

The Contributions of the Human Rights Council to Developing International Standards for the Protection of Digital Human Rights

Dr. Fesraoui Hanane

Lecturer (A), Faculty of Law

University Moulay Tahar – Saïda, Algeria

hanane.fesraoui@univ-saida.dz

Received: 16/04/2026 ; Accepted: 20/08/2026 ; Published: 09/09/2026

Abstract

Digital transformation has brought about an unprecedented expansion in the use of information and communication technologies, giving rise to a new generation of rights associated with the digital space including freedom of expression, the right to digital privacy, the right to Internet access, and personal data protection. Against this backdrop, United Nations bodies have assumed a pivotal role in laying the legal foundations and standards for the protection of digital rights. The UN General Assembly has contributed to consolidating recognition of these rights, while the Human Rights Council has emerged as the principal international mechanism for their promotion and protection. Through a series of resolutions and recommendations, the Council has affirmed that rights guaranteed offline must receive equivalent protection in the digital environment—establishing an important normative reference that guides national legislation, despite its non-binding character. This study aims to analyze the role of the Human Rights Council in the protection of digital rights by examining its resolutions, working methods, and contribution to the development of international human rights law in the digital domain, while evaluating the challenges that constrain the effectiveness of this role and identifying mechanisms to strengthen the international protection of digital rights.

Keywords: Digital Rights; Human Rights Council; Digital Privacy; Freedom of Expression; International Standards; Internet Access; Fourth-Generation Rights

Introduction

Over recent decades the world has witnessed a sweeping scientific and digital revolution that has reshaped political, economic, social, and cultural life in all its dimensions. Cyberspace has become a principal arena for the exercise of fundamental rights and freedoms. The Internet is no longer merely a technical means of communication; it has become a public space in which a wide range of rights and freedoms are exercised most notably freedom of opinion and expression, the right to access information, and the right to education—thereby making the protection of human rights in the digital environment one of the central issues of contemporary international law. This reality has given rise to a new cluster of rights, widely referred to as "fourth-generation rights."

Alongside this transformation, new challenges have emerged: mass surveillance, privacy violations, personal data breaches, website blocking, and Internet shutdowns have compelled

international organizations to develop legal and institutional tools capable of meeting these challenges.

In this context, the Human Rights Council has assumed a pivotal role in strengthening the international protection of digital rights, issuing a body of resolutions and establishing reporting and monitoring mechanisms, while mandating Special Rapporteurs to prepare periodic reports on digital violations. These efforts have contributed to the development of the concept of digital rights and to the establishment of new international principles—chief among them the protection of digital privacy and the protection of freedom of expression online. Yet the effectiveness of the Human Rights Council remains a matter of scholarly debate, given the non-binding nature of its resolutions, the dependence of their implementation on states' political will, and the challenges posed by national sovereignty and the rapid pace of technological change relative to the evolution of international law.

The significance of this study accordingly lies in its attempt to assess the genuine role played by the Human Rights Council in the protection of digital rights, and to contribute to the development of international human rights law in ways that are commensurate with the digital environment.

Research Question

To what extent has the Human Rights Council contributed to consolidating international protection for digital rights, and what are the limits and effectiveness of the legal mechanisms it employs to address digital violations?

The overarching question gives rise to the following sub-questions:

- What is meant by digital rights?
- What mechanisms does the Human Rights Council employ for the protection of digital rights?
- How have Human Rights Council resolutions contributed to the development of international law rules relating to digital rights?
- What are the most significant challenges that constrain its effectiveness?

The study concludes with a set of proposals regarding the most effective means of strengthening the international protection of digital rights.

Part I: Digital Rights Emergence and Conceptual Framework

1.1 The Genesis of Fourth Generation Rights

The human rights framework has evolved through successive generations: the first generation focused on civil and political rights (the right to life, liberty, and security); the second encompassed economic and social rights (education, health, housing, and work); the third emphasized collective and peoples' rights (self-determination, peace, development, and the right to a clean environment). The fourth generation, emerging from the digital revolution and technological progress, encompasses digital rights including the right to privacy, the right to personal data protection, the right to Internet access, and rights associated with artificial intelligence.

1.2 The Concept of Digital Rights

With the advent of technology, the development of modern communication tools, and globalization, new concepts have surfaced in the human rights field, the most prominent being

what has come to be known as 'digital human rights.' These rights have been classified by many specialists as belonging to the fourth generation of human rights, or among 'emerging' rights of the contemporary era. Digital Rights are one of the defining features of the current age, having emerged from an information revolution built upon modern technology.

The emergence of the concept of digital rights has necessitated inquiry into their legal foundations and the definition of their content—a task that certain UN bodies continue to pursue, repeatedly affirming that the rights enjoyed by individuals offline are equally protected online.

Some scholars have defined digital rights as: "the individual's right to access and use the Internet, as well as all electronic devices, communication networks, and software without restriction, these rights being connected to the right of access to information, freedom of opinion and expression, the right to privacy, and others" (Al-Azazzi, H., 2025, p. 2695).

Others have defined digital rights as: "those rights which individuals seek to enjoy effectively in the digital world, facilitated by their knowledge of specific digital skills enabling them to participate in digital society, with assurance that these rights are recognized without unwarranted suppression in the digital environment" (AL-Kasassbeh et al., 2024, p. 41).

A further definition identifies them as: "the set of guarantees, freedoms, and privileges enjoyed by individuals and groups when using digital technology and communication networks, whether on the Internet or through various electronic devices" (Ali & Al-Sayyid, 2025, p. 417).

These definitions confirm that digital human rights constitute an extension of the human rights derived from the Universal Declaration of Human Rights (1948) and the two International Covenants of 1966. Most Human Rights Council and United Nations resolutions in this regard have proclaimed: 'that the same rights that individuals enjoy in the real world must also be protected on the Internet.'

Human rights are dynamic and continuously evolving in response to technological and social transformations. The emergence of digital human rights represents one of the most significant manifestations of this evolution, as it transports traditional human rights into cyberspace. These rights enable individuals to access, use, create, and share digital content, to use communication networks and electronic devices, while safeguarding fundamental freedoms—above all the right to privacy and freedom of expression (Shatnawi, Al-Qudah et al., 2026, p. 527).

Digital rights are characterized by their universal character, irrespective of the level of Internet access—which reinforces their universality—as well as their inalienability and their grounding in human dignity. The scope of digital rights encompasses a range of core issues, including privacy and access to information, and aims to achieve a balance between technological progress and the protection of individual rights.

1.3 The Legal Foundations of Digital Rights in Human Rights Council Resolutions

The international community has made considerable efforts to approach digital human rights and to establish a legal basis for their protection, reflected in a range of international treaties and instruments that define and protect human rights in the digital age. These international instruments have established general principles that serve as essential legal building blocks for the protection of numerous digital rights.

1.3.1 The Universal Declaration of Human Rights (1948)

The Universal Declaration constitutes a foundational instrument that recognizes individual rights and guarantees those related to digital technologies. Although adopted in 1948—prior to the digital revolution—its core principles serve as a legal cornerstone for the protection of digital rights. Article 12 focuses on the protection of private life, family, domicile, and correspondence from arbitrary or unlawful interference, including the surveillance of personal data, thereby providing a basis for the protection of digital privacy in the digital age. Article 19 protects freedom of opinion and expression, as well as the right to seek, receive, and impart information and ideas through any media regardless of frontiers (Othman, 2024, p. 783). These provisions of the Universal Declaration constitute the primary legal reference from which the protection of digital rights has derived.

1.3.2 The International Covenant on Civil and Political Rights (1966)

The Covenant provides a robust legal framework for the protection of individuals' fundamental rights, including digital rights. Article 17 protects individuals from arbitrary or unlawful interference with their privacy, family, home, or correspondence, providing a legal basis for digital privacy protection. Article 19 guarantees freedom of opinion and expression, including the right to receive and impart information, with due respect for the rights of others and for national security and public order. This provision is a cornerstone in guaranteeing freedom of access to digital information and expression online; its provisions are interpreted in ways consistent with the requirements of the digital era, thereby obligating States Parties to ensure the protection of individuals and their privacy in the context of contemporary technological developments (Othman, 2024, p. 784).

1.3.3 The International Covenant on Economic, Social and Cultural Rights (1966)

This Covenant guarantees individuals' rights relating to technology and Internet access, and the right to participate in scientific and cultural progress.

1.3.4 The European Convention on Human Rights

This instrument protects individuals' rights relating to digital privacy and digital freedom within the European Union.

1.3.5 The American Convention on Human Rights

Similarly provides guarantees for freedom of expression and the right to privacy in the digital environment.

1.3.6 The Convention on Cybercrime (Budapest Convention)

This Convention aims to harmonize legislation and strengthen international cooperation in the fight against cybercrime, covering a broad range of criminal activities related to information technology, including electronic intrusion, data forgery, electronic fraud, cyber espionage, and Internet copyright offences.

1.3.7 The International Convention for the Protection of All Persons from Enforced Disappearance

This Convention constitutes a legal framework for the protection of individuals and the safeguarding of their identity and personal data. Article 18, for instance, grants relatives and legal representatives the right to access accurate information about a disappeared person, including the place of their detention, their state of health, and the authorities responsible for their fate, so as to guarantee transparency and the right to know. Article 19 prohibits the use of

personal information and medical or genetic data for any purpose other than the search for the disappeared person (Othman, 2024, p. 784), thereby confirming respect for privacy and human dignity. This Convention provides legal protection for identity and personal information even within the context of digital transformations.

1.3.8 International Conventions and Regulations Governing Electronic Commerce (WTO, 1996)

These instruments have contributed indirectly to regulating the rules of digital commercial exchange, concentrating on consumer protection and the security of personal data through encryption and password protection to ensure a safe digital environment (Al-Qabayli, 2024, p. 456).

1.3.9 WIPO Copyright Treaty (1996)

Designed to protect digital intellectual output, this treaty extended the scope of legal protection to cover computer software and databases. It affirmed the need for unified legal frameworks guaranteeing the rights of creators in the fields of literature, arts, and music, while limiting personal violations and preserving global cultural heritage (Al-Qabayli, 2024, p. 456).

Part II: The Working Mechanisms of the Human Rights Council in the Digital Space

The Council operates through several instruments to ensure respect for digital rights within its system of work. The first consists of periodic resolutions that provide a normative reference for states. The second comprises special procedures—Special Rapporteurs, Independent Experts, and Working Groups. The third is the Universal Periodic Review (UPR), to which all UN Member States are subject for the purpose of evaluating compliance with their international human rights obligations. These mechanisms have contributed to expanding the international protection of digital rights through the issuance of resolutions and the development of international standards, the monitoring of violations, the provision of recommendations to states, and the strengthening of international accountability by pressing for regulatory frameworks that oblige states and technology companies to exercise 'due diligence' in protecting individual rights.

2.1 International Resolutions as a Normative Reference for the Protection of Digital Rights

The role of the Human Rights Council is not limited to general recommendations; it extends to constituting a global normative force through resolutions that lay the legal foundations for addressing digital challenges.

The Human Rights Council resolutions on the promotion and protection of the enjoyment of human rights on the Internet reflect the progressive development of international protection for digital rights. Through a sequential series of resolutions, the Council has moved from the simple affirmation of the applicability of human rights in the digital environment to the treatment of more complex issues such as digital surveillance, Internet shutdowns, the digital divide, and digital violence. These resolutions, when analyzed, reveal a gradual evolution in the Council's approach to digital rights.

Analysis of UN Human Rights Council Resolutions on the Protection of Digital Rights

1. Resolution 20/8 (2012): Enshrining the Principle of Equivalence between Online and Offline Rights

This resolution constitutes a fundamental turning point in the trajectory of international protection for digital rights. It was adopted by the Council without a vote, under the title 'The

Promotion, Protection and Enjoyment of Human Rights on the Internet,' in a context of growing international interest in the impact of information and communication technologies on the exercise of human rights (A/HRC/RES/20/8, 2012). The resolution affirmed an important principle that subsequently became one of the most important international pillars for the protection of digital rights: 'the same rights that people have offline must also be protected online.' This means that the exercise of rights such as the right of access to information and freedom of opinion and expression does not lose its legal protection simply by virtue of its transition to the digital environment. The resolution thus expanded the scope of existing rights to encompass the digital domain, establishing the international protection of digital rights on the basis of reinterpreting and applying traditional human rights obligations in ways commensurate with technological progress.

2. Resolution 26/13 (2014): Strengthening International Protection for Digital Rights

The Human Rights Council adopted resolution 26/13 on 26 June 2014, without a vote. It reinforced the direction established by the preceding resolution and deepened international attention to rights and freedoms in the digital environment (A/HRC/RES/26/13, 2014). The key development at this stage was the transition from mere recognition of the principle that human rights apply online to enhanced discussion of the means necessary to ensure the effective exercise of these rights in practice. Theoretical recognition alone is insufficient; a digital environment must be created that allows individuals to access information, communicate, and express themselves without arbitrary constraints.

The importance of addressing the digital divide thus becomes apparent—achieving equality of access to the Internet. Persons who cannot access the Internet due to poverty, geographic location, discrimination, or inadequate infrastructure may find themselves deprived of education, access to information, and participation in public life. International protection for digital rights accordingly encompasses the positive obligation to create conditions enabling individuals to benefit from cyberspace—which is itself indirectly linked to the effective enjoyment of other rights.

3. Resolution 32/13 (2016): Establishing Protection from Internet Shutdowns and Arbitrary Restrictions

Adopted in July 2016, this resolution recognized digital rights as human rights, with the United Nations recognizing Internet access as a fundamental human right (A/HRC/RES/32/13, 2016). The resolution was approved by a majority of states, while China, Russia, Saudi Arabia, India, and South Africa objected, demanding the deletion of a paragraph condemning measures involving the intentional prevention, disruption, or obstruction of access to information. The resolution called for the provision of Internet access while addressing gender gaps and enhancing access for persons with disabilities. It further affirmed that an open information network is indispensable for achieving sustainable development goals through 2030 (Walhi Al-Mukhtar, 2025, p. 394). This resolution emerged at a stage when Internet disruptions and access restrictions had become among the most prominent challenges facing the exercise of human rights in the digital environment. The Human Rights Council unequivocally condemned Internet shutdowns—particularly through this resolution and through subsequent resolutions 38/7 and 47/16. The significant development in resolution 32/13 lies in reinforcing the idea that

restrictions imposed on the Internet must be subject to human rights standards, and must not be used as a means to curtail the exercise of freedoms and rights arbitrarily.

4. Resolution 38/7 (2018): Expanding the Scope of Protection to Address New Digital Challenges

Adopted in July 2018, this resolution was issued in a context of expanding use of digital technology and growing associated risks—including the spread of hate speech, violence, and incitement online, alongside challenges relating to privacy, surveillance, and access to information (A/HRC/RES/38/7, 2018). It highlighted the importance of protecting women and the most vulnerable groups from digital violations. The Council refrained from treating the state as the sole violating actor; violation may be committed by companies, platforms, Internet service providers, and others.

Its most significant provisions concentrated on:

- Combating digital terrorism with human rights safeguards: the resolution expressed concern over the use of information and communication technologies by terrorist groups, while explicitly emphasizing full compliance of counter-terrorism measures with states' obligations under international human rights law.
- The condemnation of deliberate Internet shutdowns during political events or protests.
- Bridging the digital gender gap: the necessity of addressing gender disparities to combat the digital divide.

The Human Rights Council also adopted resolution 31/7, approved on 23 March 2018, under the title 'The Rights of the Child: Information and Communications Technologies and Child Sexual Exploitation,' urging states to take all necessary steps to ensure all children's full, equal, inclusive, and safe access, without any discrimination, to information and communications technologies, and to guarantee the protection of children online and offline from all forms of violence—including sexual violence and violence perpetrated through the criminal misuse of information and communications technologies available on the Internet (A/HRC/RES/31/7, 2018).

5. Resolution 47/16 (2021): Consolidating Protection in the Context of Technological Transformation

Adopted on 13 July 2021 with 43 votes in favour, no votes against, and 4 abstentions (A/HRC/RES/47/16, 2021), this resolution affirms the necessity of continuing to promote and protect human rights on the Internet, and of ensuring the effectiveness of those rights in the context of accelerating digital transformation. Digital rights thus intersect with contemporary issues such as personal data protection, privacy, digital surveillance, the digital divide, artificial intelligence, universal Internet access, net neutrality, encryption, and opposition to censorship and deliberate network shutdowns.

Its most significant provisions included:

- The protection of encryption and digital privacy: acknowledging the security of digital communications—through encryption and the guarantee of anonymity—to enable individuals to exercise their rights securely, free from surveillance.

- The strict condemnation of total Internet shutdowns: the Council denounced all government practices that deliberately sever telecommunications networks.
- A call on states to combat disinformation and to address systematic hate speech online.

The expansion of surveillance technologies prompted the Council to sharpen its positions; it adopted Resolution 42/15 (2019) on the right to privacy in the digital age (A/HRC/RES/42/15, 2019), in which it warned against the unlawful use of surveillance technologies that may undermine freedom of expression. In a related development, the Council adopted Resolution 47/23 (2021) on the right to privacy in the digital age (A/HRC/RES/47/23, 2021), which emphasized the necessity for states to adopt adequate measures to protect individuals from violations of the right to privacy committed by both private companies and governments.

The Council also explicitly condemned Internet blocking and digital censorship, considering them violations of Article 19 of the International Covenant on Civil and Political Rights. The importance of these resolutions lies in the commitment of Member States to harmonize their domestic legislation with these international standards, transforming cyberspace from an arena of impunity into a space governed by the rule of law and human rights.

Resolution 48/4, adopted on 7 October 2021 (A/HRC/RES/48/4, 2021), under the title 'The Right to Privacy in the Digital Age,' reaffirms the human right to privacy—a right under which no one may be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence—and the right to the protection of the law from such interference. It emphasizes that the exercise of the right to privacy is important for the realization of other human rights, including freedom of expression and the right to peaceful assembly and association. The Council's resolution 48/4 further affirms that the same rights enjoyed by persons offline, including the right to privacy, must be protected when they are online. It obliges states to comply with the principles of legality, necessity, and proportionality in any interference affecting the right to privacy, and calls on states to respect the right to privacy in the context of digital communications and new and emerging digital technologies.

Resolution 58/23, adopted on 4 April 2023, concerns human rights defenders and new and emerging technologies—specifically the protection of human rights defenders in the digital age (A/HRC/RES/58/23, 2023).

Resolution 59/11, adopted on 7 July 2023, concerns new and emerging digital technologies and human rights (A/HRC/RES/59/11, 2023).

Resolution 56/19, adopted on 11 July 2024, concerns technology-facilitated gender-based violence.

Resolution 57/6, adopted on 9 October 2024, under the title 'Combating Cyberbullying,' calls on states to take all appropriate measures to prevent and protect children and persons with disabilities from all forms of discrimination, exploitation, violence, and abuse in the digital space—particularly cyberbullying—and to address it immediately in ways consistent with international human rights law.

Resolution 57/29, adopted on 11 October 2024 (A/HRC/RES/57/29, 2024), under the title 'The Promotion, Protection and Enjoyment of Human Rights on the Internet,' constitutes an update of the preceding historical principles. It recognizes the importance of universal and

meaningful connectivity enabling users to access the Internet in a comprehensive, secure, productive, and accessible manner—which is essential for the enjoyment of human rights. It affirms the strengthening of international cooperation to close all digital divides; it stresses the importance of a free, open, and trustworthy Internet; and it condemns all acts of deliberate or arbitrary Internet shutdown or blocking.

Resolution 56/7, adopted on 10 July 2024, focuses on the promotion and protection of freedom of opinion and expression (A/HRC/RES/56/7, 2024). It affirms that freedom of opinion and expression is a right guaranteed to all, including the seeking and imparting of information without regard to frontiers—whether digitally, technically, or in print—and emphasizes that the same rights enjoyed by individuals offline must be fully protected online. The Council expresses serious concern about the targeting of journalists through killings, detention, and violence, particularly in situations of armed conflict. The resolution criticizes the misuse of defamation laws and provisions relating to false information to suppress freedom of expression, as well as digital surveillance and the arbitrary cutting of Internet services. It points to the dangers of the spread of disinformation aimed at inciting hatred; condemns digital divides that deprive women and vulnerable groups of access to information technology; and urges states to revise their legislation to conform with international law and to ensure easy access by individuals to information, particularly in digital form. It also calls on states to adopt policies that protect personal data and the confidentiality of communications—through encryption and anonymization—and encourages social media companies to respect human rights.

The evolution of the Human Rights Council's resolutions may be summarized across five phases:

- Recognition: affirming the principle that rights enjoyed offline receive equivalent protection online.
- Empowerment: improving the conditions for benefiting from the digital environment and addressing the digital divide.
- Confronting arbitrary restrictions.
- Expanding the scope of protection: digital rights protection has become linked to emerging challenges of discrimination, violence, and others.
- Consolidation: integrating digital rights into universal human rights standards and promoting accountability mechanisms.

2.2 The Legal Status of Human Rights Council Resolutions

Despite the importance of the resolutions issued by the Human Rights Council and their contribution to the interpretation and development of international human rights standards—serving as a reference for states when drafting their national legislation and policies relating to cyberspace—they remain, as a matter of principle, resolutions emanating from an international political body that does not possess the direct binding force of international treaties or international judicial decisions. Their effectiveness therefore remains conditional upon the extent to which states are committed to implementing the principles they contain, and upon the capacity of the international community to develop mechanisms for holding states accountable for digital violations. The essential step required in the future is the transition from the stage of enshrining principles and standards to the stage of strengthening mechanisms of

implementation, follow-up, and accountability, so as to ensure that international protection for digital rights is transformed from a normative framework into effective, real-world protection for individuals.

2.3 Core International Principles for the Protection of Digital Rights Established in Council Resolutions

An examination of these resolutions reveals that they have established international legal principles pertaining to digital rights to ensure their application and protection:

- **The Principle of Equivalence in the Protection of Rights and Freedoms between Physical Reality and the Digital Space:** This principle constitutes the hard core of Human Rights Council resolutions. The Council has determined that the rights to which individuals are entitled in the real world must be guaranteed, applied, and protected to the same extent in cyberspace, without any diminution. Digital rights are an extension of traditional rights.
- **The Principle of Availability:** This principle requires enabling all individuals to access information and to use means of communication in all domains without restriction beyond what international human rights law permits, while ensuring access to all necessary devices and Internet communication technologies (Awad, 2021, pp. 46–50).
- **The Principle of Equality in Digital Rights:** This is considered a fundamental principle of digital rights, under which all individuals enjoy equal opportunities to access cyberspace and to benefit from its services without any form of discrimination—fairly and without distinction. This principle is regarded as an extension of the principle of equality in human rights (Awad, 2021, p. 48).
- **The Principle of Freedom to Use, Develop, and Innovate through Technology:** This principle guarantees users the right to access and develop digital technology without arbitrary restrictions, and to participate in the production of technical knowledge and contribute to innovation. It includes the prohibition of arbitrary restrictions on the flow of information. Human Rights Council resolutions have condemned government practices aimed at blocking websites or carrying out wholesale Internet shutdowns, considering these acts a blatant violation of the 'right of access to knowledge'—limiting states' authority to impose restrictions to the very narrow confines permitted by international law, such as combating hate speech and incitement to violence (Awad, 2021, p. 49).
- **The Freedom of Expression:** This principle opens the field to users to express their opinions and disseminate information without violating the rights of others.
- **The Right to Privacy in the Digital Environment:** This principle holds that every individual must have a private sphere for interaction free from interference by any entity, and that others may not be permitted to access their personal data or their private life. Governments, civil society organizations, and large technology companies hosting digital platforms all bear an ethical and legal responsibility to protect user data and to comply with the principles of human rights.
- **The Principle of Transparency in Digital Platforms:** The European Commission has underscored the importance of this principle in the Digital Services Act. It assists individuals by providing monitoring tools that help them detect practices violating their

rights and ensure accountability. All digital platforms must be transparent in their policies and procedures, with the aim of strengthening trust in the digital environment.

2.4 Limitations on the Protection of Digital Rights

The Human Rights Council has played a pivotal role in consolidating international principles relating to the protection of digital rights through the many resolutions outlined above—affirming the need to respect freedom of opinion and expression, the right to privacy, and freedom of Internet access. Nevertheless, the protection of these rights is not absolute; it is subject to a set of limitations to ensure compatibility with established norms. The Council has insisted in its resolutions that restrictions be compatible with the rules of international human rights law, and that they not be used as a means to circumvent fundamental freedoms or to justify arbitrary surveillance, Internet service disruptions, or unlawful monitoring. These restrictions should be grounded in the principles of legality, necessity, and proportionality—achieving a balance between the protection of rights and freedoms on the one hand, and the requirements of national security, public order, and the protection of the rights of others on the other.

Restrictions Linked to National Security

It is well established in legal scholarship that states may restrict certain rights and freedoms under exceptional circumstances—particularly during international or internal conflicts, or natural disasters. This may extend to digital rights, where states may impose restrictions on pages directed against them for the purpose of disseminating ideas that threaten national security, serving the interests of a hostile foreign state, inciting internal disputes, encouraging violence, inciting hatred to provoke civil strife, or spreading chaos and panic among civilians during natural disasters such as wildfires and floods. The exploitation of the Internet and digital freedoms by terrorist groups has also contributed to increased online surveillance both internationally and nationally (Abu al-Wafa, 2008, pp. 104–105).

Restrictions Relating to Cybercrime

Modern communication tools can be misused in ways that threaten the security of society—through electronic piracy, or through activities prohibited by international law such as drug trafficking, money laundering, trafficking in persons, and financial and administrative corruption. These include unlawful use of the Internet for extortion, defamation, fraud, impersonation, and violation of others' honor, reputation, and beliefs. All of this has led states to assert digital sovereignty over websites and to establish mechanisms for limiting their risks. Such risks may justify allowing states to restrict free Internet access, block inappropriate pages, or block those used to disseminate information that would constitute a punishable criminal act—potentially justifying increased state oversight of the free flow of data on the Internet (Al-Sa'di, 2019, p. 365). Those concerned with digital rights have expressed significant doubts about the possibility that these restrictions may be exploited to prevent individuals from exercising their digital rights—particularly since some measures amount to depriving all citizens of Internet access, or blocking certain applications or social media. This has led the Human Rights Council and the Special Rapporteur on freedom of opinion and expression to advocate strongly for digital rights, particularly the right of Internet access, and for the inadmissibility of restricting it except within the narrowest possible legal bounds.

It should be noted that the Human Rights Council does not explicitly mention these restrictions in its resolutions; rather, it calls on states to ensure that any restrictive measures relating to the Internet are compatible with their obligations under international human rights law—particularly Article 19(3) of the International Covenant on Civil and Political Rights—as stipulated in resolution 38/7.

Part III: Special Procedures and the Universal Periodic Review in the Protection of Digital Rights

3.1 The Role of Special Procedures

Special procedures constitute one of the most important mechanisms employed by the Human Rights Council to monitor the state of human rights and to address violations. These procedures include Special Rapporteurs, Independent Experts, and Working Groups, who undertake the tasks of investigation, monitoring, receiving information about human rights violations, conducting country visits, preparing reports, and directing communications to governments concerning violations.

Special procedures have acquired great importance in the field of digital rights, given that the digital environment has become a primary arena for the exercise of the rights and freedoms enshrined in international human rights instruments. The protection of freedom of expression, the right to privacy, and access to information is no longer confined to the traditional domain but has extended to cyberspace—necessitating the adaptation of these mechanisms to encompass violations carried out through technology.

The Human Rights Council, in paragraph 8 of Resolution A/HRC/32/13 (2016), called on states to address security concerns on the Internet in accordance with their international human rights obligations, in order to guarantee and strengthen freedom of expression, freedom of association, the right to privacy, and other rights online—thereby ensuring freedom and security on the Internet so that the network becomes a robust and vital force for economic, social, and cultural development. To this end, the Council appointed a new United Nations Special Rapporteur on the Right to Privacy in the Digital Domain, whose mandate includes reviewing government policies on digital communications, identifying best practices for achieving fair and human rights-consistent global oversight, and contributing to the development of international standards on privacy, freedom of expression, and other rights linked to the digital context. The UN General Assembly has given special attention to 'the right to privacy in the digital age' in this framework (Al-Azazzi, N., 2024, p. 706).

The Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has similarly played a role in enshrining the fundamental principle that rights enjoyed by individuals offline must receive the same protection when exercised online; Rapporteur reports have addressed numerous issues linked to digital rights.

The Special Rapporteur on the Right to Privacy has assumed an important role in developing international standards for the protection of privacy in the digital environment. Reports issued in this domain have contributed to the principle that data collection and processing must be subject to legal principles, and that technological progress must not become a means of violating privacy.

These mechanisms permit Special Rapporteurs to engage in communications with states, issue urgent appeals, and address governments regarding violations—thereby drawing

governmental attention to threats to digital rights and freedoms. Yet the effectiveness of this mechanism remains contingent upon the willingness of states to respond to the appeals and recommendations of Special Rapporteurs, given that these reports and appeals do not possess the same direct binding force as decisions of international courts or resolutions of binding international organizations; their importance lies rather in guiding the policies and legislation of states.

3.2 The Role of the Universal Periodic Review

The Universal Periodic Review (UPR) constitutes a central mechanism within the Human Rights Council system. All UN Member States are subject to periodic review of their human rights situations (UN General Assembly, A/RES/60/251, 2006). The UPR operates on the basis of interactive dialogue between the state under review and other states: the state presents a report on its human rights situation and receives recommendations from Member States aimed at improving the level of human rights protection and the implementation of international obligations.

The UPR has become an important tool for addressing digital rights issues—even though it was not originally established for this purpose—owing to the expansion of the concept of human rights to encompass digital rights. It provides a comprehensive framework for discussing national policies relating to digital rights, and states may present recommendations regarding the need to guarantee freedom of expression online, to refrain from imposing legally unjustified restrictions, to protect individuals from unlawful surveillance, and to guarantee the right to privacy.

The importance of this mechanism lies not only in monitoring violations, but in its capacity to integrate digital rights into national human rights policies, as states may avail themselves of recommendations to develop their internal laws and policies. The effectiveness of this mechanism, however, depends to a significant degree on the voluntary cooperation of states and their acceptance of the recommendations presented to them.

Special procedures and the UPR have thus both contributed visibly to strengthening the international protection of digital rights: special procedures have helped monitor digital violations and develop international standards relating to freedom of expression and privacy, while the UPR has provided a general framework for reviewing states' compliance with the protection of these rights and for presenting recommendations to improve national legislative and institutional frameworks. Yet the effectiveness of these procedures remains contingent upon the cooperation of states and their responsiveness to international recommendations (Al-Farr, 2025, p. 5).

Part IV: Selected International and National Experiences in the Implementation of Digital Rights

4.1 The European Declaration on Digital Rights and Principles (2022)

The European Charter of Fundamental Rights and the European Declaration on Digital Rights and Principles for the Digital Decade (2022) explicitly recognize digital rights as dimensions intertwined with economic and social rights. Chapter II of the Declaration encompasses digital education and training, and explicitly recognizes the 'right to a safe digital working environment'—regarded as a digital extension of constitutional protection and international conventions related to human rights. The European Declaration on Digital Rights

and Principles does not confine itself to enumerating digital rights; it also addresses the duties that authorities must discharge to guarantee these rights (European Commission, 2022).

- The 'right to be forgotten' was incorporated under Article 17 of the General Data Protection Regulation (GDPR).
- The Role of the European Court of Human Rights in the Protection of Digital Rights: The European Court of Human Rights has a successful track record in the general protection of human rights, which has extended to the protection of human rights in digital contexts. The Court has successfully provided effective protection for individuals' rights in cyberspace—notably in matters of mass and indiscriminate surveillance of all users. In the case of *Podchasov v. Russia* (Application No. 33696/19, ECHR, 2024), the Court found that government demands to weaken encryption constituted a violation of the right to privacy under Article 8 of the European Convention on Human Rights (Al-Farr, 2025, p. 85).

These resolutions and international trajectories clearly indicate that digital rights are increasingly acquiring a recognized status as fundamental human rights.

4.2 Algeria

Digital protection in Algeria rests upon a comprehensive legislative framework encompassing privacy and data protection, freedom of communication, cybersecurity, electronic transactions, the combating of cybercrime, and the protection of expression in digital space. This framework begins with constitutional protection for digital rights, as the Algerian Constitution protects a range of rights and freedoms whose effects extend to the digital space.

The Algerian Penal Code contains provisions concerning attacks on automated data processing systems, as well as crimes that may be committed using electronic means—including violations of private life, threats, defamation, and certain forms of offences against persons and property. The Penal Code has undergone recent amendments, including Law No. 24-06 of 28 April 2024. Additional legislation includes: Law No. 09-04 on combating crimes related to information and communication technologies; Law No. 18-07 on the protection of personal data, dated 10 June 2018—subjected to a fundamental amendment by Law No. 25-11 of 24 July 2025, reflecting the evolution of Algerian legislative policy on personal data protection and its adaptation to digital transformations; Law No. 18-04 on mail and electronic communications; Law No. 18-05 on electronic commerce; Law No. 15-04 on electronic signatures and certification dated 1 February 2015—amended by Law No. 26-02 of 17 February 2026 on trust services for electronic transactions and electronic identification; Law No. 20-05 on the prevention and combating of discrimination and hate speech; Decree No. 21-09 on the protection of administrative information and documents; and instruments related to cybersecurity and the security of information systems, most notably Presidential Decree No. 20-05 of 20 January 2020 on establishing a national system for information systems security.

4.3 Egypt

Egypt enacted Law No. 151 of 2020 on the protection of personal data, establishing a Personal Data Protection Center responsible for strengthening privacy and digital security, receiving notifications and complaints related to the provisions of this Law—thereby reinforcing citizens' confidence in the digital economy and constituting a form of protection for digital citizenship (Al-Farr, 2025, p. 9). Egypt also enacted Law No. 175 of 2018 on combating

information technology crimes, which granted the judiciary exclusive jurisdiction over the blocking of websites, stipulating a 72-hour period for a ruling from the moment the matter is placed before the courts. These controls guarantee citizens' digital freedom to create and manage websites and electronic platforms, and ensure that they may not be blocked except by judicial order (Al-Farr, 2025, p. 85).

4.4 Brazil

Brazil is among the states that have explicitly adopted digital citizenship—not merely as a natural extension of constitutionally enshrined economic and social rights, but through explicit legislative enactment. Brazil enacted the Civil Rights Framework for the Internet (Marco Civil da Internet), Law No. 12,965 of 23 April 2014, which enshrines the right of Internet access for all and explicitly affirms that 'Internet access is indispensable for the exercise of citizenship.' It also affirms the right to maintain the quality of Internet connection as contracted. Article 26 constitutionally obliges the state to provide education at all levels and to equip individuals for safe, informed, and responsible Internet use, and to promote the culture and technological development of the Internet as a tool for the exercise of citizenship (Brazilian Law No. 12965/2014).

4.5 United Kingdom

The UK Supreme Court ruled in *Uber BV v Aslam* [2021] UKSC that Uber drivers constitute 'workers' within the meaning of the Employment Rights Act 1996, entitling them to labor rights—including the national minimum wage and paid annual leave. This ruling guarantees the protection of the right to work as a constitutional economic right, affirms the importance of assessing the genuine nature of employment relationships rather than relying on contractual labels, and includes the right to remote work as a fundamental right entitled to all basic labor protections (*Uber BV v Aslam*, 2021 UKSC).

4.6 India

The Kerala High Court adjudicated the case of *Faheema Shirin R.K. v. State of Kerala* (2019), in which a student had challenged restrictions on mobile phone use in college residence hours that had resulted in her expulsion. The Court held that restrictions on the use of mobile phones in student residences constituted an unjustified violation of the right of Internet access, relying on international conventions, and further found that the college was required to guarantee freedom of online expression without discrimination on the basis of gender and to ensure students' access to educational resources. The Court considered the restriction imposed on the female students entirely unjustified and ordered the reinstatement of the student. It further recognized that the right of Internet access has become part of the right to education and the right to privacy (*Faheema Shirin R.K. v. State of Kerala*, 2019).

These judicial decisions confirm that digital rights are no longer isolated from other constitutionally enshrined rights, and that executive authorities bear the obligation to protect digital rights and to guarantee their full implementation, treating them as a natural extension of original constitutional rights.

Conclusion

Digital rights embody a prominent manifestation of the evolution of human rights within the international framework, and attest to the capacity of international human rights law to evolve and respond to all modern forms of rights, as well as to the possibility of providing

international instruments to protect them and to oblige states to take the measures necessary to ensure their implementation.

The trend toward explicitly enshrining digital rights and ensuring their application constitutes an inevitable change in the patterns of daily life brought about by technological progress, and a genuine guarantee of the enforcement of constitutional rights—what is referred to as 'digital constitutionalism' or 'the constitutionalization of the digital environment,' ensuring the concept of digital citizenship and the guarantee of human rights.

The study concluded that international recognition of digital rights continues to face a set of challenges, most prominently the absence of a unified and sufficiently binding international legal framework to regulate all aspects of digital rights. The study further concluded that the protection of digital rights requires greater international cooperation among states, international organizations and their organs, technology companies, and civil society—through the development of shared international standards and effective mechanisms for accountability and enforcement.

Recommendations

- The international community should draft international instruments that ensure the precise regulation of digital rights and treat them as a fundamental set of human rights.
- The concept of digital rights must be clearly defined and delimited.
- Developing countries should receive technological support to develop their digital infrastructure and overcome technical obstacles that hinder the provision of a safe electronic environment—ensuring that all communities may exercise their digital rights equally.
- Human Rights Council Resolution 20/8 remains the most influential historical document in shaping contemporary digital legal scholarship; it drew a clear limit to policies that sought to isolate the virtual space from international human rights oversight.
- National criminal and cybersecurity legislation must be harmonized with the requirements of Resolution 20/8 to ensure that fundamental rights are not curtailed under the pretext of security or informatics.
- National courts should be empowered to draw upon the principles of this resolution when adjudicating cases involving digital publication and expression.
- An internationally binding treaty should be developed, rooted in the principles of this resolution, to regulate digital rights and to protect personal data rigorously.
- Governments must refrain from extending restrictions on digital rights beyond the narrowest scope, and must ensure that any restrictions rest on legitimate and objective legal justifications without impairing the right to their safe and continued enjoyment.
- Although Human Rights Council resolutions are not legally binding, they carry strong normative influence, contributing to the guidance of state behavior, the setting of policies, and the strengthening of advocacy activities for digital rights at the global level.
- Raising awareness among individuals of their digital rights and responsibilities, while strengthening the role of international institutions in monitoring and protecting these rights.

References

- Abu al-Wafa, A. (2008). International protection of human rights within the framework of the United Nations and specialized international agencies. Dar al-Nahda al-Arabiyya, Cairo.
- Al-Azazzi, H. M. K. (2025). Digital human rights in international law. Journal of the Faculty of Sharia and Law in Daqahliyya, (31), December.
- Al-Azazzi, N. M. K. I. (2024). Digital human rights. Legal Journal of the Faculty of Police, Khartoum, 19(1), 685–728. Faculty of Law, Cairo University branch, February.
- Al-Farr, M. S. (2025). Towards an Arab convention on digital citizenship and data protection [Policy paper]. Arab Organization for Constitutional Law, 9th Session.
- Ali, M. S. H., & Al-Sayyid, M. T. (2025). Constitutional protection of digital rights. International Journal of Jurisprudence, Judiciary and Legislation, 6(2).
- AL-Kasassbeh, F. Y., et al. (2024). Digital human rights in Jordanian legislation. International Journal of Cyber Criminology, 18(1), January–June. DOI: 10.5281/zenodo.11201204
- Al-Qabayli, R. R. S. (2024). Digital human rights in international law. Sada al-Jamia Journal of Humanities, 4(2).
- Al-Sa'di, W. N. I. (2019). Digital rights and international protection mechanisms established in the framework of international human rights law. 4th International Legal Issues Conference – ILIC 2019.
- Awad, A. F. A. (2021). Digital rights and freedoms: Legal, technical, and Islamic jurisprudence perspectives. Arab Democratic Center, Berlin.
- European Commission. (2022). European Declaration on Digital Rights and Principles for the Digital Decade. <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>
- Mahni, W. (2020). Digital citizenship and its impact on the promotion of democratic principles and the elevation of digital human rights. Journal of Legal and Social Sciences, 10(4), December.
- Maysaa Othman. (2024). Fourth-generation rights in the digital age: Challenges of the Lebanese Constitution and the role of constitutional justice in their protection. (9th Issue), (87), January.
- Shatnawi, F. O. K., Al-Qudah, Y. A., et al. (2026). Digital human rights and the international protection mechanisms established in international instruments. Indian Journal of Information Sources and Services, 16(2), April–June.
- Walhi Al-Mukhtar. (2025). Digital human rights between international recognition and imposed restrictions. International Journal of Legal and Political Research, 9(3), 394 (pp. 388–412), December.
- A/RES/60/251. (2006). Human Rights Council [Establishing resolution]. UN General Assembly. <https://docs.un.org/en/A/RES/60/251>
- A/HRC/RES/59/11. (2023, July 7). New and emerging digital technologies and human rights. UN Human Rights Council. <https://digitallibrary.un.org/record/4087001>
- A/HRC/RES/58/23. (2023, April 4). Human rights defenders and new and emerging technologies. UN Human Rights Council. <https://digitallibrary.un.org/record/4080898>

- A/HRC/RES/57/29. (2024, October 11). The promotion, protection and enjoyment of human rights on the Internet. UN Human Rights Council. <https://digitallibrary.un.org/record/4064003>
- A/HRC/RES/56/7. (2024, July 10). Promotion and protection of the right to freedom of opinion and expression. UN Human Rights Council. <https://digitallibrary.un.org/record/4059824>
- A/HRC/RES/48/4. (2021, October 7). The right to privacy in the digital age. UN Human Rights Council. <https://digitallibrary.un.org/record/3945627>
- A/HRC/RES/47/23. (2021). The right to privacy in the digital age. UN Human Rights Council. <https://digitallibrary.un.org/record/3936036>
- A/HRC/RES/47/16. (2021, July 13). The promotion, protection and enjoyment of human rights on the Internet. UN Human Rights Council. <https://digitallibrary.un.org/record/3937534>
- A/HRC/RES/42/15. (2019). The right to privacy in the digital age. UN Human Rights Council. <https://digitallibrary.un.org/record/3837297>
- A/HRC/RES/38/7. (2018, July). The promotion, protection and enjoyment of human rights on the Internet. UN Human Rights Council. <https://digitallibrary.un.org/record/1639840>
- A/HRC/RES/32/13. (2016, July 1). The promotion, protection and enjoyment of human rights on the Internet. UN Human Rights Council. <https://digitallibrary.un.org/record/845727>
- A/HRC/RES/31/7. (2018, March 23). Rights of the child: Information and communications technologies and child sexual exploitation. UN Human Rights Council. <https://digitallibrary.un.org/record/836905>
- A/HRC/RES/26/13. (2014, June 26). The promotion, protection and enjoyment of human rights on the Internet. UN Human Rights Council. <https://digitallibrary.un.org/record/775322>
- A/HRC/RES/20/8. (2012, July 5). The promotion, protection and enjoyment of human rights on the Internet. UN Human Rights Council. <https://digitallibrary.un.org/record/731540>
- Brazilian Law No. 12965/2014 (Marco Civil da Internet). (2014, April 23). Civil Rights Framework for the Internet. Republic of Brazil.
- Faheema Shirin R.K. v. State of Kerala. (2019). Kerala High Court, India.
- Podchasov v. Russia. (2024, February 13). Application No. 33696/19. European Court of Human Rights, Strasbourg.
- Uber BV v Aslam. (2021). UKSC 5. UK Supreme Court.