження дійшло висновку, що сучасній правовій доктрині бракує єдиного стандарту цифрових прав, а розмежування між цифровими та традиційними правами потребує систематичного теоретичного підґрунтя. Узагальнено, що необхідно розробити нові правові стандарти для адекватного реагування на загрози цифровим правам, особливо в контексті штучного інтелекту, конфіденційності даних та регулювання контенту. Результати дослідження можуть бути застосовані міжнародними організаціями, національними законодавцями, правозахисниками та науковцями при розробці послідовної та адаптивної правової політики щодо захисту прав у цифровому середовищі

Ключові слова: цифрові права; свободи в Інтернеті; міжнародні правові стандарти; цифрова трансформація; кібербезпека; приватність у цифрову епоху