**InSight Bulletin: A Multidisciplinary Interlink International Research Journal**
Peer Reviewed International, Open Access Journal.
*ISSN : 3065-7857 / Website: https://ibrj.us / Volume-2, Issue-3 / March - 2025*

Original Article

# Redefining Human Rights in the Digital Age

**Dr. Kalpana M. Kawade**
Associate Professor, Department of Social Work, Sushilabai Ramchandrarao Mamidwar College of Social Work Chandrapur

**Manuscript ID:**
IBMIIRJ -2025- 0203031

**Submitted:** 09 Feb 2025

**Revised:** 01Mar 2025

**Accepted:** 16 Mar 2025

**Published:** 31 Mar 2025

ISSN: 3065-7857

Volume-2

Issue-3

Pp. 156-170

March 2025

***Correspondence Address:***
*Dr. Kalpana M.kawade*
*Associate Professor, Department of Social Work, Sushilabai Ramchandrarao Mamidwar College of Social Work Chandrapur*
***Email:*** *kawadekalpana19@gmail.com*

OPEN ACCESS

Quick Response Code:

Web. https://ibrj.us

DOI: 10.5281/zenodo.15847663
DOI Link: *https://doi.org/10.5281/zenodo.15847663*

Creative Commons

***Abstract:***

*The digital era has profoundly transformed the landscape of human rights, introducing both unprecedented opportunities and critical challenges. This paper explores how information and communication technologies (ICTs), digital surveillance, data privacy concerns, and the rise of artificial intelligence are reshaping traditional conceptions of human dignity, agency, and freedom. From the redefinition of civil liberties in cyberspace to the emergence of new digital rights such as the right to internet access and digital identity, the analysis underscores the urgent need to adapt international human rights frameworks to the digital context. Drawing on global case studies, international policy frameworks, and ethical considerations, the study evaluates how state and non-state actors negotiate power in digital environments. It concludes with recommendations for global cooperation, regulatory reform, and inclusive digital governance to ensure that fundamental human rights remain protected and relevant in the evolving digital landscape.*

***Keywords:*** *Human Rights, Digital Age, Information and Communication Technologies, Data Privacy, Digital Surveillance, Internet Access, Digital Identity, Cybersecurity, Artificial Intelligence, Ethical AI,*

## Introduction to Human Rights

The universality of human rights is a powerful and contested idea. The assertion that every person, no matter where or when born, is entitled to certain fundamental rights and freedoms has become a standard against which much political and social action is judged. By virtue of this assertion, every person has dignity, agency, and a position as the subject of entitlements and aspirations. But this idea of human rights rests on contested conceptions of the human in the context of history and social-political-economic thought. Questions about the type of being one is and relevant for whom, and who is relevant for the moral community to which one seeks inclusion are contested and have consequences (Goggin et al., 2018). The demand for recognition and entitlements rests on a vision of the collective subject of that recognition. Are the collective campaigns to claim quadrants of human rights for the global poor, for women ignored, for racial outsiders, new communications citizens, peoples stripped of their land and language, or for other entities in various ontological normativities relevant to considerations of being human? The foundations of the moral imperative of respect for human rights were laid in the transition from caste, servitude, and pre-modern hierarchies to civil societies in which each person was seen as possessing, by virtue of their humanity, the dignity of an abstract political-economic being disposed to rights in relation to one another. This vision of the human was as a capacity and craving for freedom, acting rationally in the pursuit and enjoyment of a life of flourishing, by being and existing in particular places and contexts that affirmed and fostered that being and flourishing.

**Objective:** To examine the transformation of human rights in the digital age and propose strategies to protect emerging digital rights."

Methodology:

This research adopts a **qualitative, analytical, and interdisciplinary methodology**. It involves critical analysis of academic literature, international human rights documents, legal frameworks, and digital rights case studies. The study utilizes **doctrinal legal research** to examine human rights norms in relation to digital technologies and explores the **impacts of ICTs, surveillance, and data privacy** through thematic content analysis.



***How to cite this article:***
*Kawade, K. M. (2025). Redefining Human Rights in the Digital Age. Insight Bulletin: A Multidisciplinary Interlink International Research Journal, 2(3), 156–170. https://doi.org/10.5281/zenodo.15847663*

It also includes **comparative and interpretive approaches** to highlight variations in digital rights recognition and enforcement across different countries and regions. Case studies from the USA, EU, Asia, and Africa illustrate the practical implications and challenges of human rights in digital contexts.

**Historical Context of Human Rights**

Social movements, especially in the new "media and network" paradigm in which current information is essentially created, circulated and evaluated at a speed, scale and complexity that did not exist before, have the potential to better articulate existing injustices, and to reach greater numbers of people producing an engagement that was not possible before. However, it is important to retain a critical perspective on the existing structural impediments of new communication technologies that create and reinforce systemic inequalities, in particular addressing power structures that deny voices on whose behalf and in whose name advocacy is made in the media (V Spickard, 2017). After the Second World War, there was extensive debate in the newly formed United Nations Organisation (UN) about the protection of human rights. Various treaties were written by governmental representatives and specialists, and they had to be ratified by parliaments everywhere for them to take effect. There was no guarantee that the intolerance and mass murders of the 1930s and 40s would not be repeated, however. At the same time, representatives of civil society organisations, particularly women's groups and representatives from an increasing number of nation states from Latin America, Africa, and Asia, and participation by specialists, such as anthropologists, helped determine strong but vague principles and norms. The substantive and procedural duties of civil and political, and economic, social and cultural rights were delineated, and monitoring mechanisms were established including a UN Commission on Human Rights, which was made up of governmental representatives. One strength of the model was that it offered a single international standard of human rights and a mechanism for reporting how and how well nation states complied with their obligations. The UN acknowledged civil society organisations as vital partners in these ventures. This is why the UN must make its agenda relevant to local communities and women and youth, or else this invaluable potential will be lost in the current power struggles, as it is already happening. An Agenda for Humanity must reach everyone, or the UN's legitimacy will be called into question as it endorses ignorance of the local context.

**The Impact of Technology on Human Rights**

The advent of information and communication technologies (ICTs) and social networks has profoundly impacted the traditional conceptual framework of human rights in societies all around the globe. During the past two decades, the proliferation of the Internet increased manyfold the number and variety of human rights violations. State authorities, individuals, and non-state actors alike have been abusing communication technologies to undermine the right to security, the right to development, the right to education, the right to privacy, the right to freedom of thought and conscience, the right to freedom of expression and debate, the right to access to information, and the right to peaceful gathering and to healthy dissent, as well as non-derivative rights to impunity.

In addition, new ICTs and socially unattended social networks might be construed as associated rights in themselves. There is a growing consensus regarding the recognition of the right to the Internet, the right to broadband, access to the Internet as a universal service, and access to a safe cyberspace as a human right (Karanicolas, 2012). In April 2006, the Brazilian government established Internet as a human right, and Lima was the first city in the world to declare free access to the Internet as a social right of its citizens. At the macro level, growing power asymmetries between State and non-State, authority and non-authority, and public and private continue to shape the accessibility of communication technologies and networks in many places. Cross-chain abuse of communication technologies, networks, and contents is fueling political violence and intolerance. A pervasive and top-down culture of fear driven by sub-state, state, and transnational actors is transforming political dissent, and democratic voices are becoming increasingly unsafe. The global free flow of information also means the free flow of misinformation, incitement, intolerance, and violence. Many individuals, especially women and those from minority communities or marginalized sectors, face consistently growing ciber-victimization as they communicate or engage in socio-political expressions.

**1. Digital Surveillance**

Digital technology provides unprecedented opportunities to many people. At the same time, new technologies for social control, censorship, and surveillance also emerge. Surveillance is the collection, retention, analysis, and dissemination of personal information with the purpose of monitoring, controlling, or predicting an individual's behaviour (María García Sanz, 2014). To ensure supply chain integrity, biometric screening, and large-scale screening of personal information, facial recognition, geolocation services, and large-scale profiling must be addressed in human rights. Surveillance is taking place in a context where the state is losing its monopoly on surveillance technologies; where new technologies for regulation, control, and punishment are emerging; and where the growing international circulation of information and data begins due to trade, economics, migration, and finance (W. Chan, 2019).

Surveillance markets can be divided into three types, each corresponding to three power relations. The first is the political economy of social grading and surveillance, corresponding to the social grading and policing regime. The social grading operates under the assumptions of invigilability and morbid curiosity, and assumes that one can be grasped through objective measurable data. It also purports to be objective, though it is often used for covert discrimination. The second is the expansion of monetary surveillance, which includes monitoring and determining people's credit-worthiness. This market of surveillance materializes in the form of primary commodity markets and other surveillance products that would group people according to credit risk; the latter is also found in Money Laundering Regulations. This is where the "know your customer principle" emerges and where anti-money laundering provisions also effect and facilitate wholesale surveillance.

The third is the commercialized surveillance of private life information containing intimate details about age, gender, sexual preference, and hereditary diseases. These surveillance products to re-engineer realities correspond to a moralistic

discourse, and are often disseminated through anti-hacking legislation. Project Facilitate within the United Nations' initiative may be defined as an era of "surveillance capitalism" or "big data surveillance". The political dangers, along with potential political solutions, are newly emerging questions that transnational human rights scholars need to grapple with urgently.

**2. Data Privacy**

Data privacy is a fundamental right that every individual worldwide should enjoy freely, regardless of their region. The recognition of data privacy as a fundamental right is vital in the contemporary increasingly globalized world, in which an overwhelming amount of different kinds of data (personal or not; sensitive or not) are produced on a daily basis. The interpretation of the expression data privacy in the United Nations Declaration of Human Rights should be updated and expanded to ensure the protection of data privacy in all kinds of contexts—from international organizations to social media platforms. While international documents have acknowledged privacy as a right many decades ago, the protection of privacy in its informational dimension is recent. Technological developments, especially those related to the Internet, in recent decades have brought the need for the protection of personal data privacy to the fore (J. Gstrein & Beaulieu, 2022). Personal data is a new form of official 'information' in a society in which it is incredibly important. The concept of 'information' has always varied; it has been understood as the knowledge shared, but also as an entity of certain value (in the case of trade secrets, for example). We must preserve our history as individual citizens and define who we are in society. Also, the consumption of different information shapes attitudes and feelings and is linked with the commodification of such personal data, as in the case of news agencies. Governments should limit their activities regarding the collection of citizens' data to strictly necessary objectives of state responsibility. Routinely gathering and keeping logs about people's daily life would be contrary to privacy's nature (María García Sanz, 2014). Special attention should be given to states' access to private sector data. These companies gain access to a person's whole life and accompany them almost everywhere, which underlines their relevance in the monitoring and controlling of human activity. Data privacy, as a human right, as any other right, has a title holder that must be an actor able to access and exert them. Privacy is an individual human right, whose exercise protectively rests with the vivendi's subject. However, privacy is usually understood in non-individual terms. Group privacy might refer to commercial interests, to social networks or to a group of very private photos that an individual subject does not want to share with others.

**Emerging Digital Rights**

The notion of digital rights is gaining prominence in various political and public arenas, alongside calls for greater accountability of tech companies. Kaye acknowledges that issues around digital rights concern the continuing promise of the internet and the expansion of platforms. However, occasions for the discussion and debate of digital rights have often been considered when liberal democratic institutions and states appear unable to respond adequately to challenges like political extremism, hate content, and corruption (Goggin et al., 2018). This yields a number of technical solutions to a series of political issues. Wanting to ensure the affordances of the internet are better mobilised for pressing social issues is welcomed, but it takes for granted certain assumptions – that existing international laws, norms, and institutions are sufficiently able and/or legitimate to grapple and act appropriately.

The emergence of a digital rights agenda in the region is of critical theoretical and empirical significance. Evidence is growing for an expansion of a set of issues concerning the demands for digital rights across a number of Asian locations. There is also precedent for similar sorts of agenda forming in concert with broader movements for the adjudication of rights and the social need for governance of different domains, such as media or internet rights. As a broad summary, the issues that emerge are grouped under three overlapping themes and the concerns and worries, often phrased in terms of rights. They incorporate the role and responsibilities of the state in digital spaces. First, an aspect of the democratic health of nations and their governance systems is that a citizenry participates, and also has the right to participate, in some or all public life, often through the form of political agency such as the vote.

**1. Right to Internet Access**

While there may be debates as to whether or not there is a recognised stand-alone right to access the Internet, both during and outside of the General Assembly debate on a Right to the Internet, there have been many important steps taken by UN, EC, and other regional bodies towards recognising Internet access as a prerequisite for enabling rights (Karanicolas, 2012).
The State must take all necessary means, including through collaboration with relevant private satellite operators, to restore telecommunications and Internet access services to the region in the shortest possible timeframe, facilitating free and accessible communications (accessibility, anonymity); refrain from forced Internet shutdowns, content removal, blocking of platforms, or harassment of businesses or telecommunications providers; and the protection of individuals' human right to freedom of expression and access to information is vital to the spread of truth and the ability to hold authorities accountable.

Perhaps the most important advance towards recognising a right to Internet access has been the establishment of a duty of the State not just to ensure physical access to the Internet, but to guarantee the rights of all members of society through access to the Internet. Not all States have simply been granted new duties under the existing set of rights. New duties spelt out in existing rights are enumerated expressly as stand-alone rights with State duties directly drawn from them; thus, both the role of infrastructure in exercising rights and the weight of the duty of the State to provide that infrastructure have been supplemented.

**2. Freedom of Expression Online**

Although references to freedom of expression online and offline employ similar language, the confluence of regulatory, technological, and social aspects of the Internet creates a ripe breeding ground for the non-negotiable limits to free speech that have never been widespread or even conceivable outside cyberspace. Progression from denial and/or lack of discourse regarding the social networking tools themselves to concurrent debates and negotiations on ways forward have popularised previously fringe rights advocacy postures. Everyone has undergone a journey toward acceptance of the digital as equal to the real. Talk of a digital

world, or a cyberspace is now common parlance. States, corporations, and civil society should welcome the dissolved clear-line divides between the "real" and "digital" spheres as digital content produced in the "real" ordinary lives of human beings. ontent moderation driven by monopolistic US-based web companies/services in collusion with States has consolidated into a regime of extra-judicial sanctions whereby the publishing, redistributing, and receiving of information by millions of individuals, communities, institutions and states occurs on a basis of non-appealable, non-disclosable rules, criteria, and procedures. These developments however invite contestation. Problems relating to extra-territorial and excessive state information control measures on their own are formidable challenges for collective, duty bearer accountability. Pro-actively establishing good human rights practices, institutions, discourses, frameworks for cooperation, and systems for collective action should be a priority. Individual utopian imaginings of an Internet run by people, or States free of private sector interference, coupled with individual dystopian imaginings of a common space run exclusively by large technology corporates do not capture the realities of the contemporary virtual present. As such, these visions fail to frame the digital human rights protection discourse for contestation. Understanding the Internet as an equal to non-digital channels of communication, as well as the need for States to fulfil their duty to respect and protect rights, duties, and business responsibilities as they apply in the physical world is critical. What varied, yet complementary duties rights bearers of all types, including intergovernmental, private sector, national, and local actors, should have to protect the rights of individuals in the digital sphere is integral to the quest for accountability (Karanicolas, 2012) (P. Karanasiou, 2013).

**3. Digital Identity Rights**

The digital society has transformed the way every human being lives, uses technology, and connects to others. The Internet has become a basic need and a fundamental resource for all. In this digital world, online platforms, such as social networks and e-business sites, are responsible for initiating actions with other people or organizations. This is true for both individuals, businesses, and things, since any object can now connect to the Internet and exchange data. Deciding and authorizing actions on an online service or platform involves managing an "Identity." The notion of identity is very diverse and has different facets. The offline identity is connected to the civic identity, which is unique to every individual globally. The rise of digital twins and of the Internet of Things (IoT) generates new facets of identity (STEPHANE & HENNING, 2017). In cyberspace, an identity is a deep, parallel, complex, and constantly evolving representation of the offline one (Hardjono, 2019). The identity in cyberspace is multidimensional. It contains static elements that can evolve linearly, such as the legal name of a person, and dynamic ones related to how an entity interacts online with others. This digital identity is enriched by attributes, which can be personal, blogger, and observer, among others; and is continuously renewed and expanded. The determination of action authorization is an intimate endeavor of every entity, for which it uses its own identity. The levels of anonymity in cyberspace influence perceived responsibility and risks of abuse, which varies according to user status. The more anonymous an identity is, the more careless are the actions undertaken through it. There is a tight link between identity, rights over objects, and trust, which impacts the Internet services offered, leading to asymmetric data protection.

**Challenges to Human Rights in the Digital Sphere**

A key aspect of the attention digital rights have received in relation to the digital environment, and examination of the global and regional concepts of 'digital rights.' With the rapid emergence of new standards for trusted international engagement on technology and governance, state and state-funded bodies are increasingly looking through a human rights prism at questions about new frameworks and regulatory regimes (Goggin et al., 2018).

In this light, it is significant that the foundational principles of human rights are yet to exert sufficiently coherent influence upon the global conceptions of digital rights. These issues include whether the distinction between protection from interference and provision of access still holds for social rights in the digital environment. The rights agenda has of necessity been largely reactive, following the evolution of rapidly changing socio-technical interfaces as issues arise. A series of reactive international discussions about the issues, events and technologies that prompt discussion. These have ranged from net neutrality, surveillance and information warfare, through algorithms, filters and internet censorship, to platform responsibility. In turn, national concepts of digital rights emerged, largely but not exclusively responding to local deliberations as they unfolded, with examples in India around the Aadhar biometric identification program, Myanmar around access to the internet, China around the 'Great Cannon' system to attack and pressure dissident websites, and diverse scrutiny of Facebook's actions in Brazil, India, the US, and elsewhere. The new transactional relationships emerging in the digital domain come into being as a consequence of both deliberate intent in their design and execution and unintended effects shaped by use and abuse. The genesis, evolution and elaboration of these relationships occur within complex frameworks of public rationality, formal and informal rules and procedures, histories of technological adoption, paths of cultural convergence and divergence, and systemic properties of technological and social infrastructures. These national and international 'digital agendas' are unfolding across the backdrop of a complex evolution of social, mobile, locative and other digital media platforms. It is from this vantage point that the signifier 'digital rights' is salient.

**1. Cybersecurity Threats**

Even in the digital age, human rights are directly linked to technology. Nowadays, rapid technological development is changing human life significantly. This speeds up the human right to development. However, technology can also be abused by anyone for non-peaceful activities which violate human rights. Therefore, citizens, civil societies, and human rights activists are often victims of threats against human dignity, life, liberty, security, and more. This should be properly discussed from the viewpoint of new technologies. Each individual has the right to be free from cyber threats which violate his or her rights. Human life is essential for all human rights. Each life has dignity; the chief task of governments in society is to protect all lives in safety, from the womb to the grave. In non-peaceful conditions, many human rights such as life, dignity, and safety tend to be ignored. Online threats can be classified into four groups: first, non-state actors attempting to take other lives or human dignities through threats against other people's lives. Second, a group of persons threatening others' dignity through publicity. Third, technological

threats against the social system and services. Fourth, threats against a nation-state by other states. Some states use non-state actors to attack the target states. This leads to the disintegration of human rights protection mechanisms, and human rights violations are severely repeated. All computer networks have vulnerabilities. Even one bug can be the greatest threat to a human society; great attackers with better thinking or equipment are born. Since the digital age arrived, cyber-attacks against human rights have increased rapidly. Cyber-attacks against non-state actors have also increased, and human rights activists are victims of such attacks at present. Therefore, nation-states are obliged to take preventive measures against cyber-attacks. Recently, governments and non-state organizations have started to discuss protective measures from a technical viewpoint because anonymous attacks of unknown sources have increased.

**2. Misinformation and Disinformation**

Political misinformation, defined as false or misleading information, can severely disrupt democratic processes. In addition to that, the phenomenon and the underlying process of disinformation should be better understood and analysed to make the fight against it more effective. Disinformation has been extensively studied over the last few years but is still often mislabelled, misunderstood, and misused. While sometimes political communication, false or defamatory information, and scandal are used as synonyms, in fact, they are distinct phenomena. In some cases, general disinformation processors groups or platforms are used to refer directly to "fake news," while in addition to that term, a variety of more scholarly ones such as misinformation, disinformation, and mal-information are also used in European discourse (MASSIMO et al., 2019).

The last two terms are somewhat contradictory. Disinformation is both the process of producing and spreading the false information itself and the underlying motivation to mislead, fool, annoy, or entertain. Misinformation, on the other hand, refers solely to false information spread without ill intent. For example, a newspaper publishing the wrong numbers of an election results would be an case of misinformation. The main underlying motivation of disinformation is the perception, ideally justified, of a threat felt by a (real or actual) attacker, spillover from interpersonal or social conflict. This perception can operate at different levels: from individuals to social groups, structures and countries. Dissonance is one possible outcome of such perception, resulting in attempts to debunk certain pieces of information and "going against facts" (e.g., people denying climate change, or believers of the flat Earth theory). In this case, the quantity of information in circulation actually increases. Unanswerable or ungraspable perception of threat can lead either to amnesia or adaptation (where an affected group still remembers the information, but regards it as irrelevant in making sense of daily life).

**International Frameworks for Digital Rights**

In March 2016, a report on privacy on the Internet and social platforms warned that contemporary search engines, social media, cloud computing, and e-mail networks were increasingly "intrusive and unaccountable." Companies increasingly enjoy "privileged access to personal information, translating regulatory power largely unaccountable to the public." It is difficult to enhance policies or regulations intended to stem online abuses without regard for the power of such companies. An obvious implication is that a successful rights agenda must target companies, and while there are some efforts of that sort, it is also clear that such an agenda must move beyond the companies themselves. The rights of individuals, free of harming disclosure of information, criminalisation of opinions or associations, coercion of individuals through surveillance, the need for an independent judiciary, ownership of personal information, and far more, are all unpleasantly applicable to such companies.

This text opens with an overview of digital rights today – addressing their definition, implications, actors involved, and comparisons made to existing rights. Next is a discussion of the frameworks of the rights agenda. It is emphasised here that consideration must be given not only to corporate practices, regulatory failure, and governmental overreach but also to the rights, voices, activities, and responsibilities of individuals, groups, civil society, and others. The text concludes with a discussion of the broad implications of the above analysis. It requires thinking ahead with regard to the ever-dramatically evolving rights agenda and suggests that rights are at least partly socially constructed. Contemplation of the broader social character of rights can help make them more effective. Exclusive focus on states and other actors ends up marginalising significant responsibilities, rights, and voices.

Contemporary information and communication technologies are rapidly transforming the global environment, affecting the relationships of individuals, communities, organisations, and states. These socio-technical transformations are giving rise to new types of governance involving rules, actors, practices, and technologies. Many of these regimes are celebrated and welcomed as democratising, empowering, and liberating forces shaping a new digital age. Others are more problematically interrogated, usually couched in terms of concerns: corporate influence, infrastructure monopoly, privacy and surveillance, system abuses, and civil liberties. The former advances towards cyberutopia, while the latter defensive strategies reflect fear of technological dystopia.

**1. United Nations Initiatives**

Concerns regarding privacy and data protection, media plurality and diversity, and public interest scrutiny over digital platforms, to name a few, have burgeoned in the public discourse in Europe, North America, Latin America, Asia, and elsewhere. At the same time, however, a more careful analysis of these concerns, framed in the language of rights claims, remains remarkably muted. As this last point indicates, the fundamental principles of human rights are yet to exert coherent influence upon global conceptions of digital rights. While such an agenda continues to emerge, it is focused primarily on the remediation of injustices posed by the evolution of socio-technical interfaces, raising a plethora of other issues—what each might mean and where they might lead is yet to be fully examined.

Specific worries regarding privacy, data protection, information access, social security, digital literacy, media plurality, civic rights, the digital divide, and public safety have coalesced in apprehensions over the homogenising threat of Big Data and the inadequacy of legal, institutional, and policy frameworks regulating digital telecommunications, media, and applications. As a public policy agenda, the recognition of digital rights is an attention to the conditions needed for safe, just, and satisfying usage

and application of evolving digital technologies and communications. At the same time, it is an agenda rife with complexity and contradiction, an emerging set of economic and political engagements embodying competing interests and philosophies. Digital rights issues are unfolding: they range from basic literacy rights to protective rights against the surveillance economy; from participatory rights in public interest scrutiny over digital apps, platforms, sites, and gateways to economic rights in the form of open data; and from employment battles against the precarity of gig economies to the exclusion of certain populations from the data economy.

Although scant parallels can be drawn between these diverse settings, a geography of situations is observable that is delineated by differences in the rush move to or cornering of personal data. In cases where digital rights agendas begin to emerge in the wake of privacy and data protection concerns, activism is challenging existing legal regimes, creating claims against incipient practices of automation, and tightening existing broad mandates on access and disclosure. In cases queased to more permissive regimes presently engendering uneven and inequitable formations arising from the concatenation of data, data activism is emerging and targeting new behaviours, forms, and futures now reconfigured by data (Goggin et al., 2018).

**2. Regional Human Rights Instruments**

The Constitution of the Republic of South Africa enshrines digital rights as a source of equality, dignity, and freedom in offline and online environments. This compact instrument seeks to establish and clarify a range of rights and principles relevant to digital rights discourse. The 10 principles of digital rights (i.e. access, security, privacy, decency, openness, quality, inclusion, freedom of expression, multistakeholder governance, and ethical use of technology) can be explicitly grounded in contemporary duties and obligations. These principles reinforce the initial system understanding, but collectively deepen understanding of the context at hand. Therefore, they can be useful to explore the regional scope and impact of CCDM. Applications of the 10 digital rights principles can be examined in relation to wider discourse around their regional and global relevance, associated governmental commitments to respect and protect digital rights, and the values of political, institutional, and societal actors. The division of powers is arguably a way to impose limits on public authority, thus avoiding tyranny. However, the fact that state organs employ an excessive degree of power is a fact in many developing nations across the region. Tools of oppression are being developed through technology and used against citizens. Requests for amendments to draft legislation regulating the Digital Green Certificate indicate a need for states to be humble concerning transformation.

As countries in Africa use digital technologies to exert social control, there is an urgent need for collaborative multi-stakeholder agendas to restrict governmental encroachments upon citizens' dignity, equality, and freedoms. There is a parallel need to explore the sustaining or extending functionality of authoritarianism in an age of digital deprivation and the Africa-centred agency of states to defy global expectations for the public or social internet. The Commission on the Status of Women is the primary global intergovernmental body dedicated exclusively to the promotion of gender equality and the empowerment of women. In addition to working on the theme of digital violence against women, it also drafts important implications on how digital media may be used to silence dissent and distract from other issues of state capture in Africa. Such power dynamics provide an important counterbalance to attempts at further restrictive legislation globally, regionally, and around gender issues (Goggin et al., 2018).

**National Legislation on Digital Rights**

Digital rights are becoming more prevalent in international dialogue, as possible components of human rights have yet to exert sufficient influence upon the evolving conceptions of digital rights in Asia, despite calls on the UN and UNESCO from various stakeholders (Goggin et al., 2018). In particular, the evolving rights agenda has been somewhat reactive; following up the evolution of a wide array of socio-technical interfaces as issues arise and gain the attention of activist, academic, media, and government actors. However, digital technologies raise issues that should not be thought of in terms of new rules or conditions that merely arise from the use of the physical systems, information, interfaces, and properties of computers. The concerns around privacy, subscription, and public safety are all features of the conventional public spheres and the public rights and responsibilities that should apply there. The new sets of transactional relationships now constructed in the digital domain are so for a reason. They have been deliberately designed and executed, but their operation also generates a wide array of unintended effects. New international and national digital rights agendas are coming into existence alongside this complex evolution of media platforms and cultures. There is thus a pressing need, realization, and expertise to conceive of a comprehensive agenda for the role and rights of citizens in the digital domain across Asia. A growing number of issues, concerns, agendas, and debates are emerging concerning the arena of digital rights—particularly those focused upon, or relevant to, the role of the state in and for digital spaces. The past decade has seen a dramatic increase in debate and agitation around the set of issues arising concerning the political economy of social media platforms, their role in public governance and democratic processes, and their accountability to jurisdictions. Debates concerning the set of issues, responsibilities and possible components of international human rights pertaining to the digital space have flourished over the last six years, especially at the UN General Assembly and across significant regional and national forums and treaties. Responses to the introduction of new technologies have also emerged, focusing on the increasing importance of Internet telecommunications to social order and public information; the emergence of fresh regimes of credentialisms and recognitions; the pervasive importance of national borders; and the condition of great-power competition and cyberwar.

**1. Case Studies: USA**

America has historically been the first place to celebrate freedom of expression and the sacrosanct civil and political rights. Although it paved the foundation of the guarantee of civil and political rights, using its own acculturation on new technologies to elevate social and economic rights, it subsequently neglected expeditious approaches to protect them. While the degree of social welfare in America is on par with Brazil and other developing countries, using state-of-the-art control mechanisms on civil and political rights, Holocaust survivors were rudely denied repair in America. The establishment of a human rights

system outside the legal cordon of a civil society, however, proved much less effective in the face of state power. Post-911, the United States lost law and sovereigns, which is reflected in its irreversible social problems, mainly manufacturing a large number of political subjects against the state (W. Chan, 2019).

The mass surveillance operation of Edward Snowden burst open the overburdened legislation and technical limitations in protecting the basic rights of American citizens. This technological deficiency also affects people on sites outside America, leaving American companies at liberty to evade the legislation. Under underwhelmed legal administration, a national human rights institution in non-judicial government agencies is expected to take over the task of adjudicating a invasive mass surveillance and cyber weapons, as well as seeking redress and regulation reform. The accountability of government electronic monitoring is incumbent on a third-party institution. Protesters and whistleblowers, the first liability subjects, must be provided a safety net of both instrumental binding mechanism and pragmatic anti-retaliation provisions.

**2. Case Studies: EU**

221 The World Summit on the Information Society took place in two phases. The first, in Geneva from 10 to 12 December 2003, focused on strategies. The second, in Tunis from 16 to 18 November 2005, addressed the internet governance issues. A great number of persons representing many actors took part in both phases; however, most people didn't have, or still don't have, the capability and the capacity to express themselves in the internet and to benefit from it through a regular pc connected to broadband. This situation creates new divides and conflicts in a world already torn by fragmentations and fights for rights. Poverty and economic development are the underlying issues of the WSIS. WSIS is also a great opportunity to raise issues regarding cultural diversity, language rights, gender equality, environmental and social sustainability, participation in processes, and democracy. The associative or civil society is often seen as one of the major side of this new multilateral, multi-stakeholder process. The actors of this side take many forms, from social movements to NGOs in many fields of action. However, most of the civil society actors don't see the WSIS, the process that led to it, or its outcome as a gift but as a bitter process because it was pushed mainly by the North, by national governments who think mainly about their strategic interests, by political correctness, by diplomats, and as an attempt to sideline the civil society actors and exclude their rights and demands. The adherence to principles, agreements, and declarations process at the WSIS is probably/will be named as the process of channeling and domesticating dissent. Such a huge global event raises a huge number and variety of questions. The contradictions between the lawyers and the dissidents, the critiques of the monitoring procedure, and the actors who define the post-WSIS era will shape in many ways the internet and the society in which people live. The question who speaks for whom is present. The WSIS could be regarded as an economic, political, technical, cultural, environmental, linguistic, and social threat; however, it could also be posed as an opportunity to raise demands, claim rights, and rethink ways to organize oneself by taking advantage of the dialogue and the conventions that governments and the working groups offered or will offer.

**3. Case Studies: Asia**

In contrast to the Afro-Asian basis of writing human rights into the United Nations Charter and the Universal Declaration of Human Rights as a culturally relevant and non-Western instrument, the differences over freedom of expression, privacy, and other topics are significant. While there are commonalities across national/regional borders, large-n sociolinguistic variation still exists with regard to the main concepts to which human rights are attached in domestic law. The picture of these similarities and differences is, however, complicated by the interaction of the public order in the real world and the digital age. Internet/human rights issues have been more visible in Asia as states have cracked down on dissent via technology. Despite ongoing censorship, citizen journalists, and attempts to stay anonymous are plenty, which indicates the significance of freedom of the press while at the same time challenges to it are formidable. As regards state security, the presently emerging boundaries seem to reinforce the in-group/out-group divide: Western vs. the rest; domestic vs. foreign. These differences may be manifested in the level of NATO's operations, in cyber defense funding for militaries, and in the upper hand of governments in controlling cyberspace. Questions about the future of democracy and the dissimilarities across countries arise: to what extent will blatant intolerance prevail in presently non-existent democracies? Additionally, what will the prospects for post-democratic regimes who also utilize digital media to mobilize their followers? The status of the net as a new space of the public sphere – unlimited debate or a vicious flood of hatred? The inevitability of accompanying digital spaces with preconditions for a healthy public sphere is still a matter for further discussion (Goggin et al., 2018).

Digital nation-building within digital spaces has been a classic case study for examining the boundaries of freedom of expression, privacy, and other human rights. With the advent of digital spaces, social media and other IT have become indispensable tools for politicians and diplomats to reach out to foreign colleagues, fellow citizens, and the public. The widespread access to cyberspace and the increase in the number of digital devices made the online participation of transnational cyberdissidents possible, while also opening up new venues for netizens to hold governments accountable. A privacy breach case study during the 2013 Korean presidential campaign revealed an unintended excess of political freedoms. Yet, with the new forms of liberties and communications came new abuses. By rationalizing the concept of national sovereignty as encompassing cyberspace, many governments have been able to attain unilateral control over what citizens may utter, read, and click. Additionally, increasingly sophisticated AI systems coupled with algorithmic and machine learning have led to a competitive arms race developing social control not only intra-nationally but also globally. The continuing interactivity of the Internet has meant a counter-attack as well. Powerful tools such as VPNs, the Darknet, and even simple bitching continue to be invented, despite governments' public efforts to suppress digital dissent.

**Role of Civil Society in Advocating for Digital Rights**

Digital rights, broadly speaking, encompass diverse rights issues concerning technologies that create, handle, and exchange digital materials. Like human rights, digital rights are universal moral values possessing strong historical and

institutional legitimacy. Institutions, actors, and activities who claim a digital right do so in connection with a technology governance issue. Such claims stem, in part, from the external, unintended consequences of the design and operation of the technology in question. There has been a proliferation in the number and diversity of rights claims linked to digital means and technologies, but with insufficient unity and coherence. The digital rights landscape is structurally fragmented and ambiguous, with no dominant institutional framing or international governance mechanism for digital rights (Goggin et al., 2018). The scope and nature of digital rights is in pressing need of clarification. A pressing concern in many regions is the consolidation of private control of data and digital systems, and the nexus of the data and software for social monitoring with state power and agency. This scope needs to take into account global public goods broadly defined. Initial discussions have suggested multiple frames for viewing digital rights claims: as "additional" to human rights, as new rights claiming on the one hand; and as analogous to human rights on the other. In the latter case, the challenge is to ascertain the applicability of human rights frameworks and resourcing to the diverse landscape of digital rights issues.

Patterns of institutional recognition of digital rights issues and claims are following paths similar to the trajectories of human rights. The questions behind this claim concern the types of digital rights issues or claims that have been recognized, and the institutions that have done so. Institutional recognition began or soon emerged with organizations focusing on digital technology governance, such as the Internet Society and the Association for Progressive Communications. There are two strands in the emergence of institutions focused on digital rights: advocacy organizations focused on the political aspects of information and communication technologies or the Internet, enabled and supported by the emergence of digital platforms; and advocacy organizations addressing cultural issues in digital technology.

**1. Grassroots Movements**

A new wave of human rights energy is evident in campaigns for rights disaggregation on a local level led by local authorities. The emergent grassroots movements highlighting a diverse canon of rights are often horizontal, fluid in terms of leadership and movements, and adept in the use of social media. These local movements develop a strong local base that intertwines with intersectional coalitions. The movement for racial justice, in the wake of the killing of George Floyd, shows how coalitions that mobilize around a specific cause can resonate with other campaigns built around core rights, address the culture of impunity, and highlight the critical role of local governments in regulating the policing of the community (Smith, 2017). With COVID-19, new interconnected local avenues for using digital technologies for grassroots solidarity and rights disaggregation emerged. The experience of black and radical care campaigns both at the local level—the flourishing mothers' and children's rights movement in the municipalities of São Paulo—and at the transnational level—new anti-racism and pro-rights water movements globally gripped the 61st Session of the UN Commission on the Status of Women (CSW61)—highlighted that access to new technologies alone does not yield rights realizations (Díaz-Romero, 2013). It would require forging a cogenerative and coalition memory connecting women's rights to those pressing for racial justice, economic equity, healthcare access, and protection from violence. It entails deeper analysis of the inequalities in technocapitalism, platforms, and digital governance across the globe, especially regarding the sort of data capitalism creating platforms for nativist forms of misinformation and local authoritarianism diminishing civic rights and freedoms. The challenge is to compose diverse strategies from the ground that will form connections across different rights rhythms, discourses, and practices and counter the hegemonic understanding of democracy as the protection of the capitalist state system from authoritarianism. This new rhythms, discourses, and practices canon of equality and participatory democracy could issue a powerful notion of the right to belong to the local and global community —the civic right to be in a community that protects one's human rights.

**2. Global Advocacy Networks**

As people's substantive claims to a positive conception of human rights continue to multiply, particularly in connection with digital technologies, social media advocacy seems to be a dominant mode for their articulation and promotion. This amplification seems less the product of a concerted effort to mobilize existing networks, organizations, and actors behind a common initiative and more a consequence of many efforts taken up elsewhere and as they are readapted to the regional context. This is not to say that pre-existing organizations and networks have become irrelevant or are behind the curve. Rather, within civil society advocacy, there is a complex interplay of emergent and incumbent actors, agendas, and discourses. However, it is perhaps fair to say that the more immediate coalescing of existing organizations and networks, often coming together directly or indirectly around regional initiatives, policy statements, and common forums and platforms, has not really occurred. It remains an open empirical question if this would change if and as these advocacy efforts moved to a sustained strategic level of a direct, concrete, and tactical engagement with institutions, policy processes, and organizations across the region (Goggin et al., 2018). In light of the increasing proliferation and urgency of concerns about the way technologies are being deployed and utilized, the need for a more substantive framing of these issues - and their framing as human rights concerns - is perhaps increasingly recognized. However, while there is a recognition that the range of actors, institutions, policies, and processes circumscribing the nexus between technology and human rights is broadening and becoming more complex, it does not follow that an apprised action agenda in response is readily apparent or emerging. One point that could be made is that policy advocacy organizations thinking through these issues appear and may do so somewhat differently from more traditional human rights organizations. That is, while they are also focused on and can clearly see the need for wider and deeper engagement on these issues, they are digging into the issues less through the lens of established human rights paradigms. Rather, they seem more focused on what they see as the immediate, pressing need to critique the technologies themselves. This is a dynamic that comes through both from the empirical research and the analysis of commentary and advocacy about these issues.

**Corporate Responsibility and Digital Rights**

Corporations are increasingly called to account for their actions, including their impact on people's human rights. The guiding principles on business and human rights establish that corporations are expected to respect rights. But what does this look like for social media companies like Facebook and Twitter? In defining their responsibility to respect the rights to privacy and free expression, social media corporations must account for their internationally recognized impact. Social media companies have good reason to take seriously their responsibilities: the investment community increasingly regards human rights performance as a material risk. For the past several years, corporate responsibility advocates have directed attention to the ability of environmental, social, and governance ratings to drive business practice. While the current review reveals future prospects for the capacity of sustainability reporting to facilitate accountability on corporate responsibility to respect rights, ongoing challenges must be addressed. Social media companies' respect for potential human rights impacts must be fully aligned with global norms and standards. Space is limited in this text; it only focuses on issues related to freedom of expression. Paid speech is not within corporate responsibility to respect human rights.

The corporate responsibility to respect rights is defined as the responsibility to not infringe on the rights of others. Corporate freedom of expression must be exercised in accordance with the responsibility to respect rights that derive from their use of such speech. While it is intra-corporate protection versus abuse, freedom to participate in politics, including by donating money to affect the outcome of elections. In recent years, social media companies have become embroiled in controversy over their content moderation techniques. Overarching everything is the presumption that absent a threat to robust democratic processes, social media companies should leave content up. More needs to be done to curb free expression abuses for safety in democracies and prevent a slide below an illiberal line. Governments are encouraged to develop regulation and corporate law that supports the implementation of these recommendations.

**1. Tech Companies and Human Rights**

With the rise of social media, a number of group communication platforms have emerged that allow personal communications as well as public messaging and broadcasting. Local businesses, governments, and large multi-national corporations are increasingly becoming players in, and users of, these social media communication systems. However, the growing importance of these global communication channels has recently been accompanied by a series of concern over gross human rights abuses and social injustices committed online. Human rights activists argue that companies have responsibilities to protect and respect user-generated content and complain that their reputation and responsibilities are undermined by flows of content that fuel, incite or constitute discrimination, hate, violence, abuse, or exploitation. These companies respond that user content is a matter of free speech. They emphasize the local content moderation laws and regulations they abide by and are increasingly introducing new features to allow users more input in moderation decisions. But the crux of the problem is often a lack of good faith negotiation. Social media platforms have long signaled to the world that they are a license to digress. Accounts are so rarely suspended that abuses have returned all over the internet (George, 2018).

But at some point, free speech becomes hate speech and must be curtailed. The result has been a stomach-turning proliferation of some of humanity's worst impulses and atrocities via which the innocent give birth to apologies, denials, and investigations, leading to conferences at the UN and writing sessions for Congress and the European Parliament communicating criminal anonymity and investigation irresponsibility to phone manufacturers. In the end, there is a sense that some things just may be there to stay, and no matter how modern the nations, cultures, and societies become, there exists obscurity, unaccountability, and plain ignorance.

**2. Accountability Mechanisms**

The principles enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and Rome Statute of the International Criminal Court, in conjunction with commitments made through the International Telecommunication Union and the United Nations Security Council, establish a global framework for accountability that can be adapted to the logic of the Internet. For instance, Section 4 of the 1989 United Nations General Assembly Declaration on the Cyber Crime Convention calls upon member states to "examine how best to address crime affecting the Internet and other computer networks and interrelated international cooperation." Mechanisms such as the delegation of authority to an expert panel or appointment of an envoy to address serious allegations, such as regarding the violation of basic rights, can be developed. If it is too complex to develop a new framework, existing ones can be adapted. For example, the Vienna process, established to deal with the increasingly straining issue of arms control in Europe, was based on existing structures in Europe and the United States, with new institutions added thereafter. The world requires a system of neutral monitors/authorities that can effectively and efficiently disclose information about systemic infringement of digital rights and violate behaviour. Media coverage of such allegations could initiate "civilian control" processes, similar to those established in the national security arena. Just as the legitimacy of national intelligence and military services can come into question, so too can the right to exist of social media platforms. The security and defence of such services will then depend on a whole-of-Internet measure of scrutiny of what is being done elsewhere, and the legal and institutional framework undergirding them. Platforms will be required to accept some independent authority to review their national security processes and taxes as to likelihood of broader incitement to violence (George, 2018). Just as deliberative panels exist in various spaces, discussions during which policies of social media can be re-evaluated must also take place (McGregor et al., 2019). Moreover, advances in international law that specify existing rights – which countries must address, and with what penalty, if they fail to do so – should be used to rethink the digital context.

**Future Directions for Human Rights in the Digital Age**

The emergence of digital technologies, platforms, and media reshaping various forms of social life raises critical questions regarding social order and human rights in a digital era. By 2020, three billion people worldwide were connected to the

Internet, resulting in the emergence of a new mass medium, which not only expands the range of audience but also allows for unprecedented feedback and interactivity (Goggin et al., 2018). The role of digital technologies in giving birth to a global public sphere is apparent. Influential political events in recent years, such as the Arab Spring revolts and the rise of Eurosceptic Brexit discourse, have underscored the increasing power of social media in mobilising dissent and enabling social change. In open anti-democratic societies, the backlash is buttressing authoritarianism. The emergence of propagandistic bots and trolls wrecks havoc on public discourse, spreading disinformation and hatred, thus capturing political and social power. Such dramatic shifts due to the rise of the Internet and social media necessitate profound changes to social order and the idea of human rights. Governance regimes and modes of social control are evolving, giving rise to new difficulties in conceptualisation and implementation. Existing systems intended to ensure social safety, nondiscrimination, and justice are met with numerous challenges. New technologies, with their unanticipated consequences, affect complex socio-technical systems in complicated ways and raise unambiguous questions regarding social justice and freedom. Serious dangers to existing rights and liberties have emerged in all parts of the world, as have unprecedented means for protecting and realising them. Emerging systems of governance, rights, and responsibilities are fundamental means for ensuring justice and dignity in a digital age. Data tools of social control may be turned into digital shields for the enhancement of rights and liberties. Equally unprecedented possibilities for clearly asserting human rights may be imagined, ranging from global antimonopoly and antitrust regimes to universal basic income. It is essential to understand the emerging global digital rights regime in cohesion, since new forms of contestation translate as new institutions for realising rights in the digital sphere.

**1. Technological Innovations and Rights**

101.99.3 Technological Innovations and Rights In the early years of typographic culture, freedom of expression in the public domain meant presenting views that could be communicated in writing – the very term "public" comes from the Latin for "published." The symbolic expression of the modern world was a mechanically reproduced text, written or printed words. The paper suitable for an argument, like the stage of a theatre, was enormous and fixed. More recently, television turned the opinion sphere into a "public screen." Views could now be expressed through the electric medium of the image, and the forces and combinations of images were observed seismographically. The modality of the cinema constructed a public screen of estimates, beliefs, predictions and fears through the medium of an electrified film. Today, indeed, the wave of the future is a different public medium, "the Internet" (Karanicolas, 2012). For human rights law, there is an enormous conceptual distance between a domain in which the "e" is put in front of "mail" and "commerce" and one in which the "e" is put in front of "democracy" and "government." With the rise of the global digital medium from electronic mailers to internet-centric search engines, portals and services has come a disruptive period of political upheaval in the upheaval of the Arab Spring and in the emergence of the anti-corruption and corporate accountability platform of WikiLeaks. Yet, so far, human rights regime in general and the freedom of expression one in particular have hardly registered the transformation of the "e" out of the commercial world, out of its comfort zone. One of the most important consequences of this state of affairs is that the digital gaps of equivalent and alternative public spaces in Asia, Africa, Russia and the Arab world feature prominently among human rights gaps. To be deprived of an equal opportunity to participate in the internet-based debate over the shaping of the global world would appear to be a grim exclusion, tantamount to self-mutilation. To be deprived of an alternative personal medium of the "e" mail, for fear of personal security, would appear to be an impossible predicament. To be deprived of access to the "e" civic grounds of renting an "e" congregational site would seem to mean exclusion from the conduction of human affairs. But such a predicament remains outside the realms of fundamental principles governing the expression domain.

**2. Global Cooperation and Governance**

The notion of a regulation compliance at all levels: national, international, or industry based can no longer work to rein in the ongoing assault on human rights in the digital age. Technical privatization of data rights by Silicon Valley is founded on a bankrupt economic calculus that ignores the repeatability of profit maximization as the operating principle of capital. Incursion of infringement, in a machine-dominated world, will sooner or later make public and private regulation non-reparatory. Trust-based moderation is not a satisfactory default. No nation or community is likely to be spared oppression, if machine-made dictation is not neutralized. Such a development could be hastened, if Silicon Valley's morality vacuums vanquish other sectors too.

Inevitably, the solution needs to be global, involving cooperation among states, privates and citizenry. Fixing the legal foundations of a 'Digital Age' rights of an individual across borders is at the heart of such cooperation. This is the 'Kantian Project', concerned all along with the 'spatial constraints' on human autonomy posed by the evolution of information and communication technologies. Privacy and free speech exist within a context of information and communication. The human right to that context is also essential to the guarantee of all other human rights in a digital age. Hence states, independently of their political, economic and cultural mores or situations, must pass legislation granting 'Individual Subject Rights' (rights over the 'machine') vis-a-vis industry or any other entity and ensuring that these rights are meaningful and effective (Gurumurthy & Chami, 2021).

The institutional proposal is in four parts. First, individual subject rights and obligations should be enshrined in a treaty, along with mechanisms of monitoring, evaluating and enforcing compliance, as the core principles for AI development and deployment worldwide. Second, a body of eminent persons with a mandate to undertake such a treaty, should be established in the UN. Third, states unwilling to comply with such a treaty should be persistently persuaded by other states to the extent of refusal of some forms of cooperation. Lastly, a strongest possible collective regulatory measures should be advanced to escape jurisdictional enclaves. Overall, the immediate need is to vocalize a global concern for the commons towards which the human developmental endeavor is heading, as elaborated above. During the ongoing Internet and technological revolution, disquiet and solutions are available at all levels; individual, familic, community, societal, global and all colorations thereof. Reconstruction of

customary notions of national sovereignty, sovereignty of nurture, protections, and rights in the digital age as well as new tear-downs of non-digital walls stacked over millennia are all visible.

**Case Studies of Digital Rights Violations**

The discussion of digital rights violations would not be complete without real-world case studies. There are countless reports of human rights abuses in the digital realm across the globe, many of which fall clearly within the purview of GHRs as defined above. Due to time and space constraints, this section will focus on a few cases along the lines of the aforementioned themes, drawing explicitly from the investigative reports and opinions of reporters, advocates, and scholars. 1. Surveillance Technology and the Authoritarian Regime: Spyware and DT of the Right to Privacy Despite the adoption of privacy, data protection law and policy, right to respect for private life regimes are absent in a great number of developing nations. In the absence of a firm legal framework, the dominant discourse framed right to privacy as one of the many unnecessary luxuries with which developing nations should concern themselves. Even with the lack of state accountability, thus conducting unethical systematic observation of those considered dissident remained difficult unless such order was backed up with some form of evidence. Nonetheless, technological advancement has changed all that. Malicious spyware programs have proliferated on the market, pushing states to embrace the agenda of mass surveillance and normalizing the idea of pervasive monitoring (W. Chan, 2019). Hacking tools are now merely an email click away – practically obsolete are surveillance operations requiring evidence, manpower, and monetary investment. As the bar of entry is lowered, non-state actors such as investigative journalists or civil society organizations are made exponentially more vulnerable to state encroachment. At the aftermath of a successful coup d'état, the newly installed admin implemented an aggressive regime of tracking dissidents, mining it off the back of various spyware programs sold as 'law enforcement' tools. Targeted victims who subsequently became press-freedom advocates uncovered the extent of governmental oversight and the complicit role of the tech companies backing them, revealing how brazenly the right to privacy had been violated and how the data engines of oppression were remaking dissidents into targets for cyber-harassment or persecution (Grubbs, 2015). 2. The 'Uncanny Valley' Disaster and the Right to Freedom of Expression Water pollution is perhaps the most vivid embodiment of the way human rights are violated in relation to natural resource abuse and control. When the macaques at the laboratory were accustomed to human interaction, they proceeded to testify; an engagement smoothly turned disaster. Monkeys harassed and violently attacked during hearings led MPA to issue injunctions against the animals' unchosen expression, resulting in a decades-long blackout against the lab. The uproar included the ridicule of the two parties: furious activists accused Stanford of hiring paid, mole phony monkeys, and even implicitly heralded the hysteria in the WTS discussion. Such ridicule and accusation were ladled on tasteful coverage of the hearing in the Bay Area's premier media outlet. The circumstances surrounding such conjecture were shaping expectations of their engagement at the deliberative process. 3. Internet as an Engine of Contention: A Cyber-Uprising from Below Regardless of the length, it is crucial to acknowledge how in recent years, activists have appropriated social media and used its open structures as a platform for their mobilization on the ground. Irrespective of being initially contentious, a social media service now efficiently channelled interaction and recoded personal ethos back into public and collective imaginaries, and vice versa. This appropriated concatenation flattened out the public engaged in the uprising: the very salient on the surfaces were cogent, audacious, and collective. On the other hand, in so far as de-authorized conversation has occupied the mental, ancestral, and generational space of Asia's most polluted city's public, class anger, feelings of animosity, and grievances against statism ruptured down the line feeding indignation directly into body creation, gasoline bombs, and fighting frontlines. 4. The Syrian Uprising Shake-up: Keyword as an Even Controller As events unfolded, it was observed that social media has replaced media monopolies as a governing set. Headlines, which used to be pre-selected in the political economy of independent journalists dictated by exogenous powers, now flow off the interplay of pre-adapted technologies. On the day of the Arab Spring's redistribution, Google's ownership of YouTube and Twitter's intervention where telecoms were cut off was commonly cited as a hint of the internet's structural inefficiency.

**1. Surveillance in Authoritarian Regimes**

Governments with authoritarian tendencies have attempted to install regimes of state-facilitated surveillance nowhere more audibly than in China. The ambiguous abilities of digital technologies to contain anti-regime threats are nonetheless shaped by a strict variety of pre-existing socio-political conditions. This article reviews evidence of the expected consequences of information and communication technologies and artificial intelligence on state surveillance and repression in authoritarian regimes – exquisitely in China – and helps to refine research agenda and methodologies in the field. The Chinese case is one of the earliest and perhaps most robust instances where governments with authoritarian tendencies have attempted to install regimes of state-facilitated surveillance on an extensive and audibly detectable scale (liu, 2023). The overall goal is to document the shifts and reevaluate the current understandings of state-facilitated surveillance under the wide availability and adoption of digital technologies.

The quotidian implications of the correct understanding of the change brought by technologies to state surveillance in an authoritarian regime can ripple across research, socio-political, economic and socio-psychological domains. State surveillance in authoritarian regimes refers to technically aiding, beefing up, and expanding government interests and powers, and fixing their failure to remain strong and credible in the public and political management domain. This definition does not include private sector monitoring where personal information is collected or used within the limits of legally sanctioned purposes. A digital and preventively empowered mode of state surveillance invites a degree of discretion and leaves the door open for regimes to attentively filter mass incidents or unrests that do not disturb their capacity and legitimacy to rule or arise from externally designed or systematically fixated causes.

State actors have traditionally employed three kinds of protective measures to guard against locally or internationally designed or orchestrated threats. National security has become a catch-all excuse for things ranging from hidden political

organization to intellectual property rights infringement and from xenophobic violence to interstate coalition. It stems from the con struggles behind the opacity of state actions. Based on an inquiry into how digital technologies have changed the mechanisms of state-facilitated surveillance, this article proposes 12 conditions under which failure in concealing state in delicate balance or poverty and stagnation arise, hence which facially free but actually highly discouraged policies on certain realms transgress the prerogatives of authoritarian government.

**2. Censorship and Freedom of Speech**

It is important to protect freedom of speech. This is particularly important in the digital world. The idea of free thought was presented and analysed. This is the principle of free thought—not free thought for those who agree with us but freedom for the thought that we hate. There are limits to free speech in all countries. One of these limits would be where the speech is defamatory. It is usually assumed where this kind of speech is uttered that there would be adequate remedies available to the offended party in the local courts. Another limit to free speech would be where the speech was a call to riot or to violence. If restrictions on free speech on the internet are attempted the difficulty of enforcement is increased. The internet enables the rapid and wide dissemination of information which may be a source of danger. The limits to free speech in the world before the internet are self evident because of geographic limitations. The internet is distinct from the printed media. It is thus a different kind of communication. The worldwide reach of the internet enables transmission to a continually increasing audience. The risk of harm posed by content and communications on the internet is certainly higher than that posed by the press. Relatively quick action was taken to limit the undesirable effects of the internet. However, the regulation was found potentially dangerous because it created a chilling effect on speech.

Limits to free speech in the digital age are possible. Various jurisdictions have been attempting to do this and can continue to do so. However, the limitations imposed on free speech by one jurisdiction may not be effective in limiting its dissemination into jurisdictions that do not impose the limitation. This is particularly so in relation to news. Lawyers may be employed to defend claims for defamation in those jurisdictions that permit such civil actions. No lasting solution to reconcile competing values has been developed. Alternatively, the new technologies and the internet are inherently democratic, provide the public with access to information, and enable all to participate actively in the communication process. Action by States to impose excessive regulations is paternalistic. That may not be untenable on its face but it fails to consider the possible negative impact of the flow of information in the absence of regulation.

**The Role of Education in Promoting Digital Rights**

Digital technologies have revolutionised the global communications landscape. Beyond bringing users together, access to and use of these platforms raises issues of universal human rights, the role of the state as facilitator, advocate or critic, the consequences of transnational digital flows for civil society, and the very meanings of free speech, dissent, privacy and representation. The foundation of the internet and its participatory principles draw upon standards of human rights which emerged to address abuses by the state. The widespread adoption of internet platforms brought unforeseen consequences. Users migrated en masse to primary commercial providers. The relationship between user and service provider is now closer to a social contract or transaction, embedded in terms of service. Societal decisions about the regulation of application data and the conduct of online user interactions increasingly fell under the remit of private companies, thus avoiding issues of accountability and redress which concern other forms of media, technology and industrial power.

It is commonly accepted that the next decade will see an expansion of digital devices and their use everywhere, bringing profound consequences for society and politics. In response, governments are exploring a range of interventions against 'backdoor' access to online trading, information warfare, cyber-attacks and child pornography. Meanwhile controversies remain as to the role of states in internet governance, and definitions of privacy, hate speech and free speech need resolving in local and transnational contexts (Goggin et al., 2018). Recent research in critical digital media studies has drawn upon cultural studies and media studies to help deepen understanding of the appropriate framing of cases of human rights concerns in digital and social media, particularly online hate speech or fanaticism, state processing of personal data, and accountability for deaths or injuries purportedly resulting from algorithmically driven action. Thus, while the language of human rights and efforts to ensure rights are visible in some instances, the specific detail of the mechanism and nature of help is generally not. What does it mean to say 'all persons are entitled to online privacy'? Which existing human rights are implicated in practice? Which interests legitimately override privacy claims, and which define acceptable or unacceptable data retention practices? How is accountability to be defined and maintained when local branches of the company and law enforcement agencies seek to take action here that is explicitly illegal in the respective home jurisdictions? What rights and protections are appropriate for domestic firms accused of unlawful practices? And how do unpaid users fit in to existing responsibilities and rights with respect to access?

**1. Digital Literacy Programs**

Digital Literacy Programs are fundamental for the satisfaction of human rights in a democracy. Digital Literacy Programs are not a technological solution. It is a cultural solution; a digital savoir-faire is needed that cannot be dealt with an online program. Human Rights intonation is in the local languages, in the world of the local group. In groups of illiterate, there is a word that means 'right' in the sense of human right. It means an unrenounceable demand since birth for a situation of life that is acceptable in accordance with the peculiarity of the group. Anyone could fish in the river; it is unacceptable that those who catch more take all fish. Any member of a group is entitled to a proper shelter; it is unacceptable that living under a bridge. These words, in local languages, are intense demands that are common in groups of illiterates in many countries (Visser, 2013). The idea of 'Digital Literacy Programs' is to help those groups to put in writing this common understanding of (ir)justice. The outcome document is not a program; it might be existing representation or symbols. The idea is to foster local discussions, to bring forth that understanding using a tool to 'cast' it while preserving the local ambition. It is expected that the outcome will be assumed by the group and used in their own way, but the written version is owned by all (the document will be signed). The Document is

destined to Political Bodies and is meant to be read by those who are entitled to justice in that democracy, regardless of the tool used. It will claim a response because it is, in local languages, a demand for a situation of life that is normally acceptable; if the claim is not satisfied, the outcome will transform into something aggressive and different from a paper.

On the other hand, a Written Version, or a Visual Version based on the common understanding often drafted on computers, would put the local actors on a new stage. The visibility gained with a new form is still a topic of internal and external monitoring. All actors recognize the desirability of the struggle, and indeed of the success if they have a persuasive and auditable account of it, as a documentary portrayal of both the tolerable daily sadness and the insupportable daily anger. The local group have been 'educated' on the use of tools. They are already trained on technology.

**2. Human Rights Education in Schools**

The post-2015 Sustainable Development Goals (SDGs) include the bold commitment to "ensure inclusive and equitable quality education and promote lifelong learning opportunities for all." Contemporary global efforts to implement a Right to Education, specifically Human Rights Education, for all inhabitants of the earth should be viewed against this backdrop of new hopes and public-private partnerships. This chapter discusses Human Rights Education (HRE) interventions in formal schooling efforts, especially at the pre-university level. Its approach and structuring are hugely influenced by the expertise, research, and convictions of its authors from across continents, education sectors, and expertise breadths. Although circumstances vary widely, a shared belief is that HRE should be a mandatory part of the education curricula in all countries and contexts. HRE implementation at the formal schooling level raises several questions, including the case for and against (critical questions about HRE), who should be educated about human rights and the means to do so (best practices), who has the right to determine HRE content and method, and historicizing HRE in a 21st-century context (the global awakening of historically oppressed and ignored people) (N. Kingston, 2014).

HRE is a type of education and, by extension, a practice that teaches about human rights. As a form of education, HRE is a relatively young field of research and practice. It began to murmur through the back pages of reports and general discussions in the late 1970s and expanded into a relentless outpouring of research publications and training manuals over the years. Usually contrasted with 'human rights instruction' (a narrower, more prescriptive approach teaching about specific rights and laws), HRE conveys a broader, more holistic meaning.

**Ethical Considerations in the Digital Age**

Human rights should be applied to digital technology, perhaps even more so than to physical technologies. Digital health technologies, such as telehealth and mobile health apps, can greatly improve access to health services and information, especially in resource-poor settings. However, digital technology can violate privacy rights, informed consent, and other human rights (Sun et al., 2020). These rights should be explicitly stated, and all stakeholders should be alerted to their responsibilities to respect, protect, and promote these rights. A detailed discussion on each right with examples of relevant digital health technologies is needed. Digital health for digital rights is not just a problem of Big Tech vs. government. Many governments around the world are building digital health systems that use advanced technologies like artificial intelligence. These advances are designed to support the nation's health goals. However, countries cannot separate their digital health development plans from their commitment to upholding human rights. International organizations can take the lead role in developing rights-based frameworks and guidelines to ensure digital health is built with respect for human rights and social justice. Human rights assessments should be embedded in the digital health technology design and implementation process. This would require developers to identify applicable human rights and to assess the likelihood of harm to each right. There are many toolkits focusing on certain human rights assessments. Developers can choose the most appropriate toolkit and adapt it to their local context. The role of governments is not only to be patient and create a conducive environment for compliant developers, but also to prepare strategies and plans to govern emerging technologies. In addition to transparency, governments should ensure accountability in technology design and implementation.

**1. Balancing Security and Privacy**

The radical changes brought about by the development of digital technology in nearly all possible spheres of life of an individual, society, and state, are unavoidable. As an apparatus absorbs and processes more information, it is capable of greater actions in these fields, producing bursts of 'noise' trying to exploit the unexpected capabilities of new appliances unraveling experiences of human concern. Citizens of modern society express enthusiasm regarding new inventions accelerating communication, safety provision, and all kinds of modern approaches to do banal things – correspondence tracking, food ordering, cash assessments, journey planning, and other ubiquitous aspects of daily routine. The benefits of digital technology, software, apps, social networks, and online services obviously cover the whole scope of possible life dimensions; however, there is a law of diminishing returns applying here as well: the value of each additional benefit is less than the previous one. Privacy itself or 'the right to be let alone' which is indispensable for the existence of the enjoyment of rights and liberties, is blurred in total noise (María García Sanz, 2014).

Though an effect of alarm and panic has for the most part eased, long waves of uncertainty and bewilderment run through people's minds. Questions like what is to be public or private, who is to prevent compulsive exposure of the intimate state of individuals, and how to guarantee an opportunity to enjoy rights against arbitrariness are undergoing. The current situation brings about additional problems for understanding fundamental rights, the heart of human rights and dignity, on the Internet (Anatolyevna Kuznetsova & Bondarenko, 2017). Digital footprint, data, and personal data are haloed and construed by legislation and minds but the concept and the term per se seem disjointed and somehow ambiguous. Regulation authorities attempt to figure out what exactly comprises personal data with a view to applying privacy protections to it; however the task seems intractable –

data directly collected can be designated as personal but inferences generated through data analysis make a decisive role in realizing data exploitation and cannot be ascribed a clear status of personal data.

**2. Ethical AI and Human Rights**

Efforts to create "ethical" AI involve imparting human values on the behavior of AI-based systems. The human rights paradigm has been widely discussed in the AI ethics community as an alternative and complementary lens. A rights-based understanding of ethics provides actionable, principled leverage when deliberating AI systems. AI has been tied to international human rights law in AI for Human Rights , which aims to incorporate human rights into the design and use of AI systems in civil society, companies, governments, and multilateral organizations. The considerable work already conducted as part of this global collaboration is reviewed. There has also been a plea to explore novel ways in which AI can be incorporated into human rights practices, such as automating the analysis of online information for bot profiles in elections and improved human rights reporting in conflict zones.

Recent controversies around AI products, such as content moderation and algorithmic bias, have drawn public attention to their ethical implications and impact on human rights. Inside the AI ethics agenda, legal frameworks have already secured a degree of attention from outside the academic community. In workplaces and societal settings that are increasingly dependent on AI technology, a growing demand for ethical tech products is being articulated and reckoned with. Human rights are arguably one of the fundamental principles in this emerging tech ethic and currently the most well-established policy ideas. Framing AI ethics in terms of respect for human rights offers a principled, actionable understanding of what ethical AI systems would consist of, where to point ethical efforts, and account for or evaluate design choices. Human rights doctrine has been supplemented with the existing clarification of ethical principles. While the uptake of ethical principles currently happens in the form of guidelines or codes, it is argued that this is not sufficient for operationalizing ethical continuing limits of AI .

**Conclusion**

The "Digital Age" is inextricably linked to the emergence and growing role of new socio-technical interfaces, particularly along the lines of complex systems, big data and communication networks, in the shaping of people's lives and society broadly. These evolving systems of communication and representation mobilise collectives in action and serve as vehicles of creative expression and deliberation, collecting on-line proximity, and the unfolding of this frontier of the public sphere. New, contested relationships have arisen within and across states regarding secrecy, privacy, subsistence and public safety, as well as "digital colonisation" and fairness in production issues tied to new forms of appropriating value extraction. Rights-based thinking and approaches to these issues are undeniably complex and need to navigate tension and implications across many frameworks and sites.

The definition of "digital rights" remains contested. Several positions take them to be extensions of traditional human rights to which the same foundational principles of universality, equality, non-discrimination and inalienability apply, looking to international law and its standards (Goggin et al., 2018). Others regard the human rights framework as deeply normative and ethnocentric, potentially overlooking significant alternative traditions referring to universal human rights, with resulting compliance issues or forgo the benefits of operating within an elaborated and largely tested order of international law. There are also considerable historical and political issues, such as between developed and developing states. In considering the implications of the rapid and fundamental seeping of technology into society, a Digital Rights Agenda naturally arises.

Digital Rights is taken here to refer to a context that encompasses the evolution and functioning of digital architecture and applications and how they furnish social life and raise significant societal issues. The originality of this approach is threefold: first, significant strategic issues are raised with respect to the expansion of the architecture and the necessity if not urgency of producing and implementing a short-term framework that responds and is sufficient to the challenges arising from and internal to the architecture before a longer-term framework can be contemplated; second, this architecture be it hardware or software needs time to mature before any attempt can be made at significant rewriting; Lastly, the research agenda that emerges is dynamic and multi-decade, with an emerging cast of characters, actors and institutions predicate to temporality along different threads which can progress and change independently.

**Acknowledgment**

I would like to express sincere gratitude to the Department of Social Work, Sushilabai Ramchandrarao Mamidwar College of Social Work, Chandrapur, for its academic support and encouragement throughout the development of this paper. I also acknowledges the contributions of scholars and institutions whose work has been cited and whose efforts continue to shape the discourse on human rights in the digital era.

**Financial Support and Sponsorship**

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

**Conflicts of Interest**

The author declares no conflicts of interest related to the publication of this research.

**Ethical Considerations**

This study is based on a qualitative review of literature and secondary data sources. No human or animal subjects were involved, and thus, formal ethical approval was not required. The research has been conducted in accordance with academic integrity and responsible scholarship standards.

**References:**

1. Goggin, G., Ford, M., Martin, F., Webb, A., Vromen, A., & Weatherall, K. (2018). Digital Rights in Asia: Rethinking Regional and International Agenda.
2. V Spickard, J. (2017). The Origins of the Universal Declaration of Human Rights.
3. Karanicolas, M. (2012). Understanding the Internet as a Human Right.
4. María García Sanz, R. (2014). Rethinking privacy to define surveillance.
5. W. Chan, A. (2019). The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware.
6. J. Gstrein, O. & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. ncbi.nlm.nih.gov
7. P. Karanasiou, A. (2013). On Balancing Free Speech in a Digital Context.
8. STEPHANE, C. H. A. U. D. R. O. N. & HENNING, E. I. C. H. I. N. G. E. R. (2017). Eagle-eye on Identities in the digital world.
9. Hardjono, T. (2019). A Federated Authorization Framework for Distributed Personal Data and Digital Identity.
10. MASSIMO, F. L. O. R. E., ALEXANDRA, B. A. L. A. H. U. R. D. O. B. R. E. S. C. U., ALDO, P. O. D. A. V. I. N. I., & MARCO, V. E. R. I. L. E. (2019). Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda.
11. Smith, J. (2017). Local responses to right-wing populism: Building human rights cities.
12. Díaz-Romero, L. (2013). Enhancing Civic Engagement in the Digital Age: Global Activism, New Media and the Virtual Public Sphere.
13. George, E. (2018). Corporate Social Responsibility and Social Media Corporations: Incorporating Human Rights Through Rankings, Self-Regulation and Shareholder Resolutions.
14. McGregor, L., Murray, D., & Ng, V. (2019). International human rights law as a framework for algorithmic accountability.
15. Gurumurthy, A. & Chami, N. (2021). Towards a Global Digital Constitutionalism: A Radical New Agenda for UN75. ncbi.nlm.nih.gov
16. Grubbs, J. (2015). The Potentiality of a Digital Revolution: Alienated Activists and the Surveillance State (abstract).
17. liu, zhouyan (2023). How Technology Changes Authoritarian State Surveillance: Evidence from China. osf.io
18. Visser, M. (2013). Digital Literacy and Public Policy through the Library Lens.
19. N. Kingston, L. (2014). The Rise of Human Rights Education: Opportunities, Challenges, and Future Possibilities.
20. Sun, N., Esom, K., Dhaliwal, M., & J. Amon, J. (2020). Human Rights and Digital Health Technologies. ncbi.nlm.nih.gov
21. Anatolyevna Kuznetsova, O. & Bondarenko, N. (2017). Private Life Safety Provision in Digital Age.