International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

From Classical Liberties to Digital Frontiers: Tracing the Evolution of Human Rights in the Contemporary Era

Rahul R Shetty[1], Dr Mohammed Tauheed Khan[2]

[1]Student, School of Legal Studies, Reva University
[2]Professor, School of Legal Studies, Reva University

ABSTRACT

Human rights have suffered a radical shift from classical liberal/civil and political freedoms/bill of rights conception to a much more complex multi-layered approach to social, economic and technological issues. Human rights were first postulated to guard against the arbitrary exercise of State power and then later the welfare-oriented rights and collective interests were added to the original formulations. Nowadays, digital technologies have added a new dimension – digital rights, covering topics of privacy, data protection, online expression, access to information etc.

This paper traces the historical development of human rights, looks at issues in the digital age, and considers the effectiveness of the current national legal frameworks to tackle emerging issues. It emphasises the need for positive legal and institutional responses which promote human dignity in a digital world.

Keywords: Human Rights Evolution, Digital Rights, Privacy, Data Protection, Cyber Law, Freedom of Expression, Technology and Law

1. INTRODUCTION

The human rights are the principles which form the basis of ensuring individual dignity, freedom and equality[3]. The human rights models of origin, that is, those of natural law and liberal philosophy, generally focused on limiting states and protecting civil rights[4]. The rights language didn't start with any major documents, for example the Magna Carta, nor did it begin with Universal Declaration of Human Rights[5]. No doubt there has been an expansion of what is usually understood by the term 'human rights' over the years to encompass socio-economic rights and collective rights in the context of the varying needs of the society[6].

[3] Universal Declaration of Human Rights pmbl., G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).
[4] JACK DONNELLY, UNIVERSAL HUMAN RIGHTS IN THEORY AND PRACTICE 21–25 (3d ed. 2013).
[5] supra note 1
[6] HENRY J. STEINER, PHILIP ALSTON & RYAN GOODMAN, INTERNATIONAL HUMAN RIGHTS IN CONTEXT 263–69 (3d ed. 2007).

Since the beginning of the 21 st century the world has seen a digital revolution that has transformed the way human beings communicate, rule and utilize the resources. The advent of digital technologies has required a re-evaluation of the classic human rights ideas, as new issues emerge in the virtual worlds[7].
The paper will discuss how human rights have evolved and shifted towards the digital age and why a dynamic and responsive legal framework is necessary.

1.1 Understand the history and development of human rights.

To know about human rights' historical evolution. Classical Era: Civil and Political Rights The very first and most basic thinking in relation to human rights was found during the Enlightenment and developed in what is called the "first generation" of rights[8]. These rights focused on the individual against the excessive powers of the state, and guaranteed such liberties as freedom of speech, freedom of religion, fair trial, and freedom from arbitrary arrest or detention. These rights can be termed negative in nature, as they don't mandate the government to actively do something for its citizens, but instead not to do something to them. This philosophical foundation was established by philosophers such as John Locke, who believed that individuals weave birth "natural rights" to life, liberty and property, rights that stem from being a human and which no government or individual could in good conscience claim to have the right to restrain[9]. The concept of the social contract was later expanded on by Jean-Jacques Rousseau, who proposed that human authority should be justified only in so far as it is carried out in the uncoerced consent of the people there to be governed[10].
The ideas took concrete form in historic states documents, like the English Bill of Rights (1689), American Declaration of Independence (1776), and the French Declaration of the Rights of Man, and of the Citizen (1789)[11]. They either did or did not shape together the mental and legal frame of constitutional democracy and the rule of law in the modern age.

1.2 Second Generation: Socio-Economic Rights

It was the Industrial Revolution of the 18th and 19th century that came with immense economic wealth but reluctantly along came then the terrible social divide, child labour and substandard working conditions and urban poverty[12]. As it became more apparent that there is no political freedom where there isn't any food, health care or housing. This recognition led to the emergence of the second-generation human rights, the socio-economic and cultural ones. Unlike the rights that they replace, they are positive – they are rights that must be performed by the state and that must be protected. These include the right to education, right to work and fair wage, right to health care, social security, adequate standard of living etc.
The rights are a view of the state as, not just a neutral referee, but a positive guarantor of humanity welfare[13]. The vision was made official on the international stage with the International Covenant on Economic, Social and Cultural Rights (ICESCR, 1966)[14], one of the fundamental United Nations' human rights conventions to which States have committed to bring into fuller existence the rights it guarantees to its people. The original vision is social democratic and welfare state in its emphasis that there is human dignity in freedom from oppression and access to the minimal necessities of life.

[7] Publications of the United Nations on Digital Rights and Human Rights in the Digital Age.
[8] MICHELINE R. ISHAY, THE HISTORY OF HUMAN RIGHTS 95–102 (2d ed. 2008).
[9] JOHN LOCKE, TWO TREATISES OF GOVERNMENT 287–89 (Peter Laslett ed., Cambridge Univ. Press 1988) (1690).
[10] JEAN-JACQUES ROUSSEAU, THE SOCIAL CONTRACT bk. I, ch. VI (1762).
[11] French Declaration of the Rights of Man and of the Citizen (1789); English Bill of Rights (1689).
[12] ERIC HOBSBAWM, THE AGE OF REVOLUTION: EUROPE 1789–1848, at 189–210 (1962).
[13] International Covenant on Economic, Social and Cultural Rights arts. 6–13, Dec. 16, 1966, 993 U.N.T.S. 3.
[14] Id.

1.3 Third Generation: Collective and Solidarity Rights

New global problems arose during the 20th century which required a joint and comprehensive approach to human rights beyond the scope of individual or national rights-based bodies[15]. When the environment was called into crisis, the imperiousness of colonial exploitation, the growing divide between the Global North and South, and the close proximity of nuclear war, it was time to reflect on the collective and international level of rights. This led to the third generation of human rights that are also known as solidarity rights. These rights are not for individuals, but peoples, communities and human kind as a whole[16].

These cover the rights to a clean and healthy environment, to development, to peace and to participation in the benefits of the global commons. Most importantly, these rights can only be achieved through multilateral cooperation, international cooperation institutions and shared responsibility on the border. An important example is the UN Declaration on the Right to Development, 1986, where it is affirmed that all people and all societies have the right to participate and develop in both the economic, social and cultural fields, as well as in the political, and that they are entitled to all benefits that economic, social and cultural development brings[17].

The Third Generation Rights embody a recognition that in the 21st century, the living conditions of one community are intertwined with the living conditions of other parts of the world; and that justice in relation to a community is not limited to internal society, but extends to justice between societies.

2. DIGITAL RIGHTS: CONCEPT AND NATURE

This new era in human rights has been made profoundly visible by digital technologies that are now increasingly ubiquitous in our everyday lives from enrichment of communication and information, to professional, electoral, and means of healthcare[18]. Digital rights should not be viewed as some sort of new breed of rights invented in a vacuum, but merely the extension and reinterpretation of the existing models of human rights in the digital context — dignity, liberty, privacy and equality. The internet, artificial intelligence, big data and algorithmic systems have given rise to new machines to both empower and to exploit humans[19].

A government is now able to keep track of its citizens at a level that was never thought of before. Corporations are able to create close geographies of billions of individuals without meaningful consent. Life changing decisions – such as a job and a loan or bail – can be made by automated systems with little transparency and accountability. Digital rights are meant to solve exactly these problems, by safeguarding the rights people enjoy in the real world and not removing them when they cross the line onto the Internet. Digital rights also represent a wider understanding that many other rights depend on access to the digital world – it is no longer considered a luxury but critical for the enjoyment of many other rights[20].

[15] Karel Vasak, *A 30-Year Struggle: The Sustained Efforts to Give Force of Law to the Universal Declaration of Human Rights*, UNESCO COURIER, Nov. 1977.
[16] JACK DONNELLY, *UNIVERSAL HUMAN RIGHTS IN THEORY AND PRACTICE* 68–74 (3d ed. 2013).
[17] Declaration on the Right to Development, G.A. Res. 41/128 (Dec. 4, 1986).
[18] Publications of the United Nations on Human Rights and Digital Technologies.
[19] SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* 8–15 (2019).
[20] JAN KLEIJSSEN & STÉPHANE LEFÈVRE, *HUMAN RIGHTS IN THE DIGITAL AGE* 17–21 (Council of Europe 2019).

When access to public services, education, community involvement and materials of economic activity have increasingly become digital, being shut out of the digital space is equivalent to being shut out of society.

2.1 Right to Privacy and Data Protection Perhaps the most contended and consequential of all digital rights is privacy.

In the digital era, personal information is of an unparalleled value, to the point that many view it as "the new oil", and its collection, storage and manipulation unleash deep questions of autonomy and State control[21]. Digital privacy can be broken down into three sub-areas: communications privacy, informational autonomy and data protection. The concerns have inspired strong legislation and regulation internationally, including the European Union's General Data Protection Regulation (GDPR, 2018), which has granted the individuals more rights to their personal data from which they can be accessed, rectified, and erased[22].

2.2 The use of the Internet and the new technologies of communication require the right to freedom of expression.

The Internet has become an empowering tool for free expression; for dissidents, journalists, activists, and for everyday citizens, to speak, organize and obtain information that would not have been possible before[23]. But that liberty is now being threatened. Internet shutdowns, content blocking and the criminalization of online speech are growing commonplace among governments. All content is not equal and all platforms have extensive and often hidden editorial discretion through content moderation and algorithmic amplification processes on social media. It will therefore be necessary to navigate some rough waters when discussions about freedom of expression in the online arena answer questions from the difficult tensions: protection of the individuals from harassment versus protection of free exchange of views; prevention of dangerous misinformation versus ban on misinformation; platform liability versus chilling effect of too much regulation. International human rights bodies have consistently seen it as a principle of human rights that the same rights that apply offline must apply online, the examples being, most notably, the UN Special Rapporteur on Freedom of Expression[24].

2.3 Right to Access Information and Internet Connectivity

Whilst the internet remains indispensable to achieving other rights, access to the internet has been recognised as a right in its own right[25]. In 2016, UN passed a resolution urging that people have the right to exercise their rights online, similar to exercising their rights offline, and that disrupting the Internet for a purpose a person has a right to is a human rights violation. However, a clear 'digital divide' still remains. Billions of people worldwide, especially in the Global South, are rural, and marginalised, without reliable internet access. The opportunities presented by the digital age are not equally shared within countries, as seen by differences among people of varying incomes, genders, ages, and geographic locations. The availability of connectivity is thus emerging as a social justice/policy question and a social equality issue[26].

2.4 The right to be free from electronic monitoring. Freedom from electronic surveillance.

The most serious challenge to digital rights is mass surveillance by either state or non-state actors. Recent

[21] DANIEL J. SOLOVE, *UNDERSTANDING PRIVACY* 1–12 (2008).
[22] General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.
[23] Publications of the United Nations on Freedom of Expression and Digital Media.
[24] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/17/27 (May 16, 2011).
[25] Publications of the United Nations on Internet Access and the Digital Divide.
[26] U.N. Hum. Rts. Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, Res. 32/13 (July 1, 2016).

incidents like leaking by Edward Snowden in 2013 revealed the scope of government surveillance and the existence of commercial spyware as tools such as Pegasus indicated, these have not been confined to large and democratic governments[27]. The surveillance gear at the disposal of the authorities has been extended by the other new technologies developed such as facial recognition, predictive policing algorithms and location tracking.

The right to protection from digital surveillance needs to not only be legally prohibited from false surveillance, but also to contain effective procedures of being supervised, be transparent about surveillance, and be sufficiently limited in the retention of data[28]. One of the hallmarks of human rights frameworks on state surveillance is the concept of proportionality, which holds that any kind of surveillance is "necessary," "targeted" and "proportionate" to a justifiable aim.

3. LANDMARK DEVELOPMENT IN INDIA: JUSTICE K.S. PUTTA SWAMY (RETD.) V. UNION OF INDIA (2017)

The landmark decision in Putta swamy marks a pivotal moment in this constitutional development that has placed digital privacy at the heart of the nation's privacy law[29]. The Putta swamy case was a historic ruling by the Supreme Court of India that recognized the importance of digital privacy rights in Indian privacy law. The case had emerged as an opposition to the Aadhaar biometric identification scheme and had far reaching consequences.

The Court explicitly declared the right to privacy as a fundamental right under the Indian Constitution which is covered by Article 14, 19 and 21. Significant is the fact that the Judgment did not restrict privacy to the physical world. In the concurring opinion quoted, Justice D Y Chandrachud considered the digitalization aspect and noted that the right to control information of everyone about themselves is one of the principles of privacy. This brought this right to the forefront of issues involving data protection, digital surveillance and informational strategies of the state and private sector.

There are several reasons why the ruling was a watershed moment: First, it offered constitutional support for the Indian data protection framework, as it would come to be known. Firstly, it gave India a constitutional basis for the then-to-be-developed data protection framework. Second, it acknowledged that the way citizens interact with the State is permanently changed in an era of so much data—the State can gather and analyse so much information on them compared with what they can do to safeguard it. Third, it has decided that dignity and autonomy – the principles from which constitutional rights are born – can understandably be protected only when they become part of digital life.

The judgment set the stage for the Digital Personal Data Protection Act, 2023, the most noteworthy legislation in India towards a holistic Digital Rights framework that gives rights to data principals, imposes duties on data fiduciaries and provides for enforcement by way of a Data Protection Board[30].

[27] Glenn Greenwald, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 9, 2013).
[28] supra note 2.
[29] Justice K.S. Putta swamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[30] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

4. LEGAL AND INSTITUTIONAL FRAMEWORK

4.1 International Framework - Human Rights Declaration adopted in the United Nations, 1948 (Universal Declaration of Human Rights, UDHR)

The Universal Declaration of Human Rights is the basic document in the modern international human rights system. It had been adopted by the adopted General Assembly of the United Nations after the conclusion of World War II and for the first time, it embraced a universal listing of human rights for all people, without regard to nationality, race, religion or status. Since then, however, Article 12 (Protection of Privacy) and Article 19 (Freedom of opinion/expression) have been expanded to include the digital sphere and they are the foundation for digital rights arguments worldwide[31].

The Universal Declaration of Human Rights, although not a treaty per se, has tremendous moral and political power and has actually been tracked in of many countries' domestic laws, and on the drafting of many treaties.

4.2 ICCPR and ICESCR (1966)

The two International Covenants fed into the hopes and dreams of the UDHR and were laws that were binding on signatory states. Rights most important for the digital sphere are covered by the International Covenant on Civil and Political Rights (ICCPR), for which states are obliged to make sure they are not compromised by public authorities or private individuals[32]. This is complemented by the International Covenant on Economic, Social and Cultural Rights (ICESCR) which focuses on the right to education and access to cultural and scientific life; being increasingly reliant on digital access.

These two covenants are a necessary complement to the UDHR and the treaty bodies related to both of them have regularly provided interpretive guidance on how the covenants relate to digital contexts.

4.3 UN Guidelines and Resolutions on Digital Rights

The United Nations has evolved its digital rights activities over time. The UN has increased its activities and involvement on digital rights over time. In 2016, the UN Human Rights Council decided in favour of the resolution, which reiterated that offline enjoyment of rights will carry over to the online world and criticized “deliberate Internet shutdowns” as a violation of international human rights law. The UN Special Rapporteur in freedom of expression has delivered a series of authoritative statements on encryption, online surveillance and platform regulation. Further, the United Nations Guiding Principles on Business and Human Rights (2011) laid the groundwork for companies, including tech firms, to take human rights obligations into their own hands: businesses should respect human rights in their actions, activities and practices[33].

5. INDIAN LEGAL FRAMEWORK

5.1 The 14th, 19th and 21st Articles of the Constitution

India's Constitution serves as the foundational legal instrument for digital rights with a few important articles. As algorithmic systems and government by data have emerged to mediate various forms of discriminatory treatment, Article 14's obligation to equality before the law is becoming increasingly relevant. Article 19 guarantees freedom of expression and speech; the court has expanded the definition to encompass online speech, blogging and social media. The Supreme Court in the case of Putta swamy,

[31] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).
[32] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171; International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, 993 U.N.T.S. 3.
[33] supra note 9.

has given the broadest interpretation to Article 21, which includes the right to life and personal liberty, which also encompasses right to privacy, dignity and informational autonomy[34].

These constitutional rights are not only safeguards against the state but are also a measure that can be used to assess the validity of laws passed by the state, including regulations on technologies.

5.2 Information Technology Act, 2000

This was a turning point and the first important legislation in India to begin to regulate the digital space was the Information Technology Act. It introduced legislation that made digital records and digital signatures legally acceptable, introduced new offences for hacking, data theft and cybercrime, and gave the government new powers under Section 69 in relation to interception, monitoring and decryption of digital communications for the sake of national security, which has been criticized by civil liberties campaigners.

Then, in Shreya Singhal v Union of India 2015, the Supreme Court struck down an anti-Internet policy, Section 66A, that criminalized online speech that it found "grossly offensive" due to its unconstitutional restriction on free expression, marking the first time that the judiciary would examine the constitutionality of online legislation under the grounds of freedoms of speech and expression. The IT Act has since been amended by the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 laying down specific obligations of social media intermediaries and there has been an on-going challenge to such rules[35].

The recognition of digital rights in the judiciary. Recognition of digital rights by the judiciary.

It is noteworthy that Indian courts have been able to infuse meaning into digital rights absent any comprehensive legislation. In addition to Puttaswamy, courts have discussed matters such as the right to internet access, which is considered part of fundamental rights, and indefinite shutdowns — which the Supreme Court in Anuradha Bhasin v. Union of India (2020) said were unconstitutional — to addressing the right of individuals to be protected from content that defames or harms them online[36].

The cumulative effects of this case law have given shape to the current situation in India regarding digital rights, although the laws lag in parallel with technological developments. The recently passed DP3A, 2023, is the latest and more prominent stride in the process of creating a formal regulatory body, but the details on future implementation and enforcement remain to be worked out.

6. Contemporary Challenges in the Digital Age

6.1 Data Privacy and Surveillance. Data Privacy and Surveillance, ECTS.

Ensuring that personal data is collected, processed and monetized to an unprecedented scale is one of the most significant challenges of the digital age. Governments have implemented surveillance infrastructure, including CCTV networks with face scanning capability, as well as monitoring systems for communications and conversations online, but with little transparency and without due process. Behaviours are continuously measured by large companies, especially tech companies, and this tracking of consumers' online behaviour, purchasing patterns, geography and social networks (including FB connections) culminates in the creation of deep behavioural profiles of each consumer, often without their informed consent[37].

[34] INDIA CONST. arts. 14, 19 & 21.
[35] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[36] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[37] supra note 2, at 221–35.

This data environment poses great threats. Personal data can be exploited for the specific purpose of control, why discrimination or manipulation. The Cambridge Analytica case is just one example of how personal information collected from social media sites can be used to manipulate elections on a large scale. Surveillance has been employed to monitor and quell dissent in authoritarian settings. Despite being a democracy, the laws in place around data collection have faced considerable difficulties matching the abilities of the individuals collecting it, putting individuals in a limited place to exercise meaningful control of their information.

6.2 Algorithmic Bias and Discrimination

AI and machine learning algorithms are becoming commonplace in making or informing big decisions such as whose resume is selected during the hiring process, who gets a loan, those that are flagged as suspicious for criminal activity, and who gets to see content online. These systems are trained using historical data, and if that data shows inequities and prejudices in the past, then the algorithm will learn these and remember them at scale.

One such case study is predictive policing in policing, which has been demonstrated to disproportionately identify racial minority people. The situation is analogous for automated hiring technologies, which have been shown to disproportionately harm women and some groups. Many AI systems are opaque and their decision-making is often complex and hard to audit or explain, making it difficult for those impacted to challenge the outcomes and seeks redress. Beyond the technical aspects of algorithmic bias, regulatory policies and standards must emphasize transparency, accountability, and impact assessments prior to when algorithms are put into place in sensitive areas[38].

6.3 Access to information vs. control of information.

The internet has given voice to billions of people that have never had the platform to speak through before. But this has also led to a rapid spread of misinformation, hate speech, incitement to violence and organised misinformation campaigns. As challenging as it is for lawmakers, it is also a challenge for platforms to strike a principled balance between prohibiting content that needs to be prohibited and prohibiting content that is actually harmful – without overstepping the mark into censorship[39].

The problem with over-regulation lies in the fact that it can truly stunt healthy critic voices, marginalize perspectives, and provide governments and corporations with undue editorial control over public debate. On the flipside, under-regulation enables toxic content to proliferate and can lead to real-life consequences, such as when instances of social media activity cause communal violence, as did happen in one instance. Platforms have replied by implementing content moderation policies, but there is no uniformity of application, and insufficient due process for users if their content is taken down. One of the most contentious issues in digital governance today is how to achieve a more “balanced and rights respecting” regulation of platforms.

6.4 Cybersecurity Threats

As more and more aspects of modern living are becoming online, the surface area for attack has greatly increased for malicious individuals. From ransomware attacks that paralyze hospitals and public facilities, to state-sponsored infiltrations into critical systems like power grids, financial systems and electoral infrastructure[40]. Phishing, identity theft and breaches involving the disclosure of personal information on a massive scale all threaten to break the privacy and security of individuals.

[38] CATHY O’NEIL, *WEAPONS OF MATH DESTRUCTION* 3–15 (2016).
[39] Publications on online speech regulation and platform governance
[40] Publications on cybersecurity and digital governance.

The results might be disastrous: economic damage, operational disruptions and even a loss of life and national security. Hence, today Cyber security is not just a technical issue, but a governance one that affects human rights. Ransomware attacks on healthcare systems are devastating, and so are exposures of personal medical records in a breach.People get hurt when healthcare systems get disabled by ransomware and when personal medical records are exposed in a breach. What is important is that effective responses need to be based on a collaboration of governments, the private sector, and international organizations, since a cyber threat does not respect countries' borders and often originates outside of countries' reach.

6.5 Digital Divide

Although the Internet has gained tremendous traction and popularity globally, digital technologies have been unevenly distributed. Digital divide exists at different levels, including at the country level, between urban and rural residents in countries, and between people with different income, gender, age, and disability. For a large population in large parts of Sub-Saharan Africa, South Asia and Latin America, there are no telecom services at all, or services that are slow, expensive or unreliable[41].

This inequality has huge implications on human rights. If the state powers provide more services to people online, learnings more effectively, offer more economic opportunities, and participate in government more easily, people who cannot use digital media are effectively cut off from full participation in today's society. COVID-19 vividly highlighted this disparity, with the conversion of schooling to online and healthcare delivery to digital having become a primary issue, with in-person experiences relegated to the sidelines. Fighting the "digital divide" is not only a development target — it is a pre-condition for achieving true universal digital rights instead of the digital privileges of the connected few.

7. COMPARATIVE PERSPECTIVE

The States take different visions towards digital rights. The EU prioritizes robust data protection laws, whereas other nations like India have still been working on having well-defined and structured laws in place. This is a difference that shows the necessity of aligning in the world of digital governance[42].

Interdisciplinary Dimensions

The evolution of human rights in the digital world does not only take place in legal discourse. It intersects with:

- Technology and artificial intelligence
- Sociology and digital behaviour
- Economics and Digital Markets
- Political science and governance

The interdisciplinary approach is vital for understanding digital rights in a comprehensive manner[43].

8. FINDINGS

8.1 The human rights have developed as a result of the changes in the socio-political and technological contexts.

History of human rights is not a closed book, but a never-ending one, moulded by the social, political and technological environment of the time. Civil and political rights are a reaction against the monarchical

[41] Publications of the United Nations on the Digital Divide.
[42] GDPR, supra note 5; Digital Personal Data Protection Act, supra note 13.
[43] Books and journals on technology, governance and digital society.

absolutism and the oppression of the colonial system. The socio-economic rights were a response to the inequalities brought by industrialization. Collective rights emerged in the context of the environmental and developmental crises of the late-twentieth century. Dignity, freedom and justice in practice were represented in each generation of rights.

This trend of evolution still persists even in the present times. The digital revolution is redefining power, in the shape of state control and technological power within the hands of tech giants and presence in vulnerable households, and vulnerability, in the form of individuals. The results of this work confirm that historically human rights have proven able to adapt to these changes, and this adaptive character should remain the fundamental factor in the evolution of human rights in the digital era.

8.2 Digital Technologies have dramatically broadened the scope and complexity of human rights.

The introduction of digital technologies has not just introduced new rights but the conditions for the exercise of all rights have changed. A digital dimension to privacy, expression, equality and access to justice, unimaginable a few decades ago. Rights enjoyed within the confines of territorial and boundaries have been able to be exercised in the digital realm, thus making territorial accountability and enforcement more complicated.

Concurrently, digital technologies have raised completely new rights issues—such as the right to be forgotten, the right to ‘transparency' of the algorithm, the right to ‘portability' of data and the ‘right to non be automated'—with no real equivalent in pre-digital rights vocabulary. That is complicated by the rapid pace of technological disruption, which always outstrips policy and institutional responses. Thus, this study concludes that human rights should be considered to have an evolving and broad definition.

8.3 Legal regimes are inadequate to deal with new digital challenges comprehensively.

While there have been great strides in laws, principles and resolutions around digital rights, such as the GDPR in Europe, the Digital Personal Data Protection Act in India, and many UN resolutions about freedom of the Internet, the law around digital rights is still disjointed and ad hoc and incomplete. The majority of current systems were developed in an earlier technology and have been expanded and adapted – for some, rather to the breaking point – to service digital needs which they were never meant to serve.

Key gaps persist. Most jurisdictions have weak legislation on AI-driven and automated decision making. Governments often over-wield surveillance powers with little oversight, or a lack of proportionality. The rights of individuals struggle to catch up with powerful technology companies and the rights are poorly-defined and inadequately protected. Until recently, there has not been a solid precedent for resolving questions of jurisdiction through cross-border data transfers (CBDR). Together this raises serious concerns that individuals use the digital world with significantly less effective protection than in similar physical settings, needs, and relations — a situation which requires immediate legislative investigation.

8.4 Judicial Activism has been very important to the Figure of Digital Rights.

Cs need to understand that, without a comprehensive law on digital rights, courts are becoming a crucial tool to interpret and enforce digital rights. In several jurisdictions, judges have expanded the scope of constitutional and statutory provisions in order to reach the digital world, where the legislature has been slow or hesitant to do so.

The finding of privacy as a fundamental right in India in Putta swamy with clear implications for online data. India's Supreme Court ruling in Putta swamy, finding privacy a fundamental right with clear implications for online data. In Anuradha Bhasin, the Court upheld that access to the internet is a facet of fundamental freedoms. It struck down a seemingly "over-broad" curtailment of online speech in Shreya Singhal. Over here, courts have been progressive in their interpretation of digital rights, notably in

Germany and Brazil, and other European states. Judicial activism has played an essential role in this, but it has inherent shortcomings: decisions are limited to cases before them, may not be as broadly apperceptive as a law, and decisions are not decisive enough to meet the pace of technology development. There must be legislative action to solidify and expand victories in court.

8.5 Lack of international consensus on regulating digital space

This study has revealed perhaps the most important structural problems to be whether there is a clear international structure for regulation of the digital space. The internet and digital technologies are not governed by a uniform multi-lateral regulatory regime like those of trade, aviation, or nuclear energy, where several strong powers are known for their dominant influence over policy. Aviation, nuclear energy and trade have much more uniform multi-lateral regimes than the internet and digital technologies, and in the latter, the few dominant powers have a disproportionate influence on policy.

The European Union has favoured a rights-based regulatory framework, represented by the GDPR and the Digital Services Act. Chad's history has embraced a more interventionist government approach, whereas the U.S. colonial tradition has been one of limited federal control, favouring a more market-driven approach. Several countries, including China, are promoting the concept of digital sovereignty, which calls for a state's authority over the content and data exchange on the internet. Such divergent views make cross-border data governance, content control, and the application of surveillance technologies particularly problematic, and the establishment of global standards extremely difficult.

Until there are more international cooperation and agreement, digital rights will be realised unevenly, with some jurisdictions offering comprehensive protection for digital rights and others offering scant protection. One of the biggest and least addressed issues of our time is establishing a truly universal approach to digital rights that is reflective of the global nature of the internet.

9. SUGGESTIONS AND RECOMMENDATIONS

9.1 Pass an All-Inclusive Digital Rights Act.

Governments need to advance beyond the anti-tattersall, patch-job method of digital regulation, and adopt enacting a comprehensive law that will explicitly acknowledge and safeguard digital rights. This bill should cover all aspects of data protection, on-line expression, surveillance oversight, algorithmic accountability in one unified bill in order to prevent distinct measures conflicting with each other or being interpreted through successive judicial rulings. Whilst the Digital Personal Data Protection Act, India, is a positive development, a sweeping bill on AI regulation and digital due process is yet to be put together.

9.2 Strengthen International Cooperation

Digital technologies are borderless, and rights abused in the digital space often occur with actors, infrastructure and data in multiple jurisdictions. It is unlikely that the problems can be solved by any one country. States must therefore invest in developing more robust multilateral approaches, such as those within the United Nations and other intergovernmental organisations, to ensure convergence with regard to data protection, the monitoring of cross-border transmissions of data, and to create common practice standards for responsible states' conduct in cyberspace. To be effective, greater cooperation between governments, civil society and the technical community is needed.

9.3 Address the Digital Divide.

For meaningful realization of digital rights, awareness of the digital world is the precondition. Internet connectivity should be recognized as a public good and should be given top priority for making its access more available, reliable and inexpensive, especially in rural and low-income segments and other unserved

areas, particularly in the Global South. Education in digital literacy is a one that doesn't come second to any other, where things aren't just connected, they are made aware to both use and negotiate digital worlds critically.

9.4 Reform Surveillance Laws

Current surveillance laws in most jurisdictions empower governments with wide powers without robust and appropriate constraints. These rules need to be changed to reflect the necessity, proportionality, and judicial authority of surveillance before it can be implemented. Independent surveillance bodies need to be put in place or extended to oversee adherence and there should be genuine transparency, such as making regular public reports of the use of surveillance powers, mandatory. In general mass surveillance and blanket programmes should be forbidden.

9.5 To control Artificial Intelligence and Algorithmic Systems.

The deployment of AI systems needs to be carefully monitored and guided by rights-based principles, given how those systems will continue to shape decisions that impact on people's lives. There is a need for rules and regulations to implement systematic Human Rights impact Assessment for use of AI systems in the sensitive areas like law enforcement, hiring, lending of credit, and provision of public services. There should be the right of explanation for an individual interested in decisions made by automated systems and meaningful ways to contest the decisions made. AI providers and users have a responsibility to correct the outcomes of systems if they have been discriminatory or harmful.

9.6 Encourage digital literacy and raised public awareness

Knowing and exercising legal and institutional rights depends on individuals' understanding. Governments and civil society organizations need to fund a data literacy initiative that provides general population with education on data privacy, internet safety, cyber security, rights in a digital world and more. Building a population that is digitally informed and is able to hold governments and corporations to account is the job of all schools, universities and community groups.

9.7 Enhance Cybersecurity Infrastructure

Finally, governments should put cybersecurity on the agenda as a key aspect of national security and public safety, and work on building strong cybersecurity infrastructure for essential services, public institutions and citizens against cyber threats. These may involve creating dedicated agencies for cyber security in order to improve response to incidents, creating National plans for responding to cyber incidents, and working with the private sector on Public-Private Partnerships to share threat intelligence. International norms and rules for use of cyber means in attacks on civil elements should be established and applied**.**

10. CONCLUSION

As the history of human rights from classical freedoms to digital freedoms demonstrates, the concept can evolve and thrive in changing times. Conventional systems established solid ground frameworks but required creative solutions to address the new challenges of the digital era to provide adequate rights protection. The protection and promotion of digital rights is a necessary precondition in a world that is more and more connected to human dignity. Such an approach of a forward-looking and inclusive character will have to be adopted to promote the development of technology in keeping with fundamental human values.

REFERENCES

1. Magna Carta

2. Universal Declaration of Human Rights
3. Justice K.S. Putta swamy (Retd.) v. Union of India
4. Publications of the United Nations
5. Books on human rights law and digital governance
6. Journals on cyber law, privacy, and technology