

Digital Rights as Emerging Human Rights: Privacy, Freedom and Access

Dr. Arpuda Raju¹ & Dr. Shashikumar²

¹Assistant Professor, Vidyavardhaka First Grade College, Sheshadri Iyer Road, Mysuru, Karnataka

²Assistant Professor, Chilukuri Nageswara Rao Gov't First Grade College, Sriramanagara, Gangavathi Taluk, Koppal District, Karnataka

Abstract:

The rapid expansion of digital technology has transformed how individuals communicate, work, and participate in civic life, prompting a reassessment of established human rights frameworks. This article examines digital rights centered on privacy, freedom of expression, and access to the internet as an emerging category of human rights increasingly recognized in international law and policy. Drawing on United Nations resolutions, regional instruments such as the European Union's General Data Protection Regulation and Artificial Intelligence Act, and recent empirical data from the International Telecommunication Union, Freedom House, and Access Now, the article traces how the principle that rights enjoyed offline must also be protected online has shaped international norms since 2012. It examines the persistent digital divide, the global rise in internet shutdowns and surveillance, and the tensions that arise as these three rights intersect. The article concludes that although substantial normative progress has occurred, digital rights remain under-enforced, unevenly distributed, and increasingly contested amid the growth of artificial intelligence and biometric surveillance, and it calls for stronger binding legal frameworks, meaningful connectivity investment, and sustained civil-society monitoring.

Keywords: Digital Rights, Human Rights, Privacy, Freedom of Expression, Digital Divide, Internet Governance, Data Protection, Internet Shutdowns.

Introduction

Since the Universal Declaration of Human Rights (UDHR) was adopted in 1948, human rights law has developed

largely around entitlements framed for analogue world civil, political, economic, social, and cultural rights exercised

Please cite this article as: Arpuda Raju & Shashikumar. (2026). Digital Rights as Emerging Human Rights: Privacy, Freedom and Access. *SRUJANI: Indian Journal of Innovative Research and Development*, 5(4), 19–27

through physical presence, print media, and face-to-face association. The emergence of the internet and digital communication technologies since the 1990s has introduced a new dimension to this framework, one that a growing body of scholarship describes as a “fourth generation” of human rights (Song & Ma, 2022; Risse, 2021). Digital rights are not an invented category detached from prior law; rather, they represent the application and adaptation of long-standing rights privacy, expression, association, and access to information to an environment shaped by ubiquitous connectivity, mass data collection, and increasingly autonomous algorithmic systems.

This article focuses on three closely interlinked dimensions of digital rights: privacy, freedom of expression and opinion, and access to the internet itself. Each has drawn sustained international attention over the past decade and a half, from United Nations resolutions declaring that offline rights extend online, to regional regulatory instruments such as the European Union's General Data Protection Regulation (GDPR) and Artificial Intelligence Act. Yet formal recognition has not translated into consistent protection: global internet freedom has declined for fifteen consecutive years (Freedom House, 2025), internet shutdowns reached a record high in 2025 (Access Now & Keep It on Coalition, 2026), and roughly 2.2 billion people remain entirely offline (International Telecommunication Union

[ITU], 2025). This article situates digital rights within human rights theory, examines each of the three pillars in turn, analyses the legal frameworks that govern them and the gaps in their enforcement, and concludes with policy recommendations.

Methodologically, the analysis draws on a doctrinal review of primary international instruments (UN General Assembly and Human Rights Council resolutions), regional legislation (EU regulations), and a secondary synthesis of recent empirical monitoring reports from intergovernmental and civil-society organizations, integrated with academic literature on the theoretical status of digital rights.

Digital Rights as an Emerging Category of Human Rights

The classical taxonomy of human rights, developed by Karel Vasak in the 1970s, divides rights into three generations: civil and political rights (first generation), economic, social, and cultural rights (second generation), and collective or solidarity rights such as development and a healthy environment (third generation). Contemporary legal scholarship increasingly argues that digitalization has produced a fourth generation of rights connected to digital identity, algorithmic governance, and what some scholars term epistemic rights rights to reliable information and protection from manipulation in digital environments (Risse, 2021). Song and Ma

(2022) frame this shift around the emergence of digital identity as a new object of legal protection that requires dual mechanisms in both public and private law, given the imbalance between individuals' right to access information and the concentration of data control among a small number of corporate actors.

Rather than treating digital rights as entirely new entitlements, most international bodies have adopted an equivalence principle: that the rights people enjoy offline must be equally protected online. This principle first appeared in a 2012 UN Human Rights Council resolution the first of its kind which affirmed that free-expression protections under Article 19 of the International Covenant on Civil and Political Rights (ICCPR) apply regardless of medium and characterized the open internet as a driving force for development (UN Human Rights Council, 2012). The Council reaffirmed this principle in subsequent resolutions in 2014, 2016, 2018, and 2021, progressively expanding its scope to address digital divides, gender-based restrictions, encryption and anonymity, and the responsibilities of internet intermediaries such as social media companies (UN Human Rights Council, 2016, 2021).

Privacy in the Digital Age

Privacy has arguably received the most sustained international legal attention of the three pillars examined here. The

catalyst was the 2013 disclosure of mass electronic surveillance programs, which prompted the UN General Assembly to adopt Resolution 68/167, The Right to Privacy in the Digital Age. The resolution reaffirmed privacy as a human right under Article 12 of the UDHR and Article 17 of the ICCPR and, for the first time, explicitly linked privacy violations unlawful or arbitrary surveillance, communications interception, and mass data collection to interference with freedom of expression, describing both as threats to the foundations of democratic society (UN General Assembly, 2013). A follow-up resolution in 2017, Resolution 71/199, extended this reasoning to metadata, recognizing that aggregated metadata can reveal sensitive details about an individual's behaviour, relationships, and identity even without interception of communications content (UN General Assembly, 2017).

At the regulatory level, the European Union's GDPR, effective since 2018, has become what commentators describe as the de facto global benchmark for data protection, shaping subsequent legislation in Brazil, Canada, and a growing number of U.S. states, alongside comprehensive frameworks emerging in Japan, South Korea, and Singapore (Force point, 2026; Privacy Perfect, 2026). However, 2026 marks what analysts describe as an inflection point for this model. The European Commission's proposed "GDPR Omnibus" reforms, introduced in November 2025, would narrow the

definition of personal data and explicitly embed artificial-intelligence consideration into data protection law for the first time, ending what had previously been a technology-neutral approach (Future of Privacy Forum, 2026). This shift is occurring alongside the phased rollout of the EU Artificial Intelligence Act, which imposes penalties of up to €35 million or 7 percent of global turnover and becomes fully applicable in August 2026 (Kiteworks, 2026).

Privacy concerns have also intensified around biometric surveillance. The EU AI Act bans several “unacceptable risk” applications, including real-time remote biometric identification by police in public spaces, emotion recognition in workplaces and schools, and indiscriminate scraping of facial images to build recognition databases, although broad exceptions remain and enforcement mechanisms are still developing (European Digital Rights, 2024; Privacy International, 2025). The UN High Commissioner for Human Rights has separately called for a moratorium on facial recognition in public spaces until adequate safeguards exist, citing accuracy disparities that disproportionately affect women and people with darker skin tones, along with the broader chilling effect that mass surveillance exerts on free expression and assembly (is4.ai, 2026).

Freedom of Expression and Information Online

The second pillar, freedom of expression and access to information, has

followed a more troubled trajectory. Successive Human Rights Council resolutions since 2012 have condemned government measures that intentionally disrupt access to, or dissemination of, information online, and have called on states to formulate national internet policies grounded in universal access and human-rights principles (UN Human Rights Council, 2016, 2021). Despite this normative consensus, empirical monitoring paints a starkly different picture. Freedom House's Freedom on the Net 2025 report found that global internet freedom declined for the fifteenth consecutive year, with conditions deteriorating in 27 of 72 countries assessed and improving in only 17 (Freedom House, 2025). Notably, this decline was not confined to authoritarian states: half of the eighteen countries rated “Free” experienced score declines during the coverage period, including Georgia, Germany, and the United States, while at least 57 of the 72 countries monitored recorded arrests or imprisonments for online expression a record high (Freedom House, 2025).

Internet shutdowns represent one of the most direct infringements on both freedom of expression and access. The #KeepItOn coalition, coordinated by Access Now, documented at least 313 shutdowns across 52 countries in 2025, surpassing the previous year's record and meaning that some part of the world experienced a shutdown on every day of the year (Access Now & Keep It on

Coalition, 2026). Conflict remained the leading trigger, accounting for 125 shutdowns across 14 countries, while a newer tactic has emerged: rather than severing connectivity entirely which imposes steep economic costs, estimated at \$19.7 billion globally in 2025 governments increasingly block specific platforms or disrupt satellite-based alternatives such as low-earth-orbit internet services, which were interrupted fourteen times across seven countries in 2025 alone (Access Now & Keep It On Coalition, 2026).

Content moderation introduces a further complication: platforms and states alike face the challenge of curbing hate speech, incitement, and disinformation without disproportionately silencing legitimate expression. Automated moderation systems, deployed at the scale of billions of posts daily, frequently generate errors that disproportionately affect marginalized communities and non-English speakers (is4.ai, 2026). Regulatory responses such as the EU's Digital Services Act attempt to impose accountability on large platforms for systemic risks to fundamental rights, marking a shift toward treating intermediaries as bearing direct human-rights responsibilities rather than acting purely as private commercial actors.

Access to the Internet as a Foundational Right

The third pillar access is both a precondition for exercising the other two

rights and a distinct area of unmet need. According to the ITU's Facts and Figures 2025 report, approximately 6 billion people, or about three-quarters of the global population, were using the internet in 2025, up from 5.8 billion the previous year (ITU, 2025). Yet 2.2 billion people remained entirely offline, with 96 percent of them concentrated in low- and middle-income countries. The report documents persistent, multidimensional divides: 94 percent of people in high-income countries use the internet compared with just 23 percent in low-income countries; 85 percent of urban residents are online compared with 58 percent in rural areas; and a modest but persistent gender gap remains, with 77 percent of men online globally compared with 71 percent of women (ITU, 2025).

Importantly, ITU researchers emphasize that connectivity is no longer solely a binary question of access versus non-access; it increasingly concerns "meaningful connectivity," defined by speed, reliability, affordability, and digital skills. Even in high-income countries, gaps in advanced digital skills such as problem-solving and safe online behaviour can exceed 30 percentage points between the most and least educated users, while mobile broadband remains unaffordable in roughly 60 percent of low- and middle-income countries despite falling median prices (ITU, 2025). This reframing matters for a human-rights analysis because it shifts the policy question from simply connecting

the unconnected toward ensuring that access translates into genuine enjoyment of expression, information, and participation rights.

Intersections and Tensions among the Three Pillars

Although privacy, freedom, and access are frequently treated as parallel policy tracks, they are deeply interdependent and, at times, in tension with one another. The 2013 and 2017 UN privacy resolutions explicitly recognized that surveillance threatens not only privacy but also freedom of expression, since individuals who believe they are being monitored tend to self-censor (UN General Assembly, 2013, 2017). Conversely, measures ostensibly designed to protect one right can undermine another: content moderation intended to protect users from harassment or disinformation can suppress legitimate speech, and national-security justifications for internet shutdowns or biometric surveillance often override both privacy and expression simultaneously. Meanwhile, expanding access without corresponding privacy and safety protections risks exposing newly connected populations already among the more vulnerable to heightened risks of surveillance, fraud, and exploitation. A comprehensive digital-rights framework therefore requires treating these three pillars holistically rather than as isolated policy silos, recognizing that progress on one dimension can either reinforce or

come at the expense of the others depending on how it is implemented.

Legal and Institutional Frameworks

At the international level, digital rights derive primarily from Articles 12 and 19 of the UDHR and Articles 17 and 19 of the ICCPR, as elaborated through the UN General Assembly's privacy resolutions and the Human Rights Council's internet resolutions. These instruments carry significant normative weight but remain non-binding, relying on state goodwill, periodic reporting, and civil-society advocacy rather than direct enforcement mechanisms.

Regional frameworks have moved further toward binding obligations. The European Union's regulatory architecture the GDPR, the Digital Services Act, and the AI Act represents the most comprehensive attempt to translate digital-rights principles into enforceable law, backed by substantial financial penalties for non-compliance (Kiteworks, 2026). National frameworks vary considerably in both substance and enforcement. India's Telecommunications Act 2023, for example, formalizes procedures for internet-shutdown orders, requiring that justifications be published and limiting the duration of any single order, even as the country recorded 65 shutdowns in 2025 the highest total among the world's democracies (Vision IAS, 2026). The United States, meanwhile, continues to rely on a patchwork of state-level privacy statutes in the continued absence of

comprehensive federal legislation, with twenty states having enacted comprehensive privacy laws as of 2026 (StormyCloud, 2026).

Emerging Challenges

Several developments complicate the trajectory of digital-rights protection going forward. First, the growing integration of artificial intelligence into governance and commerce is reshaping privacy law itself, as reflected in the EU's proposed narrowing of what constitutes personal data to accommodate AI training needs (Future of Privacy Forum, 2026). Second, a wide enforcement gap persists between normative commitment and practice: internet shutdowns and content restrictions continue to rise even as states formally endorse resolutions condemning them. Third, digital repression is no longer confined to authoritarian systems; established democracies have also contributed to recent declines in internet freedom, suggesting that erosion of digital rights is not tied to any single form of government (Freedom House, 2025). Finally, biometric and algorithmic surveillance technologies continue to advance faster than the legal frameworks meant to govern them, with facial-recognition deployment continuing even where formal restrictions exist, particularly in law-enforcement and border-management contexts (Privacy International, 2025).

Recommendations

Based on the foregoing analysis, several policy directions merit

consideration. First, states should move toward binding international commitments on digital rights rather than relying solely on periodic, non-binding resolutions, potentially through a dedicated protocol addressing internet shutdowns and mass surveillance. Second, investment in affordable, meaningful connectivity rather than basic access alone should be prioritized, with particular attention to rural populations, low-income countries, and the persistent gender gap documented by the ITU. Third, regulatory frameworks for artificial intelligence and biometric technologies should embed human-rights-by-design principles from inception rather than retrofitting safeguards after deployment. Finally, sustained support for independent civil-society monitoring such as the work of Freedom House, Access Now, and the #KeepItOn coalition remains essential to maintaining transparency and accountability, particularly as funding for such monitoring has come under increasing pressure in recent years (TechPolicy.Press, 2025).

Conclusion

Digital rights have moved, over little more than a decade, from a peripheral concern to a recognized extension of established human-rights law. The principle that rights held offline must be equally protected online now commands broad international consensus, reflected in successive UN resolutions and an expanding body of national and regional legislation. Yet the empirical record

documented in this article fifteen consecutive years of declining internet freedom, a record number of internet shutdowns in 2025, and 2.2 billion people still offline demonstrates that formal recognition has outpaced substantive protection. As artificial intelligence, biometric surveillance, and algorithmic governance continue to reshape the digital environment, the task facing states, regulators, and civil society is not to invent new rights but to enforce privacy, freedom of expression, and access to the internet with the same seriousness historically reserved for their offline counterparts.

References

- Access Now & #KeepItOn Coalition. (2026). *Rising repression meets global resistance: Internet shutdowns in 2025*. Access Now.
- European Digital Rights (EDRi). (2024). *How to fight biometric mass surveillance after the AI Act: A legal and practical guide*.
- Forcepoint. (2026). *Global data protection laws in 2026*.
- Freedom House. (2025). *Freedom on the Net 2025: An uncertain future for the global internet*.
- Future of Privacy Forum. (2026). *2026: A year at the crossroads for global data protection and privacy*.
- International Telecommunication Union. (2025a). *Global connectivity report 2025*.
- International Telecommunication Union. (2025b). *Measuring digital development: Facts and figures 2025*.
- Is 4.ai. (2026). *Top 10 AI and human rights issues in 2026: Global ethics perspectives*.
- Kiteworks. (2026). *Global data privacy laws 2026: Cross-jurisdiction compliance guide*.
- Privacy International. (2025). *Toward regulation: Addressing the legal void in facial recognition technology*.
- PrivacyPerfect. (2026). *Global trends in privacy, security and AI regulations in 2026*.
- Risse, M. (2021). *The fourth generation of human rights: Epistemic rights in digital lifeworlds* (HKS Faculty Research Working Paper No. RWP21-027). Harvard Kennedy School, Carr Center for Human Rights Policy.
- Song, L., & Ma, C. (2022). Identifying the fourth generation of human rights in digital era. *International Journal of Legal Discourse*, 7(1), 83–111.
- Stormy Cloud Inc. (2026). *Understanding your digital rights in 2026: A guide to the resources that matter*.
- Tech Policy Press. (2025). *Global internet freedom declines for 15th consecutive year*.
- United Nations General Assembly. (2013). *The right to privacy in the*

digital age (Resolution 68/167, A/RES/68/167).

- United Nations General Assembly. (2017). *The right to privacy in the digital age* (Resolution 71/199, A/RES/71/199).
- United Nations Human Rights Council. (2012). *The promotion, protection and enjoyment of human rights on the Internet* (Resolution A/HRC/RES/20/13).
- United Nations Human Rights Council. (2016). *The promotion, protection and enjoyment of human rights on the Internet* (Resolution A/HRC/RES/32/13).
- United Nations Human Rights Council. (2021). *The promotion, protection and enjoyment of human rights on the Internet*.