Adv. J. Manag. Humanit. Soc. Sci. (2025), Volume 1, Issue 10, 640-645

Advanced Journal of Management, Humanity and Social Science

Journal homepage: https://www.ajmhss.com/

DOI: https://doi.org/10.5281/zenodo.17914402

The Internet as a Human Right: A Comparative Study

Farshid Imani

Ph.D. student in International relations at The Department of Politics and International Relations, Florida International University, Fiman001@fiu.edu

Article info

Received: 30.10.2025

Accepted: 30.11.2025

Available Online: 30.11.2025

Checked for Plagiarism: Yes

Keywords:

Internet Access; Human Rights; Digital Constitutionalism; Internet Shutdowns; Privacy and Surveillance

ABSTRACT

Each This research assesses whether, and in what manner, broader access to the internet should be recognized as a human right in contemporary international law and practice. It first outlines how established human rights instruments, such as the universal declaration of Human Rights, the international covenant on civil and Political Rights, and regional systems in Europe and the Americas, already link freedoms like expression, information, education, participation, and equality to the right to enjoy the benefits of scientific progress and its applications. Although these documents predate the digital age, they collectively provide strong normative support. This backing helps to conceptualize meaningful internet access as a component of existing rights, rather than as a new, additional entitlement. The manuscript next analyzes how expanding digital infrastructure raises privacy and data protection challenges. It explains the tension between using data collection to serve public interests, such as health or security, and the risks of surveillance, profiling, and discrimination that result. These issues are explored through debates over contact-tracing apps, mass surveillance, and algorithmic control, illustrating their complexities. This investigation shows that, in case studies of China, India, and selected sub-Saharan African states, internet shutdowns and internet control practices operate under distinct political contexts. In all three cases, governments use technical and legal mechanisms to reduce connectivity during protests, elections, or crises. These actions are frequently in violation of their international obligations. The investigation concludes that effective enjoyment of many human rights now clearly relies on secure, affordable, and continuous access to the internet. Future legal and policy reforms at international, national, and local levels must treat internet access and digital connectivity as key conditions of human dignity and democratic accountability.

Introduction

The way we observe the internet has shifted in the last thirty years. It began as a novel technical development and is now a fundamental basis for participation in politics, education, work, and social life. However, access to and control over the internet remain deeply uneven and hotly contested. States, corporations, and international organizations mediate the experience and functionality of the internet. At the same time, individuals rely on their access to exercise and claim rights articulated decades, and even centuries, before the digital age. This raises the question: Should internet access, and an individual's ability to use it freely and securely, be recognized and protected as a human right?

In response to this question, the paper begins by examining how existing human rights instruments and regional human rights declarations provide a normative and legal basis for internet access as a necessary component of existing rights. The paper then examines the relationship between the internet, privacy, and surveillance. It identifies how digital technologies both increase human capacities and place individuals at risk.

Finally, the paper analyzes examples of internet shutdowns and internet control practices in the political contexts of China, India, and selected countries in sub-Saharan Africa. Together, these sections show that the way states govern the internet is increasingly seen as a definitive test of their commitment to human rights.

Corresponding Author:* ***Farshid Imani* *(Email: Fiman001@fiu.edu)*

The Internet as a Human Right in Declarations, Resolutions, and Movements

In 1948, Resolution 217A, the Universal Declaration of Human Rights (UDHR), established core principles. While these principles predate the digital age, they remain relevant to modern issues such as internet access. Articles on expression, information, education, and cultural participation illustrate these foundational rights. Today, these principles support the argument that internet access should be a human right. Article 19 of the UDHR explicitly recognizes the right to access any media without interference as a fundamental right. For example, an activist denied internet access during protests in a restrictive regime demonstrates the importance of a free internet for upholding Article 19. Similarly, articles 26 and 27 show that full participation in education and scientific development is now nearly impossible without internet connectivity [1].

Building on the UDHR, the 1950 European Convention on Human Rights (ECHR) contains articles that support the view that free internet access is a right today. Article 10 ensures freedom of expression and information free from state interference. While 'media' once meant traditional forms, it now includes the internet. This shift is central to the European Union's debates on platform regulation under the Digital Services act. The Convention's protections for education, equality, and non-discrimination (articles 2 of Protocol No. 1, 14, and 12 of Protocol No. 12) closely align with the view that access to these rights now depends on free internet access [2-4].

As the digital era advanced, a key event occurred in the late 20th century: the first successful ARPANET link in 1969. This moment illustrated the evolution of media and laid the groundwork for what we now understand as the modern internet. Meanwhile, human rights frameworks evolved. The American Convention on Human Rights, 1969, like the UDHR, contains provisions that can provide a legal and moral foundation for free internet access. Article 13 covers freedom of thought and expression. It stresses the importance of the "freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, orally, in writing, in print, in the form of art, or through any other medium of one's choice." This right is granted to all. The article suggests that, under this convention, all forms of media, including the internet, qualify as dominant platforms for sharing information today. Article 26 further supports these rights. "Progressive development" obliges states to work toward the full realization of economic, social, educational, and cultural rights. In today's interconnected world, internet access is essential for exercising these rights [5,6].

Continuing the legal evolution, the International Covenant on Civil and Political Rights (ICCPR) entered into force in 1976. It upholds freedom of expression in article 19, including the key phrase "through any other media." This phrase supports the argument that internet access is part of this right. Recent decisions of the UN Human Rights Committee confirm that online platforms are essential for the exercise of freedom of expression. Articles 17,18, and 25 address privacy, participation, and thought, all of which are now closely tied to internet access [6].

Despite predating the internet era, the discussed Conventions and Declarations articulate rights, expression, privacy, education, and equality. Today, these are impractical to achieve without internet access. Taken together, these documents highlight the necessity of viewing internet access through a human rights lens. Though none explicitly recognize internet access as a right, the practical exercise of these rights now relies on it.

Looking beyond global conventions, the African Declaration on Internet Rights and Freedoms states that all Africans should benefit from the development of the internet. It supports an internet that is accessible, available, and affordable as vital for economic, social, cultural, governance, and equality rights. The Declaration insists on internet access as a precondition for key freedoms, condemns shutdowns and discrimination, and calls for equal access and privacy protections [7].

This regional focus is echoed at the international level. A 2016 UN Human Rights Council rapporteur report stressed that article 19 of the ICCPR means free access to information is central to freedom of expression. The report identifies access, search, and sharing of digital information as critical to human rights. Restrictions such as shutdowns or censorship block this and threaten fundamental freedoms. The 2017 follow-up underscores growing risks like vague laws, surveillance, and state suppression of dissent. To ensure internet access, legal and technological solutions, such as community-run mesh networks, are needed to protect online freedoms [8-10].

Recent years have underscored the importance of internet access as a vital right. Human Rights Council Resolution 47/16 states that offline rights must be upheld equally online. Freedom of expression, anchored in article 19 of both the UDHR and ICCPR, is at the core. The resolution identifies internet access as key to the exercise of civil, political, economic, social, and cultural rights. It highlights the internet's role in democracy and public services. The resolution instructs states to ground internet policy in human rights. It opposes shutdowns and censorship as violations of rights. By asking readers to imagine a day without connectivity, the resolution underscores the practical significance of internet access and the need to protect it [11,12].

In addition to state and international bodies, digital constitutionalism, embodied by movements like the Internet Bill of Rights (IBRs), frames internet access as a foundational right beyond formal treaties. IBRs and similar initiatives work to entrench digital rights in line with international norms, emphasizing that internet access is central to dignity, freedom, and equality. These efforts give legitimacy and legal force to the concept of internet access as a right. National models like Brazil's Marco Civil da Internet and Italy's Declaration of Internet Rights expand this consensus, further cementing internet access within the framework of contemporary human rights [13-16].

The Internet, Human Rights, and Individuals' Privacy

Consider the case of Maria, a small business owner in Brazil, who found herself entangled in a digital privacy nightmare. Without her consent, her data was harvested through a seemingly harmless app she used daily for inventory management. This data was later used to target her with misleading advertisements that damaged her reputation within her local community, causing a tangible impact on her livelihood and personal freedom. Digital privacy and data protection are fundamental human rights that require modern legal protection. Current human rights law should adapt to technological advances to prevent exploitation. Practices like digital contact tracing and profiling involve gathering data without consent or transparency, justified by public health but risking rights violations. Such practices expose unaware individuals to discrimination, surveillance, and profiling. Authoritarian regimes often exploit this data against protests, activists, and dissidents. As technology becomes ingrained in daily life, it increasingly impacts human dignity, autonomy, and freedom, which are central to the UDHR and ACHR. Article 17 of the ICCPR upholds the right to privacy and shields against unlawful interference, while the IACHR seeks minimum data protection standards across Latin America to ensure privacy and free internet. Revelations from Edward Snowden and the Cambridge Analytica scandal underscore mass surveillance, misuse of personal data, and weak international legal safeguards [17-24].

The Internet Control and Human Rights

It was supposed that the Internet could help people construct their own communities and identities without geographical or state constraints. However, this perspective was misguided, as states directly or indirectly control the internet. (Brazil's Supreme Court clears way to hold social media companies liable for user content, 2025) In authoritarian regimes, states also use it to repress dissent. Understanding the layers of control reveals a nuanced picture: infrastructure control, where governments manipulate internet backbones and gateways; content regulation, through censorship and control of information; and commercial gatekeeping, influencing through major tech firms. These layers reveal the varied levers governments deploy to shape online freedoms. Nevertheless, the internet can help people bypass censorship, expose human rights violations, and organize protests. These abilities help challenge state power, which is why many scholars believe the internet shifted the balance between state sovereignty and individual liberties. For this reason, authoritarian regimes often resort to internet shutdowns and service disruptions in response to unrest and elections, aiming to suppress protests and block access to information. These actions are commonly justified by portraying the internet as a threat to national security and stability. As a result, internet shutdowns limit access to emergency services, health care, banking, education, and democratic participation. Furthermore, these deprivations violate freedom of expression, access to information, peaceful assembly, and rights to health, education, and work. Violations of the right to information in Brazil are the subject of a new hearing by the Inter-American commission on human Rights (IACHR) in 2024. Based on these declarations and Resolutions, internet shutdowns contradict international obligations and democratic norms. Therefore, states must not cut internet access without a legitimate justification and must ensure universal, affordable, and meaningful access [26-33].

Virtual control refers to government surveillance of individuals' internet communications. While government security agencies often argue that such surveillance is necessary to ensure national security and prevent criminal activities, it often violates human rights, privacy, and freedom of expression. These actions should be critically examined through the lens of proportionality and necessity tests to ensure they align with international human rights obligations. Over time, surveillance regimes have evolved, reflecting the maturation of state mechanisms. Historical methods of oversight have gradually given way to sophisticated artificial intelligence technologies, demonstrating a shift in governance tools and strategies. Government security agencies usually implement such monitoring, either directly or through artificial intelligence technologies, such as algorithmic censorship and biased content moderation. Artificial intelligence is also used by states and technology companies to marginalize specific groups and minorities. Research shows that both authoritarian states (such as China) and democratic nations (such as the United States) exercise significant influence over digital life, shaping political discourse, civic participation, and autonomy. Additionally, major platforms such as Facebook and Google can enable networked authoritarianism by aiding in internet disconnection or censorship [20, 34-42].

Case Studies: China, Sub-Saharan African States, and India

This research examines China, India, Kenya, Nigeria, and Togo, focusing on internet access and human rights in each country. At the outset, it is important to clarify the analytical criteria for comparison: the legal basis for internet policies, technical methods of enforcement, and the social impacts of these actions. Notably, China is authoritarian while India is democratic, yet both have responded to crises with internet shutdowns. In contrast, Kenya, Nigeria, and Togo in sub-Saharan Africa, despite expanding internet use, have also resorted to shutdowns, typically for political reasons. The key contrast is that despite differences in political systems and regional contexts, all five countries display a similar pattern: recent, well-documented internet shutdowns that significantly impact human rights, though the underlying motives and legal justifications often differ.

1- China: Turning first to China, the constitution guarantees freedom of speech. However, the state uses broad definitions of state secrets to justify censorship. The government imposes regulations, monitors online discourse, and pressures journalists through arrests and lawsuits. These actions are carried out through the Central Propaganda and state agencies. Internet censorship occurs through 60 regulations issued by provincial branches of state-owned ISPs. Domestic companies and organizations assist with enforcement. Control has escalated since President Xi Jinping took power. China's censorship regime is strongly supported by restrictive cybersecurity laws and is one of the most advanced in the world. The Great Firewall uses various techniques: DNS poisoning (Cybersecurity Law a rticle 27), IP blocking, URL filtering, blocking VPNs (article59), and deep packet inspection. These actions restrict access to content critical of the Communist Party, to sensitive topics such as the Tiananmen Square massacre, and to many foreign websites, including Google, Facebook, and Twitter [43-48].

Building on this analysis of China's legal and technical approaches, it is notable that the state controls nearly all internet infrastructure and access through the "Great Firewall," making China the world's most repressive country for internet freedom for nine consecutive years, as highlighted by Freedom on the Net reports. The key finding here is the extraordinary breadth and depth of China's censorship and surveillance, including frequent internet shutdowns during politically sensitive moments. Unique among the cases studied, China uses its extensive censorship not only to block anti-state content but also to conceal internal issues such as instability, corruption, and human rights abuses. Multiple state agencies enforce these measures, and the judiciary imposes harsh penalties, ensuring the robustness and effectiveness of the censorship regime. "The sudden cut left us isolated," a Chinese netizen shared, "unable to check facts or express ourselves online." Such personal experiences illuminate the profound personal impact of these systemic actions. In contrast, while other countries implement internet shutdowns, the use of censorship to obscure internal governance issues sets China apart. This analytical distinction sets the stage for exploring how other nations differ in their internet policies and human rights impacts [47].

2- Sub-Saharan Africa: Shifting focus from China to sub-Saharan Africa highlights both similarities and differences in government approaches. Many people in Kenya, Nigeria, and Togo face serious internet shutdowns and censorship. Like China and India, these incidents usually occur during political crises, protests, and other forms of unrest. For example, Kenya's nationwide internet disruption in June 2024, during protests over a finance bill, is the most recent example and caused widespread inconvenience. These governments justify their actions as necessary for national security or public order. However, scholars and experts often argue that these strategies are used intentionally to suppress free expression and prevent people from mobilizing through social media. These actions also disrupt normal communication and prevent people from accessing critical information, undermining several Sustainable Development Goals, such as SDG 9 on infrastructure and SDG 16 on peace and justice [49-52].

To further understand the legal landscape in these African cases, several significant findings emerge at both national and regional levels. Some countries lack domestic laws to protect internet access, while others lack laws to prevent service shutdowns. A key finding from Kenya and Zimbabwe shows that national courts may support or reject shutdowns, reflecting inconsistent legal protections. For instance, in 2018, a Zimbabwean court ruled in favor of shutdowns during protests, citing national security concerns, while in 2022, a Kenyan court rejected a similar move, highlighting the importance of free expression. Regionally, the African Charter and court cases, such as Amnesty International Togo and Others vs the Togolese Republic, confirm that proportionality and legality are essential for restrictions. However, despite such rulings, enforcement remains a challenge. For instance, after the Togolese court ruling, the government continued to impose frequent regional internet blackouts under the guise of security, illustrating a significant gap between legal decisions and actual government compliance. This case, in particular, found that Togo's shutdown violated freedom of expression, reinforcing the critical role of internet access in human rights and the need for strict legal standards before imposing restrictions [53-57].

3- India: Shifting to India, the world's largest democracy, reveals that internet shutdowns during protests, political unrest, and examinations are a major concern. Much like the African cases, these shutdowns are often justified under vague provisions of laws such as the Indian Telegraph Act and Section 144 of the Criminal Procedure Code. *C*ritics argue that the ambiguous language and lack of accountability in these laws allow the government to implement shutdowns without adequate justification. This is particularly concerning when considered alongside article 19(1)(a) of the Indian Constitution, which guarantees freedom of speech and expression to all citizens. The tension between this constitutional right and the discretion allowed by the Indian Telegraph act foregrounds a significant legal conflict. In the last crisis, the government stopped internet and call services in Jammu and Kashmir from august 2019 to mid-2020. During this time, the government revoked Article 370 of the Indian Constitution, stripped the region of its autonomous status, and performed a crackdown by detaining political leaders and deploying tens of thousands of troops. The government ignored a 2020 Supreme Court ruling, "Anuradha Bhasin vs Union of India." This ruling emphasized that internet shutdowns must be lawful, necessary, proportionate, and temporary. The shutdown had negative personal, educational, and economic impacts. The Kashmir chamber of commerce and Industry published a report on economic losses, estimating over $2 billion in losses and the loss of half a million jobs in six months [58-62].

Finally, across all cases, international organizations and scholars consistently find these shutdowns violate international legal obligations, including Articles 19 and 26 of the UDHR and article 19 of the ICCPR. The key contrast is that, while India's broad, ambiguous legal framework enables recurrent shutdowns in a democratic context, China's shutdowns are part of a systematic authoritarian strategy, and African nations implement shutdowns episodically, often around political unrest, in varied legal contexts. Each country undermines access to information and expression, but the mechanisms, motivations, and legal justifications differ widely. Organizations urge urgent reforms and greater transparency across all settings, noting that current practices are inconsistent with democratic or human rights standards, though the nature of the inconsistency varies sharply by context [58].

Conclusion

This paper has argued that major human rights instruments do not explicitly recognize a separate "right to the internet." Yet, effective access to the internet is a prerequisite for realizing freedom of expression, freedom of information, the right to privacy, access to education, and participation. Regional initiatives and movements of digital constitutionalism deepen this connection. They arguably translate these broad principles into concrete legal guarantees, such as access, non-discrimination, and data protection. Conversely, the growth of surveillance, algorithmic control, and commercial gatekeeping demonstrates how digital infrastructures can be weaponized against the rights they were meant to protect.

Case studies of China, India, and sub-Saharan African states show that internet shutdowns or limitations are not exclusive to certain regimes. Authoritarian and democratic governments alike use legal and technical tools to quash dissent, manage crises, or consolidate power. They do this while often violating their own international obligations. Scope, transparency, and remedies may differ, but the human impact is consistent: silenced voices, undermined livelihoods, and weakened democratic oversight. Recognizing internet access as central to human rights requires more than political theatre. Enforceable and powerful domestic laws must be enacted. Independent oversight must be instituted. Regional and international jurisprudence must be established. Civil society must actively make digital technologies serve human dignity, not state control.

Disclosure Statement

No potential conflict of interest reported by the authors.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] Yilma K M. Bill of rights for the 21st century: Some lessons from the internet Bill of Rights movement. The International Journal of Human Rights; 26(4): 701–716, 2022.

[2] Moncau L F, Marrey L F. The Marco Civil da Internet and digital constitutionalism. 2020.

[3] Nobre J C, Soares J C, Huaytalla L R, Granville B O, Zambenedetti L. On the privacy of national contact tracing COVID-19 applications: The Coronavírus-SUS case. arXiv preprint; 2021.

[4] Obladen de Almendra Freitas C, Pamplona D A, Zanetti de Oliveira D H. Duty to protect and responsibility to respect: Data privacy violations in pandemic times. *The International Journal of Human Rights;* 26(8): 1313-1332, 2022.

[5] Humble K P. International law, surveillance and the protection of privacy. The International Journal of Human Rights; 25(1): 1-25, 2021.

[6] Wolfson J. The expanding scope of human rights in a technological world: Using the Inter-American Court of Human Rights to establish a minimum data protection standard across Latin

America. University of Miami Inter-American Law Review; 48(3): 188-231, 2017.
[7] Emmerson B. Mass internet surveillance threatens international law, UN report claims. The Guardian; 2014.
[8] Borges G O, Aguiar G O. Navigating human rights in the digital age: An exploration of data protection laws in Brazil and in Europe. Beijing Law Review; 14: 1772-1789, 2023.
[9] Associated Press. Serbian police use mobile phone spyware to keep track of opponents and journalists, Amnesty says. 2025.
[10] Associated Press. Brazil's Supreme Court clears way to hold social media companies liable for user content. 2025.
[11] Internet Society. Policy brief: Internet shutdowns. 2025.
[12] Axios. Government-forced internet disruptions hit record high. https://www.axios.com/2025/02/24/global-internet-blackouts; 2025.
[13] Reuters. Bolsonaro was main beneficiary in illegal surveillance scheme, Brazil police allege. 2025.
[14] Ryng J, Guicherd G, Al Saman J, Choudhury P, Kellett A. Internet shutdowns: A human rights issue. The RUSI Journal; 167(4-5): 50-63, 2022.
[15] Ziccardi G. Resistance, liberation technology and human rights in the digital age. Springer, 2013.
[16] Goldsmith J, Wu T. Who controls the internet? Illusions of a borderless world. Oxford University Press, 2006.
[17] United Nations High Commissioner for Human Rights. UN High Commissioner for Human Rights says any internet shutdown should be authorized by court. 2022.
[18] Associated Press. Brazil police conduct searches targeting intelligence agency's use of tracking software. 2023.
[19] Ashraf C. Exploring the impacts of artificial intelligence on freedom of religion or belief online. The International Journal of Human Rights; 26(5): 757-791, 2022.
[20] MacKinnon R. Consent of the networked: The worldwide struggle for internet freedom. Basic Books, 2012.
[21] MacKinnon R. Liberation technology: China's "networked authoritarianism". Journal of Democracy; 22, 2011.
[22] Reuters. Brazil authority suspends Meta's AI privacy policy, seeks adjustment. 2024.
[23] Human Rights Watch. Brazil: children's personal photos misused to power AI tools. 2024.
[24] Algorithmic arbitrariness in content moderation. arXiv preprint; 2024.
[25] CIVICUS, Digital Democracy Initiative. Advancing digital democracy: A policy and advocacy framework for global action. 2023.
[26] Reuters. Brazil turns facial recognition on rioters despite racism fears. 2023.
[27] Xu et al. Study on Chinese internet control and censorship (full reference details not provided by author); 2017.
[28] Hoffman. Study on Chinese internet regulation (full reference details not provided by author); 2016.
[29] Sallycroft. Study on Chinese internet censorship (full reference details not provided by author); 2015.
[30] Time. The Tiananmen massacre is one of China's most censored topics: Here's a look at what gets banned. 2019.
[31] Time. Global internet freedom declines, aided by AI. 2023.
[32] Reuters. China court jails journalist for seven years on spy charges, family says. 2024.
[33] Kenyans.co.ke. Communications Authority of Kenya assures public there will be no internet shutdown. 2024.
[34] Oginga A, Udo Udoma & Belo-Osagie Advocates. Regional and national laws on internet shutdowns and legal mechanisms in sub-Saharan Africa. Media Defence; 2024.
[35] Mintz J. Analysts troubled by trend of internet, social media shutdowns in Africa. Voice of America; 2024.
[36] Access Now, KeepItOn coalition. Emboldened offenders, endangered communities: Internet shutdowns in 2024. 2024.
[37] Media Foundation for West Africa. Togo: Internet disruptions amid post-protest repression. 2025.
[38] ECOWAS Court of Justice. Amnesty International Togo and Ors v. The Togolese Republic. 2020.
[39] Global Freedom of Expression. Amnesty International Togo and Ors v. The Togolese Republic.
[40] The Guardian. Zimbabwe high court orders government to restore full internet. 2019.
[41] Mwamuye, Bahati. Court blocks government, mobile operators from shutting down internet. Citizen Digital; 2025.
[42] Human Rights Watch. "No internet means no work, no pay, no food": Internet shutdowns deny access to basic rights in "Digital India". Human Rights Watch; 2023.
[43] Sherman J. Kashmir internet shutdown continues, despite Supreme Court ruling. The Diplomat; 2020.
[44] Asia Times. India revokes Kashmir's special status. 2019.
[45] Lawful Legal. Anuradha Bhasin v. Union of India: Internet shutdowns and the digital dimensions of free speech. 2020.
[46] India Today. Kashmir turmoil: Mobile internet services snapped in Jammu and Kashmir, security tightened. 2019.