https://doi.org/10.38044/2686-9136-2025-6-10

ESSAYS

PROTECTING HUMAN RIGHTS IN THE DIGITAL AGE: LEGAL FRAMEWORKS AND MEDIA LITERACY AS A COMPLEMENTARY SAFEGUARD

Nour Nfissi

Autonomous University of Barcelona
Carrer de la Vinya, Bellaterra, Barcelona, Spain, 08193

Abstract

The expansion of digital technologies has reshaped the exercise of fundamental rights, prompting growing scholarly and regulatory attention to the notion of digital human rights. As digital platforms increasingly structure communication, access to information, and social participation, existing legal categories face conceptual and practical strain. While some accounts portray digital rights as a straightforward extension of classical human rights, others emphasize their transformative impact on constitutional principles, enforcement mechanisms, and the distribution of power between public authorities and private actors. This paper situates digital rights within contemporary academic debates and emerging regulatory frameworks in order to clarify their normative scope and conceptual boundaries. It advances the argument that digital rights cannot be adequately understood through purely legal or purely technological lenses. Instead, they emerge at the intersection of constitutional law, digital governance, and public policy, where regulatory instruments, institutional design, and educational strategies jointly shape the conditions for rights protection. The analysis highlights the constitutional paradox of digital platforms, which exercise functions traditionally associated with public authority while remaining only partially subject to democratic accountability and judicial oversight. Drawing on European constitutional principles, supranational regulation, and policy initiatives, the study demonstrates how current legal frameworks seek to respond to private digital power while revealing their structural limits in data-driven and algorithmic environments. At the same time, scholarship on Media and Information Literacy is mobilized to show how citizens' informational capacities function as a normative complement to legal safeguards, enabling individuals to exercise their rights meaningfully rather than merely formally. By integrating legal doctrine, public policy analysis, and MIL, this article contributes a coherent analytical framework for understanding digital rights as a hybrid normative construct. It concludes that the effective protection of digital rights depends not only on legal guarantees and regulatory enforcement, but also on policy choices that strengthen individual and collective capacities within the digital public sphere.

Keywords

digital human rights, cybersecurity, digital law, data protection, legal framework, media and information literacy

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.

For citation Nfissi, N. (2025). Protecting human rights in the digital age: Legal frameworks and media literacy as a complementary safeguard. *Digital Law Journal*. https://doi.org/10.38044/2686-9136-2025-6-10

Submitted: 8 July 2025, accepted: 15 Aug. 2025

ЭССЕ

ЗАЩИТА ПРАВ ЧЕЛОВЕКА В ЦИФРОВУЮ ЭПОХУ: ПРАВОВЫЕ ОСНОВЫ И МЕДИАГРАМОТНОСТЬ КАК ДОПОЛНИТЕЛЬНАЯ ГАРАНТИЯ ИХ ОСУЩЕСТВЛЕНИЯ

Н. Нфисси

Автономный университет Барселоны
08193, Испания, Барселона, Беллатерра, Пласа Сивика

Аннотация

Распространение цифровых технологий изменило осуществление прав человека, что привело к росту внимания ученых и регулирующих органов к понятию цифровых прав человека. Поскольку цифровые платформы все больше структурируют коммуникацию, доступ к информации и социальное взаимодействие, существующие правовые категории сталкиваются с концептуальными и практическими трудностями. В то время как некоторые исследования представляют цифровые права как прямое продолжение классических прав человека, другие подчеркивают их преобразующее воздействие на конституционные принципы, механизмы обеспечения соблюдения прав и распределение власти между государственными органами и частными субъектами. В данной статье цифровые права рассматриваются в контексте современных академических дискуссий и формирующихся нормативных рамок с целью уточнения их нормативного охвата и концептуальных границ. В ней выдвигается аргумент о том, что цифровые права не могут быть адекватно поняты исключительно с юридической или исключительно технологической точки зрения. Вместо этого они возникают на пересечении конституционного права, цифрового управления и государственной политики, где регулирующие инструменты, институциональный дизайн и образовательные стратегии совместно формируют условия защиты прав. Автор подчеркивает конституционный парадокс цифровых платформ, которые выполняют функции, традиционно связанные с государственной властью, оставаясь при этом лишь частично подлежащими демократической подотчетности и судебному надзору. Опираясь на европейские конституционные принципы, наднациональное регулирование и политические инициативы, исследование демонстрирует, как правопорядки реагируют на цифровую власть частных субъектов, одновременно выявляя свои структурные ограничения в средах, основанных на данных и алгоритмах. В то же время используются исследования в области медиа- и информационной грамотности, чтобы показать, как информационные возможности граждан функционируют в качестве нормативного дополнения к правовым гарантиям, позволяя людям осуществлять свои права осмысленно, а не просто формально. Интегрируя правовую доктрину, анализ государственной политики и медиа- и информационную грамотность, эта статья предлагает целостную аналитическую основу для понимания цифровых прав как гибридной нормативной конструкции. В заключение делается вывод,

что эффективная защита цифровых прав зависит не только от правовых гарантий и правоприменения, но и от политических решений, которые укрепляют индивидуальные и коллективные возможности в цифровой публичной сфере.

Ключевые слова

цифровые права человека, кибербезопасность, цифровое право, защита данных, правовое регулирование, информационная грамотность

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Нфисси, Н. (2025). Защита прав человека в цифровую эпоху: правовые основы и медиаграмотность как дополнительная гарантия их осуществления. *Цифровое право*. https://doi.org/10.38044/2686-9136-2025-6-10

Поступило: 08.07.2025, принято в печать: 15.08.2025

Introduction

Digital human rights encompass all the fundamental rights and essential protections to which users are entitled when engaging with digital platforms. They include both traditional human rights—such as freedom of expression and access to information— and new forms of rights.

This paper's claim that a new generation of rights, commonly referred to as digital rights, should be delineated due to profound digital transformations of society. However, it would be a significant overstatement to assert that these rights are entirely separate from traditional human rights; rather, they represent their extension and adaptation to the digital sphere: they are bound to them by indissoluble ties of shared principles.

The corpus of digital rights should include, among others, the right to privacy online, the right to control one's personal data, the right to access reliable digital information, the right to digital literacy, and the right to protection from algorithmic discrimination.

In the digital era, these rights have already become essential to ensuring that individuals can fully participate in social, economic, and political life while preserving their autonomy and dignity. Their recognition and protection are now central to any legal system that seeks to uphold fundamental rights in a technology-driven world.

At the same time, the digital revolution has introduced a new wave of digital threats that pose serious and complex risks to well-known human rights, such as privacy, equitable access to information, and the existing principles of exploitation personal data.

These threats make the protection of digital human rights by their theoretical and practical recognition more crucial than ever, and a robust legal and regulatory framework governing digital spaces is vital for understanding the mechanisms that ensure compliance with fundamental rights and democratic values.

In this context, the intersection between human rights and digital spaces raises a wide range of questions. How has the digital revolution reshaped the interpretation and application of fundamental human rights? In what ways do digital technologies challenge the enforcement of rights such as

privacy, freedom of expression, and access to information? What challenges and threats do they face in the digital age? What is the legal and practical significance of international instruments and conventions in regulating digital platforms and protecting users? What are the normative foundations of digital rights, and how should they guide legal regulation? Beyond legal measures, what educational and media literacy strategies can empower individuals to understand and assert their digital rights? And how can educational tools contribute to the protection of human rights within broader legal strategies?

This research aims to provide an overview comprehensive of how the digital revolution has transformed the interpretation and application of fundamental human rights. In the course of this study, I will address some of the questions outlined above, explore the complex challenges posed by digital technologies, particularly regarding privacy, freedom of expression, and access to information, as well as examine the emergence of new categories of digital rights.

Through a normative analysis of international human rights instruments, the study assesses their practical relevance in regulating digital platforms and safeguarding users. It also considers the theoretical foundations of digital rights, advocating for a regulatory approach that is both legally sound and socially responsive. In doing so, it integrates educational and media literacy strategies as complementary tools that empower individuals to understand, exercise, and protect their digital rights within a broader legal and democratic framework.

Digital Human Rights in the General Context: Insights from History and Legal Scholarship

In the 21st century, digital technologies have become an inseparable part of everyday human experience. The internet, social media, and digital platforms are now essential tools for communication, education, governance, and civic participation. As societies increasingly move into digital spaces, the exercise and protection of human rights are being redefined in real time.

Contextualizing human rights in the digital age therefore requires more than a mere technical update of legal texts; it calls for a deep reflection on how human dignity and freedom are being reshaped by technological forces. This reflection must also include an examination of the historical development of human rights and the ways in which they have adapted or struggled to adapt to successive waves of technological change. Furthermore, understanding the practical application of new digital human rights is essential. Finally, this discussion must remain sensitive to multicultural perspectives, recognizing that the interpretation and implementation of digital rights are influenced by cultural, political, and socio-economic contexts.

The Historical Background: From Classical to Digital Human Rights

The foundational principles of human rights were first formally articulated in the Universal Declaration of Human Rights of 1948.[1] However, the understanding and scope of these rights have evolved significantly over time, particularly following the development of the theory of the "generations of human rights, which provided a nuanced classification and expansion of rights concept in response to emerging social, political, and technological realities.

The evolution of human rights has often been viewed through the lens of the "three generations" theory developed by the French jurist Karel Vasak. Karel Vasak's late-1970s classification proposed that human rights evolved in three successive waves, ranging from civil and political freedoms to socio-economic guarantees and collective entitlements. Today, scholars question whether this model

[1] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

still reflects the complexity of contemporary rights frameworks (Domaradzki et al., 2019, pp. 424-425). The so-called "first generation" encompasses civil and political rights, such as freedom of expression and the right to privacy (Domaradzki et al., 2019, p. 424). The "second generation" includes economic, social, and cultural rights, while the "third generation" refers to collective and solidarity rights, including the right to development and the right to a healthy environment (Domaradzki et al., 2019, 425).

Vasak's tripartite model later influenced scholarly and institutional debates on the development of human rights. However, only the first two generations of rights he identified are reflected in the Universal Declaration of Human Rights,[2] whereas the third generation emerged gradually in later instruments of a declaratory character, such as the Stockholm Declaration[3] and the Rio Declaration.[4]

During the latter half of the 20th century, the first forms of digital human rights began to emerge. In Europe, the development of digital human rights started at the national level, led by pioneering countries such as Sweden and West Germany (Dowd, 2022, p. 72).

Sweden was the first to take the lead, enacting the world's first data protection law in 1973 (Dowd, 2022, p. 81). This law was designed to regulate the use of computers to ensure the protection of personal data and safeguard individuals' privacy. The core aim of Sweden's Data Act was to protect citizens' personal data from misuse and to ensure that the growing use of computerized systems did not infringe upon individual privacy rights.[5] As Lee Bygrave observes, Swedish data protection law has operated under a very stringent individuation requirement (Bygrave, 2002, p. 47).

A similar development took place in Germany, where a data protection law was introduced to safeguard personal privacy through the principles of data minimization and purpose limitation. The first national multimedia law in Germany was adopted in 1997 to regulate the internet and online services, setting out the conditions for information and communication services and harmonizing state media laws (Wuermeling, 1998, pp. 41–44).

Spiros Simitis, a Greek-German jurist and the principal pioneer of data protection and digital law, is widely regarded as the father of data protection in Germany. His work established the conceptual and normative foundations of data protection, emphasizing that it is not merely an administrative or technical issue, but a fundamental right tied to the preservation of human dignity (Schwartz, 2025, p. 111).

Simitis argues that data protection must encompass normative dimensions beyond mere technical control, particularly in the field of employment (Simitis, 1999). He also develops a conceptual framework in which data protection becomes an indispensable component of democratic societies undergoing rapid digital transformation (Schwartz, 2025, pp. 105–106.)

The concrete efforts of Sweden and Germany in developing security and data protection policies later influenced European digital frameworks and laid the groundwork for national initiatives in countries such as France and Spain.

In 1978, France adopted a law aimed at regulating the increasing use of data within both public and private sectors[6]. Following its adoption, France established the National Commission on Informatics

[2] Ibid.

[3] Declaration of the United Nations Conference on the Human Environment, June 16, 1972, U.N. Doc. A/CONF.48/14 (1972).

[4] Rio Declaration on Environment and Development, June 14, 1992, U.N. Doc. A/CONF.151/26 (Vol. I) (1992).

[5] DATALAG (Svensk författningssamling [SFS] 1973:289) (Swed.). See the English translation available at: https://www.worldlii.org/int/other/NDPrivLegis/1973/1.pdf

[6] Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Jan. 7, 1978, p. 227.

and Liberties (*Commission nationale de l'informatique et des libertés*, *CNIL*), an independent administrative authority empowered to oversee compliance, safeguard citizens' privacy, and ensure that data processing respected fundamental freedoms. This piece of legislation was a landmark act that laid the foundations for modern data protection in Europe. It was particularly significant because it explicitly recognized that the regulation of personal data was not merely a technical or administrative matter, but one directly tied to the preservation of civil liberties and fundamental rights (Dowd, 2022, pp. 185–187).

In the late 20th century, Spain adopted its first comprehensive legal framework on data protection through the enactment of Organic Law 5/1992 of 29 October on the Regulation of the Automatic Processing of Personal Data.[7] In response to the growing use of computerized systems for data collection, storage, and processing, Spain introduced a legal framework in 1992 designed to regulate the protection of personal data and limit potential misuse (Dowd, 2022, p. 185).

Over time, the European Union has remained at the forefront of digital regulation, continuously adapting to new technological challenges and innovations in the digital age. The digital era has brought about conceptual transformations in the content, understanding, implementation, and protection of human rights (Razmetaeva et al., 2022, pp. 55–56). Accordingly, this first part seeks to explore the real impact of digital technologies on users and human rights, as well as the emergence of new forms of human rights—digital human rights—within the technological and digital domain.

The Place of Digital Human Rights in Contemporary Legal Thought

The emergence of digital rights has become a prominent topic in contemporary legal scholarship, reflecting the growing intersection between technology and fundamental rights. Scholars have debated how traditional constitutional, human rights, and international law frameworks should adapt to the challenges posed by the digital environment.

For instance, Balkin (2004, p. 47) argued that existing constitutional rights—such as freedom of expression and privacy—should be reinterpreted to encompass digital contexts rather than replaced by entirely new legal categories.

According to Floridi, the digital revolution has reconfigured the "infosphere," transforming the conditions of informational privacy and personal identity; this conceptual shift suggests the need to reinterpret traditional rights, such as the right to privacy, in light of modern technologies (Floridi, 2005, pp. 185–188). And yet, it seems, that the reinterpreting approach was also supported by scholarship. As Hildebrandt argues, smart-technologies increasingly "invalidate previous forms of legal protection" by enabling profiling and control that current law cannot adequately address. In her book she further demonstrates how data-driven agency threatens traditional rights such as privacy, identity, due process and calls for a reconfiguration of legal guarantees under the conditions of a data-driven society (Hildebrandt, 2015, pp. 77–90; 186–200).

Constitutional Law Perspectives

Constitutional law has traditionally served as the cornerstone for the protection of fundamental rights within national legal systems. With the advent of the digital age, however, constitutional frameworks face unprecedented challenges, as rights originally conceived for the offline world must be reinterpreted and adapted to new technological realities. Issues such as data protection, online privacy, freedom of expression on digital platforms, and equal access to digital infrastructures have

[7] Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal [Organic Law on the Regulation of Automated Processing of Personal Data; L.O.R.T.A.D.], (B.O.E. 1992, 262) (Spain).

raised the question of whether existing constitutional guarantees remain sufficient or whether new, explicitly recognized concept of "digital rights" is needed.

This intersection between constitutional law and digital rights has given rise to the notion of digital constitutionalism, which highlights the role of constitutional principles in regulating the digital environment and safeguarding individual freedoms in cyberspace (De Gregorio, 2022, pp. 1–25). The rapid expansion of digital technologies has challenged traditional constitutional frameworks, prompting scholars to reconsider how fundamental rights can be effectively protected in online environments.

Several European scholars have made significant contributions to the theoretical and constitutional understanding of digital rights in the age of algorithmic governance. For instance, Oreste Pollicino, in his research, introduced the concept of the "constitutionalization of the Internet" within the European context. He argues that as private digital platforms increasingly perform functions traditionally carried out by public authorities, constitutional safeguards—particularly those concerning democracy and pluralism—must be extended into the digital sphere. While Mireille Hildebrandt highlights the profound implications of algorithmic systems for constitutional guarantees. She examines how data-driven environments undermine classical legal safeguards by shifting regulation from ex-ante legal norms to real-time computational architectures, arguing that constitutional rights must be re-conceptualized to remain effective in an algorithmic society (Hildebrandt, 2015, p. 223). Building on a more philosophical foundation, Luciano Floridi introduces the concept of the infosphere to describe the totality of digital interactions that shape contemporary human existence (Floridi, 2016). From an institutional perspective, Giovanni De Gregorio adopts a more structural approach, where he formalizes the notion of digital constitutionalism (De Gregorio, 2022, pp. 1–25). He emphasizes the need to adapt constitutional structures to regulate private digital actors and to uphold fundamental rights within the European Union. His work identifies the EU's emerging digital legal framework as a prototype for global digital governance (De Gregorio, 2022, pp. 290–296).

These scholars offer complementary yet distinct perspectives on the intersection between digital technology and constitutional law. I largely concur with Pollicino's claim that digital platforms have assumed quasi-governmental roles and that constitutional principles must evolve accordingly. However, his framework tends to idealize the capacity of constitutional law to restrain private power without fully addressing the limitations of enforcement mechanisms in the digital environment[8].

The contributions of these authors are both persuasive and intellectually rigorous. Yet, their analyses leave several crucial questions unresolved: What is missing from the current debate? Which normative and institutional challenges remain insufficiently explored? And, most importantly, how is constitutional law itself evolving and adapting in the digital age?

From my perspective, the relationship between constitutional law and emerging digital rights demonstrates both continuity and transformation. On the one hand, constitutional law continues to serve as the primary normative framework for the protection of fundamental rights, ensuring that liberties such as privacy, freedom of expression, and equality remain legally enforceable even within digital environments. On the other hand, the rapid expansion of algorithmic governance reveals the limitations of constitutions drafted in a pre-digital era, which are still deeply rooted in national boundaries.

So, in this context, several new key challenges emerge.

[8] Pollicino, O. (2019). *Digital private powers exercising public functions: The constitutional paradox in the digital age and its possible solutions*. European Court of Human Rights. https://www.echr.coe.int/documents/d/echr/Intervention_20210415_Pollicino_Rule_of_Law_ENG

The first is *the temporal gap* between constitutional frameworks and the accelerating pace of digitalization. Constitutions, often rigid and slow to adapt, struggle to keep up with the disruptive innovations of digital platforms and algorithmic systems, creating normative vacuums where rights are insufficiently protected.

A second challenge lies in *the ambiguity surrounding the constitutional status of digital rights*. While courts and legislatures increasingly interpret traditional rights in light of digital realities, the absence of explicit constitutional recognition leaves digital rights in a fragile and uncertain position. This makes the clear constitutional enshrinement of digital rights a pressing necessity, both to ensure their legal force and to reinforce their legitimacy as fundamental rights.

Third, there is *the displacement of power from the state to private actors*. Global technology companies now perform functions once reserved for public authorities, from moderating speech to managing digital infrastructures. This shift raises profound questions about accountability and the role of constitutional safeguards in regulating entities that often operate beyond the reach of national jurisdictions.

Finally, *the tension between judicial activism and democratic legitimacy* adds yet another layer of complexity. Courts often intervene to fill the constitutional void left by legislative inertia, but their actions may raise concerns about the democratic legitimacy of judge-made digital rights and the balance of powers within constitutional systems.[9]

In this regard, constitutional law is evolving in the context of digitalization through two interconnected dynamics. First, courts engage in evolutionary interpretation, extending traditional rights to digital contexts—for instance, construing the right to privacy as encompassing data protection, or recognizing online freedom of expression as essential to democratic participation. Second, we are witnessing the emergence of explicit digital rights frameworks, whether through constitutional reforms or supranational initiatives (e.g. EU Charter of Fundamental Rights[10] or EU Declaration on Digital Rights and Principles[11]), which already provides a normative foundation for digital constitutionalism.

Nevertheless, these developments demonstrate that constitutional law can no longer remain confined within its traditional boundaries. In my view, its future in the digital age requires a pluralist and layered conception of constitutionalism—one that recognizes constitutional guarantees must operate not only within states but also across regional and global levels, while simultaneously engaging with the regulatory power of private actors.

Only such a multi-level approach can reconcile technological transformation with constitutional legitimacy and preserve human dignity, autonomy, and the democratic values placed under unprecedented pressure by digitalization.

Human Rights in the International and European Law Discourse

Digital technologies have transformed the ways in which fundamental human rights are exercised and protected. Rights are increasingly shaped by online platforms, social networks, and digital

[9] For example, the German Federal Constitutional Court, in case 1 BvR 370/07 (27 February 2008), established a new fundamental right protecting the confidentiality and integrity of computer systems, illustrating how courts can regulate digital matters in the absence of clear legislation. *See,* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], 1 BvR 370/07, Feb. 27, 2008.

[10] Charter of Fundamental Rights of the European Union, art. 7, 8, 11, 2012 O.J. (C 326) 391, 397–398.

[11] The European Commission proposed a "European Declaration on Digital Rights and Principles" in 2022, outlining rights such as digital inclusion, online privacy, and access to digital services, aimed at guiding both EU institutions and Member States in the digital transition. *See,* European Declaration on Digital Rights and Principles for the Digital Decade, 2023 O.J. (C 23) 1.

services. International organizations including the United Nations, the Council of Europe, and the European Union have acknowledged that the digital environment presents both opportunities and challenges for human rights.

Through various declarations, resolutions, and policy frameworks, these organizations emphasize that digital rights represent an extension of classical human rights and require adaptation to ensure their protection in the digital age. This perspective provides a normative foundation for understanding digital rights as integral to the promotion and safeguarding of human dignity, freedom, and equality in the online sphere.

Several scholars have expanded the discussion on digital rights into the international and transnational arena, placing human rights at the core of digital governance. Ian Brown and Douwe Korff emphasize in their report the central importance of privacy and data protection within the European human rights framework.[12] They argue that classical rights enshrined in international human rights treaties must be reinterpreted and strengthened to address the complex challenges posed by digital technologies, particularly in relation to surveillance and data exploitation. From a more intersectional and socio-legal perspective, Sonia Katyal examines the tensions between privacy, freedom of expression, and intellectual property enforcement (Katyal, 2005). She advocates for a digital civil rights approach that acknowledges the overlap—and at times, the conflict—between these rights in online regulation, calling for balanced policies that avoid undermining one right in the name of another (Katyal, 2005).

These scholars contribute valuable to the discourse on digital rights, particularly at the international level. They emphasize the importance of grounding digital rights in robust, adaptable, and globally aware legal systems. Their work complements European constitutional perspectives by extending the conversation beyond the EU and highlighting the inherently global nature of digital freedoms.

While the contributions of Katyal as well as Brown & Korff offer significant insights, they also expose certain unresolved challenges, which as previously discussed are equally characteristic of constitutional law. The first is *the legal and territorial fragmentation of digital rights protection* (Brown & Korff, 2012). Katyal highlights the *conflicts between privacy, freedom of expression, and intellectual property enforcement* (Katyal, 2005). A second issue concerns *the ambiguous constitutional and legal status of digital rights*, which makes them vulnerable to selective or inconsistent application across jurisdictions. A third challenge lies in *the conflicts between fundamental rights*, such as privacy versus freedom of expression or intellectual property versus access to information, which remain insufficiently resolved at the international level, creating uncertainty for both individuals and regulators. Finally, the *temporal gap* between rapid technological change and the slow evolution of international institutions continues to undermine effective governance in the digital sphere.

Key International Instruments Contributing to the Development of Digital Rights within the Human Rights Framework

At the institutional level, several key international and regional organizations have established the normative foundations for the recognition and protection of digital rights, often by extending classical human rights into the digital environment.

[12] Brown, I., & Korff, D. (2012). *Digital freedoms in international law: Practical steps to protect human rights online.* Global Network Initiative. https://ssrn.com/abstract=2085342

The United Nations, through the Universal Declaration of Human Rights, provides the foundational framework: Article 12 protects the right to privacy, and Article 19 guarantees freedom of expression.[13] Although these principles were drafted in a pre-digital era, they are increasingly interpreted as applicable to online spaces, serving as the moral and legal basis for the global digital rights discourse (De Gregorio, 2022, pp. 45–47).[14]

The International Covenant on Civil and Political Rights further reinforces this applicability. Article 17 safeguards the right to privacy, while Article 19 ensures freedom of expression and access to information, all of which are directly relevant to digital communication, surveillance, and data collection practices.[15] These provisions have been invoked by NGOs and courts, to frame violations of digital rights as infringements of human rights.[16]

At the regional level, the Council of Europe has taken proactive steps to articulate digital rights more explicitly. The Committee of Ministers' Recommendation on Human Rights and the Internet urges member states to ensure that core human rights including privacy, freedom of expression, and access to information are effectively upheld in the digital sphere. It also encourages national legal systems to adapt to the realities of cyberspace.[17]

Complementing this, the European Declaration on Digital Rights and Principles, adopted by the European Union in 2022 seeks to systematize digital rights, aligning them more clearly with existing human rights law.[18] The Declaration highlights key issues such as transparency, access, digital education, and protection from harm in online environments, advocating for a comprehensive and people-centered digital rights agenda.

These institutional initiatives provide an essential normative backbone for the protection of digital rights. The UN frameworks—particularly the Universal Declaration of Human Rights[19] and the International Covenant on Civil and Political Rights[20]—remain foundational. However, their broad and non-binding nature limits their effectiveness in addressing complex cross-border digital threats. Their implementation depends heavily on the political will and institutional capacity of states, which vary considerably.

The Place of Digital Rights in Media and Information Literacy as a Complement to Legal Approaches

While legal frameworks provide the formal recognition and protection of digital rights, Media and Information Literacy (MIL) offers a complementary, people-centered dimension that focuses on individuals' ability to understand, exercise, and defend those rights in practice.

The literature increasingly recognizes that laws alone are insufficient to safeguard freedoms in digital spaces: citizens must also possess the critical skills to navigate information flows, detect

13 G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

14 Human Rights Council Resolution 32/13, U.N. Doc. A/HRC/32/L.20, at 48 (27 June 2016).

15 International Covenant on Civil and Political Rights, art. 17, 19, Dec. 16, 1966, 999 U.N.T.S. 171.

16 Human Rights Council Res. 32/13, U.N. Doc. A/HRC/32/L.20, at 48 (June 27, 2016). Rep. of the Spec. Rapport. on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, ¶ 1, U.N. Doc. A/HRC/29/32 (2015).

17 Council of Europe, Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users (Apr. 16, 2014).

18 European Declaration on Digital Rights and Principles for the Digital Decade, 2023 O.J. (C 23) 1.

19 G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

20 International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

misinformation, and assert their rights online (Livingstone & Bulger, 2014, pp. 321–325; Potter, 2013, pp. 45–50).[21]

Scholars in the field of MIL emphasize the interplay between regulation and empowerment, arguing that digital rights cannot be fully realized without informed and literate users. This dual perspective—law as a structural safeguard and MIL as a practical enabler—constitutes an emerging discourse in academic research, underscoring that the protection of rights in the digital age requires not only robust legal instruments but also educational strategies that strengthen resilience among individuals and communities.

Key Scholarly Contributions on Media and Information Literacy and Their Role in Advancing Digital Rights

Several authors regard Media and Information Literacy as a crucial tool for protecting fundamental rights and strengthening democratic values in the digital age. José Manuel Pérez Tornero, working with various collaborators, consistently emphasizes that MIL fosters civic responsibility, critical thinking, and what he describes as a "new humanism." For him, it serves not only as a defensive measure against misinformation and manipulation but also as an active means of promoting peace, tolerance, and freedom of expression.[22]

Howard Tumber and Silvio Waisbord similarly view MIL as a mechanism for empowering citizens to challenge human rights violations, resist disinformation, and reinforce democratic accountability (Tumber & Waisbord, 2017, pp. 10–11). While José Manuel Pérez Tornero focuses on education and value formation, Howard Tumber and Silvio Waisbord broaden the focus by highlighting the political dimension of MIL, emphasizing its role in empowering citizens to demand accountability, resist misinformation, and defend democratic rights (Tumber & Waisbord, 2017, pp. 10–12; 24–28).

Likewise, José Julio Fernández Rodríguez and Jackeline Argüello Lemus examine both the opportunities and risks that digital media pose to fundamental rights. Recognizing the importance of MIL, they argue that education alone cannot safeguard democracy and personal freedoms legal and policy frameworks must evolve alongside it (Fernández Rodríguez & Argüello Lemus, 2019, pp. 45–48; 72–75).

Despite these nuanced differences, a common thread runs through all these works: media literacy is inseparable from human rights protection in the digital age. Each scholar views MIL as a means of resisting manipulation, promoting democratic participation, and fostering resilience against extremism. Taken together, these authors offer complementary yet distinct perspectives on how MIL supports fundamental rights in the digital era.

While much of the literature highlights the transformative potential of MIL for the protection of human rights and fundamental freedoms, the discourse often overlooks the practical and structural challenges that hinder its effectiveness.

First, the *problem of unequal implementation* is crucial. While Torero's vision is inspiring, it risks remaining somewhat idealistic if MIL is confined solely to the educational domain. Given the unprecedented economic and political power of digital platforms in shaping the public sphere, MIL should not be viewed merely as an educational or cultural initiative, but also as a protective and juridical tool that operates alongside legal frameworks to ensure accountability, transparency, and the safeguarding of human rights.

---

[21] See also: UNESCO. (2013). *Global media and information literacy assessment framework: Country readiness and competencies*. https://unesdoc.unesco.org/ark:/48223/pf0000224655

[22] Pérez Tornero, J. M., & Varis, T. (2010). *Media literacy and new humanism*. UNESCO Institute for Information Technologies in Education. https://iite.unesco.org/pics/publications/en/files/3214678.pdf

Indeed, Tornero now engages precisely with this intersection, exploring how MIL can be integrated with law to create a more robust architecture for the protection of rights in the digital age. This evolution in his thinking is reflected in his shift from an early emphasis on MIL as a primarily educational and cultural project to a later recognition of its legal and policy dimensions within European digital governance (Pérez-Tornero & Martire, 2017). Second, although scholars such as Howard Tumber and Silvio Waisbord rightly emphasize that MIL fosters political participation and empowers citizens to defend human rights, their analysis does not fully address the problem of **global inequality of access**.

In Europe, MIL initiatives are often integrated into public education systems and policy frameworks, whereas in many other regions, MIL remains underdeveloped or limited to elite groups.[23]

This creates a paradox: those who most need MIL as a tool for empowerment and the protection of digital rights—communities subject to censorship, manipulation, or digital exclusion—are often the least likely to have access to it. In this sense, MIL risks becoming a privilege of advanced democracies rather than a universal safeguard for all citizens.

Third, and perhaps most fundamentally, *the literature continues to treat MIL primarily as a "pedagogical tool"* rather than recognizing it as a potential fundamental right in itself.[24] MIL is conceived as an adjunct to regulation rather than as a right that should be codified alongside freedom of expression, the right to information, and the right to education. The lack of recognition of MIL as a fundamental right remains a significant shortcoming. By contrast, if MIL were recognized as a normative right enforceable at the constitutional or international level, it could operate not only as an educational framework but also as a legal safeguard against disinformation, manipulation, and violations of digital rights.

---

[23] For evidence that MIL is comparatively more integrated into public education and policy frameworks in Europe while remaining patchy elsewhere, see: European Commission, Digital Education Action Plan (2021–2027) (setting out the EU strategy for digital and media competences) (*See*, Opinion of the European Committee of the Regions — Digital Education Action Plan 2021–2027, 2021 O.J. (C 300) 65). See also the Commission's requirement that Member States submit national reports on media-literacy measures under the Audiovisual Media Services Directive (*See,* Directive 2010/13/EU, of the European Parliament and of the Council of 10 March 2010 on the Coordination of Certain Provisions laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive), 2010 O.J. (L 95) 1 as amended by Directive 2018/1808, of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the Coordination of Certain Provisions laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in view of Changing Market Realities, 2018 O.J. (L 303) 69), which documents national MIL initiatives across the EU. For an EU assessment of programme activity and coordination, see the European Digital Media Observatory (EDMO) report on media literacy in Europe (Goodman, E. (2021). Media literacy in Europe: Current programmes and initiatives. EDMO. https://edmo.eu/wp-content/uploads/2022/02/Media-literacy-in-Europe-and-the-role-of-EDMO-Report-2021.pdf). By contrast, UNESCO's global assessments and recent issue briefs document significant gaps in MIL policy and education internationally and provide global statistics on public exposure to disinformation and low fact-checking practices, demonstrating uneven uptake of MIL outside Europe. (UNESCO. (2013). Global media and information literacy assessment framework: Country readiness and competencies. https://unesdoc.unesco.org/ark:/48223/pf0000224655).

[24] UNESCO. (2013). *Global media and information literacy assessment framework: Country readiness and competencies* (pp. 17–20). https://unesdoc.unesco.org/ark:/48223/pf0000224655; Frau-Meigs, D. (2023). Declaration on Media and Information Literacy (pp. 21–24). UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000386080.locale=en; Carlsson, U. (Ed.). (2019). *Understanding media and information literacy (MIL) in the digital age: A question of democracy* (pp. 9–14). University of Gothenburg. https://www.gu.se/sites/default/files/2020-08/JMG_understanding-mil.pdf

From Traditional Rights to Digital Realities: Confronting the Gaps in the Court and Building New Concepts in the Regulatory Field

Building on the analysis of human rights frameworks and the identification of key gaps in the previous part, this section examines how these shortcomings have led to the emergence of new digital human rights. The unprecedented scale of digitalization—combined with algorithmic governance, transnational data flows, and the growing power of private platforms—has exposed the limitations of classical rights and prompted courts, legislators, and international bodies to adapt existing protections or create new ones.

Moreover, Media and Information Literacy (MIL) emerges as a crucial complementary mechanism within this legal and juridical context. While legal instruments provide formal protections, MIL empowers citizens to understand, claim, and exercise their rights in digital spaces, fostering civic responsibility, critical awareness, and democratic participation. Yet, its potential remains constrained by its current treatment as primarily an educational tool rather than a recognized instrument of legal protection. Integrating MIL into legal frameworks can enhance both the enforceability and the effectiveness of digital rights, bridging the gap between normative guarantees and practical empowerment.

In sum, this section explores how deficiencies in traditional frameworks have catalyzed the development of new rights, the challenges they face today, and the synergistic solutions that combine law and MIL to safeguard fundamental rights in the digital age.

Evolving Rights in the Digital Era: A New Birth through Case Studies

The emergence of digital rights has not occurred in a vacuum. Unlike traditional human rights, which were often proclaimed in foundational texts following revolutions or political declarations, digital rights have evolved gradually and reactively, shaped by the concrete challenges of the digital age.

Two main vectors explain this evolution. On the one hand, judicial cases in which courts were confronted with unprecedented issues such as mass data collection, algorithmic bias, restrictions on online freedom of expression, and both state and private surveillance, forcing them to adapt or reinterpret classical rights. On the other hand, Media and Information Literacy (MIL) initiatives, although primarily educational in nature, have played a crucial role in raising public awareness and empowering citizens to defend their fundamental rights in digital environments.

Thus, it is not through abstract proclamations but through engagement with real-world situations that new rights—such as the right to be forgotten, the right to algorithmic transparency, and the right to equitable access to information—have gradually emerged. This section therefore examines a series of emblematic cases that illustrate this process.

Decisions of the European and National Courts

Mario Costeja González v. Google Spain

In 1998, a Spanish newspaper published a legal notice concerning the auction of a property belonging to Mario Costeja González, following the seizure of assets due to outstanding debts. Years later, when searching for his name on Google, this outdated information still appeared prominently in the search results. Although the debt had long since been resolved, the

continued accessibility of this information harmed Mr. Costeja's reputation and his right to privacy.[25]

Mr. Costeja therefore lodged a complaint with the Spanish Data Protection Agency (AEPD), requesting that Google remove links to these outdated and prejudicial notices.[26] At the time, the applicable legal framework was the 1995 EU Data Protection Directive, which had been designed for traditional forms of data processing but did not explicitly regulate search engines or reflect the realities of the digital environment.[27]

The case ultimately reached the Court of Justice of the European Union (CJEU), which delivered a landmark judgment in 2014. The Court held that Google was indeed a data controller under the Directive and could therefore be held responsible for processing personal data through its indexing activities.[28]

More importantly, the Court articulated a new principle: individuals have the right to request the delisting of search results that are inaccurate, irrelevant, no longer relevant, or excessive in relation to the purposes of processing.[29]

This decision marked the birth of a new digital right the right to be forgotten. It demonstrated how traditional legal instruments, when confronted with new digital realities, must be reinterpreted and expanded by the judiciary. The ruling also highlighted the inherent tension between classical rights and emerging digital rights, particularly the delicate balance between the right to privacy and the right to freedom of information.

Delfi AS v. Estonia

Freedom of expression, as a classical right, is considered a pre-digital right under Article 10 of the European Convention on Human Rights.[30] It was originally designed to safeguard the ability to express oneself through the press and other traditional media within a stable legal framework. However, in today's digital environment, online platforms carry new risks, particularly regarding the publication of hate speech, cyberbullying, and other harmful content.

A clear illustration of this challenge is the Delfi case.[31] Delfi is a news portal that publishes political, economic, and social articles while allowing users to comment freely on the published content[32]. On one occasion, a woman became the target of defamatory comments posted on the site and decided to pursue legal action against Delfi.[33]

The European Court of Human Rights ultimately held that Delfi had a duty to moderate content proactively. The Court's judgment established a new rule—the proactive responsibility of online platforms to protect individuals from harmful content.[34] This case demonstrates how classical rights,

25 Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) & González, ECLI:EU:C:2014:317, ¶ 14 (May 13, 2014).

26 Ibid.

27 Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. (L 281) 31 (repealed 2018).

28 Case C-131/12, Google Spain, ECLI:EU:C:2014:317, ¶¶ 45–60.

29 Ibid., ¶¶ 89–99.

30 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), art. 10, Nov. 4, 1950, 213 U.N.T.S. 221.

31 Delfi AS v. Estonia, App. No. 64569/09 (June 16, 2015), https://hudoc.echr.coe.int/fre?i=001-155627

32 Ibid., ¶¶ 11–15.

33 Ibid., ¶¶ 16–31.

34 Ibid., ¶¶ 125–129.

when confronted with digital realities, can evolve into new digital rights, creating legal obligations for platforms to safeguard users while maintaining a balance with freedom of expression.

VZW Klimaatzaak v. Kingdom of Belgium & Others

In Belgium, the Youth for Climate movement mobilized thousands of young citizens around climate issues, relying heavily on social media platforms to inform, raise awareness, and organize public demonstrations.[35] As part of their legal actions, the activists sought access to specific environmental data essential to substantiate their arguments before the courts.

However, a significant portion of this information was not readily accessible online, creating a tangible obstacle to exercising the right of access to environmental information as guaranteed by the Aarhus Convention (1998).[36]

In June 2021, the Brussels Court of First Instance found that the Belgian State had failed to meet its obligations both regarding environmental protection and the online accessibility of information.[37] This ruling marked the emergence of a new right: the "online right to know." Nevertheless, this right remains fragmented, indirectly recognized, and has yet to be elevated to the status of an autonomous fundamental digital right.

This case illustrates the intersection of classical rights with digital realities, demonstrating how traditional legal frameworks must adapt to guarantee access to information in the digital age, and underscoring the role of courts in shaping the contours of emerging digital rights.

Media and Information Literacy (MIL) Case Studies

Case Study 1: The Papua New Guinea Experience in Social Media

Social media platforms are widely used by adolescents and young adults worldwide. While these platforms provide opportunities for social interaction and access to information, they also expose users to risks such as cyberbullying, misinformation, and online exploitation. Scholars in Media and Information Literacy (MIL) emphasize that education in digital literacy is essential to equip young people with the skills to navigate online environments responsibly and protect their personal information (Livingstone et al., 2017, Siraba, 2019).[38]

Encouraged by the insights provided through MIL, the government of Papua New Guinea implemented several regulatory measures to complement its educational strategy. Specifically, it restricted access to social media platforms for users under the age of 14 and introduced a mandatory identification system called SevisPass for those above this age threshold. This measure aims to protect young users while simultaneously promoting safer and more responsible participation in digital space.[39]

---

35 Wouters, R., & De Vydt, M. (2019, April 12). *Youth for climate Belgium: The narrative of an exceptional protest wave*. Mobilizing Ideas. https://mobilizingideas.wordpress.com/2019/04/12/youth-for-climate-belgium-the-narrative-of-an-exceptional-protest-wave/

36 Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Aarhus Convention), June 25 1998, 2161 U.N.T.S. 447.

37 Civ. [Tribunal of First Instance] Brussel (4th ch.), June 17, 2021, English translation available at https://cdn.climatepolicyradar.org/navigator/BEL/2014/vzw-klimaatzaak-v-kingdom-of-belgium-others_50dbc50006ca324347b2de2119ec5a0b.pdf

38 UNESCO. (2013). *Global media and information literacy assessment framework: Country readiness and competencies* (pp. 17–20). https://unesdoc.unesco.org/ark:/48223/pf0000224655

39 Anadolu Agency. (2025, October 3). *Papua New Guinea Mulls age restrictions on social media*. https://www.aa.com.tr/en/asia-pacific/papua-new-guinea-mulls-age-restrictions-on-social-media/3706540

Overall, this case underscores the crucial role of Media and Information Literacy in addressing emerging challenges in the digital environment. It illustrates how MIL can inform policymaking, enhance online safety, and contribute to the recognition of new digital rights particularly the right to data protection and the right to responsible participation in digital spaces.

Case Study 2: False Information in the United Kingdom

In the United Kingdom the rapid proliferation of misinformation and disinformation on digital platforms has emerged as a major challenge, particularly affecting young people who often lack the critical skills needed to evaluate the credibility of online content. This situation threatens informed citizenship and democratic participation, as the spread of false or misleading information can distort public understanding and decision-making.

Recognizing the seriousness of this issue, the Guardian Foundation has actively promoted the integration of MIL into the national curriculum, advocating for media literacy to become a core competency at all stages of education.[40]

Its initiatives include comprehensive teacher training programs to equip educators with the tools to foster critical thinking, as well as student-centered projects such as the Media Literacy Ambassador Program, which empowers students to teach their peers how to identify misinformation, reinforcing critical skills through peer-to-peer learning.

Through these interventions, students and young citizens gain the ability to navigate complex digital spaces, assess the reliability of information, and engage responsibly in online environments. Importantly, this work has contributed to the recognition of new digital rights, including the right to reliable information and the right to informed participation, ensuring that citizens can meaningfully engage in democratic processes with awareness and critical judgment.

This case clearly illustrates how MIL can serve not only as an educational tool but also as a mechanism for the emergence and reinforcement of digital human rights, equipping individuals to exercise their rights and responsibilities effectively within the digital sphere.

Digital Human Rights: Practical Extensions of Existing Rights

With the technological revolution, a new category of digital rights has emerged to ensure that users are protected in the digital environment just as they are in their everyday lives. These rights aim to guarantee access to essential services on digital platforms—mirroring those in the real world—and include the right to digital inclusion, the right to protection from digital violence, and the right to be forgotten.

Right to Digital Inclusion

Being connected is essential to enhancing personal and societal well-being and enabling digital livelihoods. In this sense, every individual has the right to digital inclusion. This right ensures that all people have access to digital systems and online services—particularly persons with disabilities, the elderly, young people, and communities living in low-income regions.[41]

---

[40] Harrison, T., Polizzi, F., McLoughlin, S., Clark, C., Picton, I., & Bushby, R. (2024). *Educating and measuring news literacy and civic engagement in 9 to 11 year olds*. University of Liverpool; University of Birmingham; National Literacy Trust. https://www.jubileecentre.ac.uk/wp-content/uploads/2024/02/News-Literacy-and-Civic-Engagement-Full-Report-1st-Feb.pdf

[41] United Nations. (n.d.). Definition of digital inclusion. Retrieved June 7, 2025, from https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/general/Definition_Digital-Inclusion.pdf

In a dynamic and interconnected world, digital inclusion goes beyond the conventional focus on access and skills. It seeks to promote a holistic, action-oriented approach that remains responsive to evolving global trends.[42]

The European Commission, in its 2024 report, outlines a vision aimed at ensuring the protection of rights and freedoms while effectively upholding European values in an increasingly digital world. The European Union seeks to safeguard these values by fostering solidarity and digital inclusion through enhanced connectivity, digital education, freedom of choice, and a fair digital environment; by promoting participation in the digital public sphere; by increasing online safety, security, and empowerment particularly for young people; and by advancing sustainability.[43]

Right to Protection from Digital Violence

Digital violence refers to criminal and harmful behaviors committed through digital tools and spaces. It can take various forms of abuse and harassment against both children and adults, including cyberbullying[44], doxing[45], misinformation and deepfakes, and digital blackmail. The term digital violence is a relatively new term. It has been expressed in the last twenty years and constantly rising. There are several definitions of digital violence in use, depending on the types of digital harassment or forms of digital violence (Jevtić, 2020, p. 198). Digital violence also disproportionately affects women and girls, reflecting and reinforcing gender inequalities while exposing them to new forms of abuse in online spaces. The rise of digital technologies has become a double-edged sword for women's rights, impacting them more acutely than men and children.[46]

Right to Be Forgotten

In fact, the right to be forgotten certainly belongs to the field of rights attributable to privacy, which cannot be identified as a single and well-defined right, but rather as a complex of rights relating to the sphere of a person's private life (Maietta, 2020, p. 209).

The right to be forgotten is a modern legal concept that allows users to delete information, publications, images, or videos from digital spaces if they so choose. It first emerged in the jurisprudence of the Court of Justice of the European Union (CJEU) as an aspect of the right to privacy of data subjects in the context of personal data processing.[47]

---

[42] United Nations Development Programme. (2024). From access to empowerment: Digital inclusion in a dynamic world (p. 6). United Nations. https://www.undp.org/sites/g/files/zskgke326/files/2024-05/undp_digital_inclusion_in_a_dynamic_world.pdf

[43] *Commission Communication on the State of Digital Decade 2024*, COM(2024) 260 final (July 2, 2024). The Annex 4 dedicated to the monitoring of the European Digital Rights and Principles is published separately. *See*, *Commission Communication on the State of Digital Decade 2024*, annex 4, COM(2024) 260 final (July 2, 2024), https://ec.europa.eu/newsroom/dae/redirection/document/106722

[44] Cyberbullying — bullying that occurs through digital devices such as mobile phones, computers, and tablets.

[45] Doxxing — the act of publicly disclosing personally identifiable information about an individual or organization, usually via the Internet and without their consent.

[46] Zamfir, I., & Murphy, C. (2024). Cyberviolence against women in the EU (European Parliamentary Research Service Briefing, No. PE 767.146). European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI%282024%29767146_EN.pdf

[47] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) & González, ECLI:EU:C:2014:317 (May 13, 2014). See the section above dedicated to this decision.

Today, this right is framed and protected under the General Data Protection Regulation (GDPR), which mentions the "right to erasure" in the Article 17, balancing it with the right to freedom of expression and information, and the protection of personal data.[48]

Right to Algorithmic Transparency

Adopted by the European Union in March 2024, the AI Act is the world's first comprehensive legal framework regulating the development and use of artificial intelligence.[49] Its core objective is to ensure that AI systems operate in alignment with European values, fundamental rights, and human dignity. The Act introduces a risk-based approach, categorizing AI systems as unacceptable, high, limited, or minimal risk. Applications such as government social scoring, manipulative algorithms, and biometric surveillance in public spaces are strictly prohibited.[50]

For high-risk AI systems including those used in healthcare, education, recruitment, and law enforcement developers must comply with stringent obligations regarding transparency, human oversight, data quality, and accountability.[51] The Act also reinforces individuals' right not to be subjected to decisions made solely by automated systems without human intervention,[52] echoing Article 22 of the GDPR.[53] This Act therefore establishes a new digital right to algorithmic transparency, fairness, and human oversight in AI governance.

Right to Disconnect

The right to disconnect (also known as the "right to be offline") protects workers from the expectation of constant digital availability outside working hours. Formally recognized by the European Parliament Resolution of January 21, 2021, this right allows employees to disengage from emails, calls, and other work-related digital tools beyond their contractual working time.[54] Its purpose is to safeguard mental health, privacy, and work–life balance in an era defined by remote work and digital communication.

France was the first country to introduce this right through the El Khomri Law (Law No. 2016-1088)[55], followed by Spain (Royal Decree-Law 28/2020 on Remote Work)[56] and Italy (Law 81/2017)[57].

---

48 Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 43–44.

49 Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2016/798 of the European Parliament and of the Council, 2024 O.J. (L 202) 1.

50 *Id.*, art. 5, 2024 O.J. (L 202) 51–53.

51 *Id.*, art. 6, 2024 O.J. (L 202) 51–54.

52 *Id.*, art. 8-9, art. 14, 2024 O.J. (L 202) 55–57, 60–61.

53 General Data Protection Regulation, 2016 O.J. (L 119) 39–40.

54 Resolution on the Right to Disconnect, Eur. Parl. Doc. 2019/2181(INL)) (2021).

55 Loi 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels [Law No. 2016-1088 of August 8, 2016 on Work, the Modernization of Social Dialogue and the Safeguarding of Career Paths], J.O., Aug. 9, 2016, p. 1 (Fr).

56 Remote Work Law (B.O.E. 2020, 77064) (Spain).

57 Legge, Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato [Law on Measures for the Protection of Self-Employed Work and to Encourage Flexible Work Arrangements], n. 81, 22 May 2017 (It.).

These laws require employers to establish clear internal policies on digital disconnection and to ensure that employees are not penalized for exercising this right. By recognizing the right to disconnect, European legislation has created a new form of digital labor right—one that ensures humane working conditions in the digital age and protects individuals' rights to rest, privacy, and psychological well-being.

Emergent Threats to Human Rights in Digital Spaces

Alongside the rapid advancement of digital technologies, new threats to digital human rights have emerged. While the Internet offers vast opportunities for the exercise of human rights, it also possesses features that make it a significant source of risks and threats to those very rights.[58]

Cyber Attacks

One of the most significant threats to digital human rights is cyber-attacks, which involve the exposure of personal data and user information. A cyber-attack represents a violation of privacy, in which hackers steal financial, medical, or personal details about users.

Attackers can range from individual hackers and activists to petty criminals, corporations, and even national governments.[59] To counter such threats, strong cybersecurity measures are essential.

Indeed, the term cybersecurity itself is defined by the European Union as "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure.[60]"

Challenges to Digital Human Rights

Unfortunately, these new digital rights still face numerous challenges and threats that shape the ways in which users exercise their freedoms. In this context, challenges refer to systemic obstacles that require technological, regulatory, or societal solutions, while threats encompass the risks directed against the exercise of those very rights. There is a broad range of threats and challenges associated with the ongoing digitalization of traditional spheres of state and social life and the integration of smart technologies such as artificial intelligence and neural networks (Volodenkov & Fedorchenko, 2022, pp. 283-291).

Balance Between Digital and Real-Life Privacy

In today's hyperconnected environment, maintaining a balanced relationship between digital life and real-life privacy has become increasingly challenging. Constant engagement with digital platforms not only exposes individuals to information overload and continuous connectivity demands but also intensifies the production of personal data, which places additional pressure on the protection of digital rights and well-being (Turkle, 2015, pp. 3–28).

---

58 Pajuste, T. (Ed.). (2022). Specific threats to human rights protection from the digital reality. Tallinn University. https://graphite.page/GDHRNet-threats-to-human-rights-protection/assets/documents/GDHRNet-ThreatsReport-EditedVolume.pdf

59 Rossini, C., & Green, N. (2015). Cybersecurity and human rights. In *Webinar series training summaries*. Global Partners Digital. https://bestbits.net/wp-content/uploads/2015/04/Cybersecurity-and-Human-Rights-GCCS2015-Webinar.pdf

60 European Commission. (2013, February 7). EU cybersecurity plan to protect an open Internet and online freedom and opportunity — cyber security strategy of the European Union: An open, safe and secure cyberspace [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_13_94

This continuous interaction with digital technologies inevitably generates a digital footprint comprising all traces of data that individuals leave behind through browsing, posting, location sharing, and platform interaction. This footprint, once accumulated and processed in the context of big data, can circulate across multiple domains such as commercial advertising, algorithmic profiling, and public or private databases, raising concerns about privacy, autonomy, and long-term control over personal information (Lin et al., 2022, pp. 1–2, 6–7).

Thus, the challenge of balancing digital and real-life privacy is inseparable from the issue of digital footprints: the more individuals depend on digital environments, the more personal data they generate, amplifying both the opportunities and risks inherent to contemporary digital ecosystems.

Digital Divide

The concept of the digital divide is generally defined as the gap between people who have access to information and communication technologies and those who do not (van Dijk, 2017, p. 1). It refers to limited access to the Internet, digital tools, and essential online services such as education, healthcare, and employment opportunities.

The digital divide became particularly evident during the COVID-19 pandemic, when Internet access became a necessity for education, work, and social interaction, millions of students and individuals were left without reliable Internet connections and access to online services.[61]

Gap Between Digital Laws and Real-World Realities

Despite significant legal progress—such as the EU's Artificial Intelligence Act[62], Digital Services Act[63], and Digital Markets Act[64]—a major challenge persists in the discrepancy between the legal framework and its practical enforcement. Many digital rights remain largely symbolic, as citizens often lack the digital literacy, institutional support, or procedural mechanisms necessary to exercise them effectively.

For instance, while users are legally entitled to transparency regarding algorithmic decision-making, few possess the technical capacity or access required to verify how these algorithms function in practice. Moreover, enforcement authorities (such as data protection agencies and digital regulators) frequently face limited resources and insufficient technological expertise, undermining their ability to monitor compliance or impose sanctions for violations. This has created an expanding gap between the normative promise of digital rights and their lived implementation.

The Growing Power and Responsibility of Private Actors

Perhaps the most complex challenge lies in the concentration of digital power in the hands of private corporations. Global technology platforms such as *Meta**, *Google*, *X* (*Twitter*), and *TikTok* have

[61] UNESCO. (2020, April 21). Startling digital divides in distance learning emerge [Press release]. https://www.unesco.org/en/articles/startling-digital-divides-distance-learning-emerge

[62] Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2016/798 of the European Parliament and of the Council, 2024 O.J. (L 202) 1.

[63] Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

[64] Regulation 2022/1925, of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) 1.

* Ed. note: By decision of the authorities of the Russian Federation, *Meta Platforms, Inc.* has been declared an extremist organization, and its activities are prohibited on the territory of Russia.

become de facto regulators of online spaces, controlling access to information, moderating content, and shaping public discourse.

Their algorithms determine visibility, engagement, and even the contours of democratic participation—often without adequate transparency or accountability. Although recent laws, such as the Digital Services Act, attempt to rebalance this power by imposing stricter obligations on very large online platforms, the enforcement of these obligations remains uncertain.[65]

Moreover, the privatization of rights enforcement where companies decide what constitutes "harmful content" or "free expression" raises serious ethical and legal concerns about legitimacy and democratic control.[66] The key challenge today is to redefine a governance model that ensures private accountability within a framework of public responsibility, reinforcing the principle that digital rights are not corporate privileges but universal human rights.

Strengthening Digital Rights: Present Solutions and Strategies for Protecting the Digital Sphere

Within this general regulatory context, the law recognizes that individuals possess a fundamental right to information and communication. In today's world, the media, digital platforms, and regulation represent three interdependent domains.

The media require legal frameworks to regulate the circulation of information in order to safeguard public opinion and collective rights. Digital platforms, in turn, need a strict regulatory structure to protect users from fake news and deepfakes, to govern a new category of information disseminators (influencers and content creators) to regulate communication among users, to uphold freedom of expression, to ensure the accountability of emerging technologies, and to protect copyright and intellectual property on social networks.

Finally, it is through regulation and law that the media can play a fundamental role in facilitating access to legal information and raising public awareness of rights and responsibility. The law, in turn, requires a fair, transparent, and responsible media ecosystem and well-regulated platforms to popularize legislation, inform individuals of their duties, and disseminate newly adopted rules effectively.

Legal and Framework Solutions

The European Declaration on Digital Rights and Principles as a Foundational Pillar for Analysis

The rapid advancement of technology has necessitated the continuous adaptation of various laws and regulatory approaches. Legislators, for their part, often struggle to keep pace with users' growing agency and acts of digital appropriation, sometimes overlooking or diminishing legitimate user claims to control how their data and digital interactions are used. Consequently, a range of legal frameworks have been updated to strengthen the protection of digital human

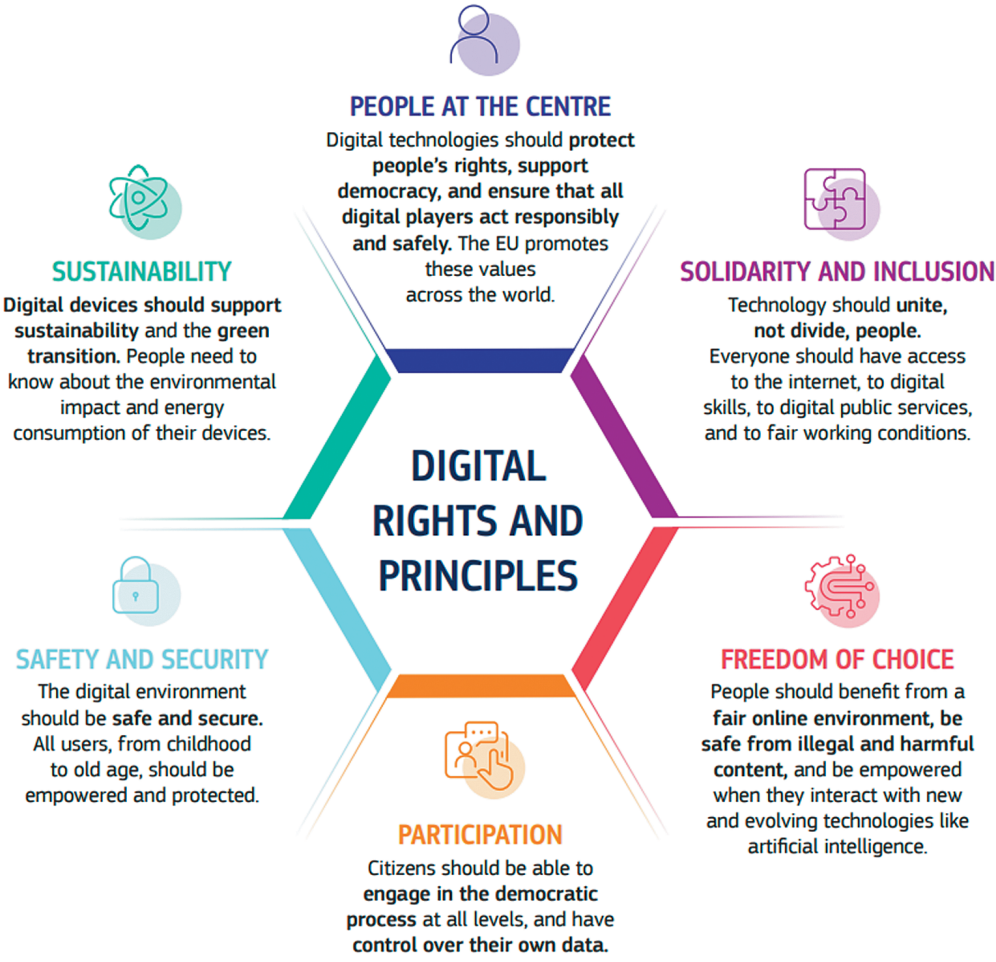
[65] Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), art. 33, 38, 40, 42, 2022 O.J. (L 277) 63–64, 69, 70–72, 73–74.

[66] Ortutay, B. (2025, January 9). *Meta* eases some restrictions on speech targeting transgender people, immigrants, and other groups after review tied to elections*. Associated Press. https://apnews.com/article/meta-facebook-hate-speech-trump-immigrant-transgender-41191638cd7c720b950c05f9395a2b49

* Ed. note: By decision of the authorities of the Russian Federation, *Meta Platforms, Inc.* has been declared an extremist organization, and its activities are prohibited on the territory of Russia.

Figure 1

The six Chapters of the European Declaration on Digital Rights and Principles for the Digital Decade



Note. Reproduced from the European Commission's study to support monitoring of the Declaration on Digital Rights and Principles.[67]

rights, among which the European Declaration on Digital Rights stands out as one of the most significant.[68]

Adopted in 2022, the European Declaration on Digital Rights represents a landmark policy instrument that embodies the EU's vision of a human-centric digital transformation. It reaffirms the EU's commitment to ensuring that the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union[69] and in international human rights instruments are effectively upheld in the digital realm.

[67] European Commission. (2025). *Study to support the monitoring of the Declaration on Digital Rights and Principles : Final Report* (2nd ed., p. 28). European Union. https://doi.org/10.2759/0915515

[68] European Declaration on Digital Rights and Principles for the Digital Decade, 2023 O.J. (C 23) 1.

[69] Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.

The Declaration is built around six core principles: placing people at the center of the digital transformation; promoting solidarity and inclusion; ensuring freedom of choice; fostering participation in the digital public sphere; enhancing safety, security, and empowerment; and advancing sustainability in the digital age.

Following the adoption of the European Declaration on Digital Rights and Principles, scholars and institutions across Europe welcomed it as a significant milestone in embedding human-centric values within the digital transformation. Experts in digital constitutionalism, such as Cristina Cocito and Paul De Hert, praised its transformative vision and its potential to shape governance in the digital domain (Cocito & De Hert, 2023). Policy analyst Anna Pingen viewed it as a strategic framework designed to inspire legislation and policymaking throughout the EU.[70]

While the European Economic and Social Committee (EESC) acknowledged the Declaration's value,[71] it also pointed to challenges in implementation and public awareness. Critical commentators cautioned against placing excessive responsibility on individuals without providing sufficient institutional safeguards. Overall, the Declaration has been positively received for articulating a shared vision of Europe's digital future, while underscoring the need for stronger enforcement mechanisms and inclusive implementation.

Sporadic Constitutional Recognition of Digital Rights

The constitutional recognition of digital rights by a few European jurisdictions represents a fundamental advancement in safeguarding human rights in the digital era.

For instance, the Portuguese Constitution protects the right to privacy under Article 26, which prohibits arbitrary interference with personal data.[72] Moreover, under Law No. 58/2019, Portugal has enshrined the rights to data protection and access to digital information, providing citizens with strong legal remedies against excessive surveillance or misuse of personal data.[73]

In Spain, Organic Law 3/2018, following the constitution, establishes key digital rights, including the rights to privacy, security in digital interactions, digital identity, and the right to disconnect.[74] These rights are closely linked to constitutional protections, creating a robust legal framework for their enforcement.

---

70 Pingen, A. (2022, February 22). Commission proposes Declaration on European Digital Rights and Principles. Eucrim. https://eucrim.eu/news/commission-proposes-declaration-on-european-digital-rights-and-principles/

71 Opinion of the European Economic and Social Committee on (a) 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — Establishing a European Declaration on Digital rights and principles for the Digital Decade' and on (b) 'Digital rights and principles'. O.J. (C 365) 13.

72 Constitution of the Portuguese Republic art. 26 (Rev. 2005), English translation available at https://www.parlamento.pt/sites/EN/Parliament/Documents/Constitution7th.pdf

73 Law No. 58/2019, of August 8, on the implementation in the national legal order of Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Diário da República [D.R.] No. 152/2019 — Série I of 8 Aug. 2019 (Portugal). Available at https://diariodarepublica.pt/dr/en/detail/act/58-2019-123815982

74 Constitución Española, art. 18.4, B.O.E. n. 311, Dec. 29, 1978 (Spain). See about interpretation of Article 18.4 as a basis for data protection law: GDPR Hub. (n.d.). *Data protection in Spain*. Retrieved July 7, 2025 from https://gdprhub.eu/Data_Protection_in_Spain. This provision should be read in conjunction with Organic Law 3/2018, see: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [Organic Law on on Personal Data Protection and Guarantee of Digital Rights], (B.O.E. 2018, 294) (Spain).

Similarly, the Constitution of the Republic of Estonia, in Article 43, guarantees access to the internet and secure digital identity as integral components of its constitutional and digital governance framework.[75]

The constitutional codification of digital rights ensures legal stability, enforceability, and resilience in the face of technological evolution, providing a solid foundation upon which legislative measures, regulatory frameworks, and educational initiatives can build to protect citizens effectively in the rapidly evolving digital landscape.

Educational Safeguard for Digital Human Rights: Media and Information Literacy Solutions

In an era where digitalization marks a new stage of human evolution, media and information literacy serves as a crucial tool for protecting digital human rights. It empowers users to understand and critically assess information circulating in digital spaces, to distinguish between reliable and false content, and to recognize their responsibilities within the online environment.

Many scholars emphasize that Media and Information Literacy movement functions not only as an educational instrument but also as a form of empowerment, enabling citizens to recognize and resist disinformation, online manipulation, and violations of privacy[76]. Within the framework of digital human rights, MIL should be a preventive social mechanism that complements legal and regulatory measures by fostering informed, autonomous, and resilient digital citizens capable of asserting their rights within complex online ecosystems.

The protection of digital human rights requires the joint operation of law and MIL. Law provides the formal rights and standards, while MIL equips individuals with the competencies to understand, exercise, and defend these rights online. Without Media and Information Literacy, legal protections remain abstract; without law, literacy alone cannot ensure enforcement. Together, they establish a holistic framework that empowers citizens and safeguards human rights in the digital environment.

Conclusion

As the digital world continues to evolve and assumes a central role in the dissemination of information and the fulfilment of everyday needs, it simultaneously presents major challenges for fundamental rights. On the one hand, it enables unprecedented forms of expression, civic participation, and access to information; on the other hand, it has become a space marked by troubling phenomena such as disinformation, hate speech, and violations of users' privacy.

To safeguard these digital rights, legal protections must be effectively enforced, including robust data protection, the security of digital transactions, laws imposing stricter age restrictions to limit minors' exposure to harmful content on social media platforms, and the promotion of social justice.

Furthermore, high levels of education in media and information literacy enhance users' ability to critically assess media content, while awareness-raising campaigns can strengthen public understanding of global challenges and foster a more informed and resilient digital society.

---

[75] Constitution of the Republic of Estonia art. 43 (1992, as amended 2015), available at https://www.riigiteataja.ee/en/eli/521052015001/consolide

[76] For instance, Kostas Karpouzis argues that MIL is essential for individuals to critically engage with information, navigate the digital environment safely, and counter both disinformation and hate speech. Karpouzis, K. (2024). *Media and information literacy as a fundamental human right*. Preprints. https://doi.org/10.20944/preprints202408.2242.v1

References

1. Balkin, J. M. (2004). Digital speech and democratic culture: A theory of freedom of expression for the information society. New York University Law Review, 79(1), 1–55. https://nyulawreview.org/issues/volume-79-number-1/digital-speech-and-democratic-culture/
2. Bygrave, L. A. (2002). Data protection law: Approaching its rationale, logic and limits. Kluwer Law International.
3. Cocito, C., & De Hert, P. (2023). The transformative nature of the EU Declaration on Digital Rights and Principles: Replacing the old paradigm (normative equivalency of rights). *Computer Law & Security Review, 50*, Article 105846. https://doi.org/10.1016/j.clsr.2023.105846
4. De Gregorio, G. (2022). *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*. Cambridge University Press. https://doi.org/10.1017/9781009071215
5. Domaradzki, S., Khvostova, M., & Pupovac, D. (2019). Karel Vasak's generations of rights and the contemporary human rights discourse. *Human Rights Review, 20*(4), 423–443. https://doi.org/10.1007/s12142-019-00565-x
6. Dowd, R. (2022). *The birth of digital human rights*: *Digitized data governance as a human rights issue in the EU*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-82969-8
7. Fernández Rodríguez, J. J., & Argüello Lemus, J. (2019). Digital media and the challenges for fundamental rights. In A. Berea (Ed.), *A Complex Systems Perspective of Communication from Cells to Societies* (pp. 1–14). IntechOpen. https://doi.org/10.5772/intechopen.82435
8. Floridi, L. (2013). *The ethics of information*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199641321.001.0001
9. Floridi, L. (2016). *The fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press.
10. Hildebrandt, M. (2015). Smart Technologies and the End(s) of Law. Edward Elgar Publishing. https://doi.org/10.4337/9781849808774
11. Hildebrandt, M. (2020). *Law for computer scientists and other folk*. Oxford University Press. https://doi.org/10.1093/oso/9780198860877.001.0001
12. Jevtić, R. (2020). Digital violence and the role of different factors in its prevention. *Zbornik radova Pedagoškog fakulteta, Užice, 23*(22), 195–212. https://doi.org/10.5937/ZRPFU2022195J
13. Katyal, S. K. (2005). Privacy vs. piracy. *Yale Journal of Law & Technology, 7*, 222–345.
14. Lin, X., Ju, F., Zhao, C., Feng, X., & Luo, D. (2022). The wave of the digital economy: The conflict and balance between data sharing and personal privacy. *SHS Web of Conferences, 148*, Article 03055. https://doi.org/10.1051/shsconf/202214803055
15. Livingstone, S., & Bulger, M. (2014). A global agenda for children's rights in the digital age. *Journal of Children and Media, 8*(4), 317–335. https://doi.org/10.1080/17482798.2014.961496
16. Livingstone, S., Mascheroni, G., & Staksrud, E. (2017). European research on children's internet use: Assessing the past and anticipating the future. *New Media & Society, 20*(3), 1103-1122. https://doi.org/10.1177/1461444816685930
17. Maietta, A. (2020). The right to be forgotten. *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito*, *12*(2), 207–226. https://doi.org/10.4013/rechtd.2020.122.03
18. Pérez Tornero, J. M., Orozco, G., & Hamburger, E. (Eds.). (2020). Media and information literacy in critical times: Re-imagining learning and information environments. Autonomous University of Barcelona; The Arab Academy for Science.

19. Pérez-Tornero, J. M., & Martire, A. (Eds.). (2017). Educación y nuevos entornos mediáticos. [Education and new media environments]. Editorial UOC.
20. Potter, W. J. (2013). *Media literacy* (6th ed.). Sage Publications.
21. Razmetaeva, Y., Barabash, Y., & Lukianov, D. (2022). The concept of human rights in the digital era: Changes and consequences for judicial practice. *Access to Justice in Eastern Europe, 3*(15), 41–56. https://doi.org/10.33327/AJEE-18-5.3-a000327
22. Schwartz, P. M. (2025). Spiros Simitis as Data Protection Pioneer. *George Washington Journal of Law & Technology*, *1*(1), 102–118.
23. Simitis, S. (1999). Reconsidering the premises of labour law: Prolegomena to an EU regulation on the protection of employees' personal data. *European Law Journal, 5*(1), 45–62. https://doi.org/10.1111/1468-0386.00065
24. Siraba, A. (2019). Cyberbullying and online harassment among Facebook users in Papua New Guinea. *Contemporary PNG Studies, 30*, 42–50.
25. Turkle, S. (2015). Reclaiming conversation: The power of talk in a digital age. Penguin Press.
26. Tumber, H. & Waisbord, S. (2017). Media and human rights: Mapping the field. In H Tumber, & S. Waisbord, (Eds.), *The Routledge companion to media and human rights* (pp. 1–14). Routledge.
27. van Dijk, J. A. G. M. (2017). Digital divide: Impact of access. In The International Encyclopedia of Media Effects. Willey. https://doi.org/10.1002/9781118783764.wbieme0043
28. Volodenkov, S., & Fedorchenko, S. (2022). Digital human rights: Risks, challenges, and threats of global socio-political transformations. *Cuestiones Constitucionales*, *1*(46), 279–316. https://doi.org/10.22201/iij.24484881e.2022.46.17057
29. Wuermeling, U. (1998). The first national multimedia law — How Germany regulates online services and the internet. *Computer Law & Security Report, 14*(1), 41–44. https://doi.org/10.1016/S0267-3649(97)88076-4

Information about the author:

Nour Nfissi — L.L.B, LL.M. of Business and Digital Law (Faculty of Law, University Sidi Mohamed Ben Abdelah, Morocco), Ph.D. student, Department of Journalism and Communication Sciences, Faculty of Communication Studies, Autonomous University of Barcelona (Barcelona, Spain), with an international co-supervision with the Faculty of Law, Sidi Mohamed Ben Abdelah, Fez, Morocco.
nournfissi41@gmail.com
ORCID: https://orcid.org/0009-0003-0731-5718

Сведения об авторе:

Нфисси Н. — бакалавр права, магистр бизнес-права и цифрового права (юридический факультет, Университет Сиди Мохаммед бен Абделлах, Марокко), аспирант, кафедра журналистики и коммуникационных наук, факультет коммуникационных исследований, Автономный университет Барселоны (Барселона, Испания) в рамках международного научного руководства совместно с юридическим факультетом Университета Сиди Мохаммеда бен Абделлаха, Фес, Марокко.
nournfissi41@gmail.com
ORCID: https://orcid.org/0009-0003-0731-5718