YOUTH
TRAINING
MODULE

DIGITAL HUMAN RIGHTS

FUNDAMENTAL FREEDOM IN DIGITAL AGE

Pairvi

Supported by MISEREOR IHR HILFSWERK

YOUTH
TRAINING
MODULE

DIGITAL HUMAN RIGHTS

FUNDAMENTAL FREEDOM IN DIGITAL AGE

Pairvi

Supported by MISEREOR IHR HILFSWERK

Digital Human Rights; Fundamental Freedom in Digital Age

January 2024

Training Module prepared by Dinbandhu Vats *and published by*
Public Advocacy Initiatives for Rights and Values in India (PAIRVI)
K8, Third Floor, Lajpat Nagar III, New Delhi 110024 (India)
Ph. +91 11 29841266, email: pairvidelhi1@gmail.com, info@pairvi.org, Web: www.pairvi.org

CONTENT

UNDERSTANDING THE DIGITAL HUMAN RIGHTS

- Defining the Digital Human Right
- Key Terminologies Used in Digital World

In the era of rapid technological advancement and digital transformation, the way we live, communicate, work, and access information has drastically evolved. The internet, mobile devices, social media, and digital services have become integral parts of our daily lives. There can be no doubt that digital technologies have thrust our world forward towards unprecedented human progress. We are in the midst of a massive digital transformation that has affected every aspect of society. In 2016, UNHRC General Assembly articulated access to the Internet an essential human right. Internet is the undiscovered ocean of information and in present the greatest supplier. Technology is an empowering agent of rights and not privilege all by itself. Supreme Court of India in its ruling has termed the right to internet as fundamental human rights and it must be read with Article 19 and 21 of our Constitution.

Human rights apply online just as they do offline. Digital rights are defined as the realisation of the values in the Constitution of India's preamble in our digital worlds today. Digital rights must not be considered separate from basic human rights. It encompasses a broad range of principles and protections that are fundamental in ensuring that individuals can navigate the digital world with dignity, privacy, and freedom. The digital age has heralded a new era in human history, fundamentally altering the way we interact, learn, conduct business, and participate in society. This transformation has been driven by the proliferation of digital technologies, internet connectivity, and the growth of online platforms. In this context, the concept of digital human rights becomes increasingly relevant as we seek to safeguard essential freedoms in the digital realm.

Digital human rights are an extension of traditional human rights into the digital domain. They recognize that as individuals engage with digital technologies and the internet, they should continue to enjoy the same fundamental rights and protections that are enshrined in international law and human rights frameworks. Digital human rights encompass a variety of principles, including but not limited to privacy, freedom of expression, access to information, and protection from discrimination and surveillance

Key Terminologies used in Digital Human Rights

Digital Divide: The digital divide is the unequal access to digital technology, including smartphones, tablets, laptops, and the internet. The digital divide creates a division and inequality around access to information and resources.

Net Neutrality: Net neutrality is a principle that ensures internet service providers treat all data equally. It prevents discrimination or charging differently based on content, source, or application. Net neutrality is a critical component of digital human rights because it preserves an open and equal internet where all individuals and organizations have the same opportunities to communicate and innovate.

Digital Security: Digital security encompasses the right to have secure digital communications and transactions. As cyberattacks and hacking become more prevalent, it is essential to protect individuals' digital lives from unauthorized access and data breaches. Digital human rights include the right to cybersecurity and protection against online threats.

Data Protection: Data protection is the process of protecting sensitive information from damage, loss, or corruption. As the amount of data being created and stored has increased at an unprecedented rate, making data protection increasingly important. Data protection has become a significant concern in the digital age. The way personal data is collected, processed, and stored can have profound implications for individuals' privacy and security. Regulations like the General Data Protection Regulation (GDPR) in Europe have set standards for data protection, and digital human rights affirm the importance of responsible data handling and the right to control one's personal information.

Digital Access: Digital access is the right to use the internet and digital technologies. It is crucial to ensure that everyone, regardless of their socioeconomic status, has equal opportunities to participate in the digital society. Digital human rights demand efforts to bridge the digital divide and expand access to digital resources and education.

Anonymity: Anonymity is the right to remain anonymous or pseudonymous online. It allows individuals to express themselves without revealing their true identities, protecting them from potential consequences or retaliation. Digital human rights uphold the right to online anonymity while acknowledging that it should not be used to engage in illegal or harmful activities.

Ownership and Control: The digital age has given rise to new forms of digital assets, including intellectual property and personal data. Digital human rights emphasize the right to own and control these assets, ensuring that individuals can exercise control over their digital lives.

Digital Due Process: Digital due process is the right to a fair and just legal process in the digital realm. It includes protections against arbitrary digital surveillance, censorship, and violations of individual rights. Digital human rights aim to establish clear legal standards and procedures to safeguard individuals' rights in the digital space.

Digital Health: Digital health encompasses the right to secure and confidential healthcare-related data and services. As healthcare information becomes increasingly digital, it is vital to protect the privacy and security of individuals' health data.

Digital Education: Digital education is the right to access quality education in digital literacy and ensure that everyone can participate in the digital society. It is essential to empower individuals with the knowledge and skills needed to navigate the digital world effectively and responsibly.

Freedom of Assembly: The digital realm has become a space for individuals to assemble and organize for political, social, and other purposes. Digital human rights guarantee the right to gather and express collective voices online, promoting freedom of assembly and association in the digital age.

CHALLENGES OF DIGITALIZATION IN PROTECTION OF HUMAN RIGHTS

- Digital Divide and Digital inequality
- Freedom of Speech and Expression
- Data Protection and Surveillance
- Internet shutdown and Violation of Human Rights
- Propaganda, misinformation and fake news
- Systemic Cyber Vulnerability and Digital Insecurity
- Digitalisation induced centralisation
- Online Harassment

Digital Divide and Digital inequality

Digitisation has transformed the daily experience of Indian citizens over the last few decades. In particular, Goal 9 of the SDGs sets an ambitious target to significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020 but it has not been achieved yet. Today, the average number of internet connections in India has reached about 800 million. Yet, tele density in rural areas is far lower than in cities. For instance, according to the TRAI data, rural tele density stands at 58 per 100 inhabitants, in contrast to the urban tele density, which stands at 135[1] . In rural India, higher pricing for broadband connectivity and wireless access means that access is generally much lower. And with more pronounced social hierarchies around gender and caste and other social determinants, access is also restricted for segments of the population. Between urban and rural India, there is a wide digital infrastructure divide, the problem of funding is still not able to meet the cost of infrastructure creation in rural areas. Due to the booming private telecom industry, the competent private sector organisations avoid building towers in rural areas as they are not commercially viable. Currently over 25,000 villages remain deprived of mobile connectivity because providing mobile connectivity in such locations is not commercially viable[2].

High level of digital illiteracy is the biggest challenge and hindrance in the success of digital Rights. Also, India had a rank of 73 out of 120countries for internet literacy. (2021)In addition, digital services are not available in local languages, which is a major barrier to digital literacy[3].

One traditional human rights concern that has been aggravated by digital technology is global inequality. This is caused by the lack of access to technology, rather than technology itself. While those of us who live in the digital ecosystem can't remember what daily life is like without Internet connectivity or our digital devices, the majority of people in the world have zero digital experience. Globally, nearly six out of ten people are not connected to the Internet. Even more stark is the fact that roughly 65 percent of people in the developing world do not yet use the Internet[4]. And women generally have less access to the Internet (another expression of gender inequality), as do people living in rural area.

These digital divides have the potential to significantly exacerbate existing global inequality and lead to conditions where conflict is more likely. Nearly all of the UN Sustainable Development Goals adopted depend on expanding access to information and communications technology infrastructure around the planet.When we consider the growing emphasis on providing services, facilities, and opportunities via digital means. In a country where universal digital literacy and access are still a ways away, making access to public services dependent on digital infrastructure means that we are in fact leaving a large section of our population behind. And, in doing so, we are deepening the same historical inequalities that have existed in our society for centuries.

According to India Inequality Report 2022, the digital divide in the access and usage of ICTs and the internet has also led to an exclusionary consequence in three sectors of utmost significance: education, health and finance. In a country plagued by high socioeconomic inequality, the digitalisation process cannot be posited as the panacea for the inherent challenges of the physical world. It becomes particularly problematic when half of the population neither has access to gadgets and the internet or the technological know-how to move to a digital environment. In such circumstances, the digitalisation process becomes unequal, favouring the digitally connected while excluding the rest, and in certain cases, exacerbating the already existing inequalities[5].

Freedom of Speech and Expression

Freedom of expression is a cornerstone of democracy and a fundamental human right. In the digital age, this right takes on new dimensions. The internet provides a platform for individuals to express their views, access information, and participate in public discourse. However, it also poses challenges in terms of hate speech, misinformation, censorship, and online harassment. Digital human rights demand that individuals be allowed to express themselves online without fear of censorship or retribution while balancing the need to combat hate speech and disinformation. Here, it is also important to ensure that digitisation is grounded in democratic values, and it provides power to the users where their freedom of speech and privacy is protected. The right to freedom of expression must be preserved online as well as offline, and must go hand-in-hand with addressing online hate speech and disinformation.

Digital technology can also facilitate repression. Governments unfortunately have enhanced capacities to censor expression, block or filter access to information, monitor online activity, and more effectively and efficiently control populations than they did in the pre-digital world. Perhaps the most advanced version of cyber repression is seen in China where a combination of digital tools for mass surveillance, censorship, and social monitoring provide a rich and comprehensive means of social and political control. China apparently employs two million Internet police who are tasked with monitoring online activity of citizens and sifting through millions of messages on social media and micro-blogging sites. This data is compiled into government reports about the potential for social unrest and is used to clamp down on political and social activity. In light of these developments, one of the most fundamental questions that must be addressed is: How can we ensure technology is used to enhance freedom, rather than to facilitate repression or other nefarious objectives? Making progress on this question alone would be a big contribution to international human rights.

Data Protection and Surveillance

Privacy is one of the most fundamental human rights. It is enshrined in international documents such as the Universal Declaration of Human Rights and is essential for protecting human dignity. In the digital age, privacy is at risk due to the constant collection and analysis of personal data. Companies, governments, and other entities can gather vast amounts of information about individuals, often without their knowledge or consent. Digital human rights include the right to privacy in the digital realm, ensuring that personal data is protected, and surveillance is conducted within the bounds of the law.Data is not without errors and is prone to manipulation. Hence, conversations and considerations around data privacy is a growing concern. Here a question arises whether any organization really need all the data they collect. Risk will be minimized with data minimisation i.e. gathering the least amount of data possible to fulfil one's purpose. One of the most important considerations when it comes to data and privacy is not just when you take the data, but also what you do with that data beyond the purpose for which it was collected. Data can have very real repercussions on people's lives and safety. Moreover, when everything is online, glitches and errors can deprive people of basic fundamental entitlements. We need to approach data privacy laws in India in the same way that we did the Right to Information Act.

Internet shutdown and Violation of Human Rights

India's frequent internet shutdowns have a disproportionately negative impact on impoverished communities that rely on the government's social protection programs for sustenance. The country's extensive internet shutdowns since 2018, the highest in the world, undermines the effectiveness of the government's flagship "Digital India" initiative, which emphasizes the importance of regular internet access for delivering essential public services[6]. Access to the internet is not only essential for freedom of expression and association, but also for a range of economic and social rights. As governments continue to digitize and automate core social security programs, internet access has and will increasingly become vital for the realization of the rights to social security, education, health, work, and the right to food, among others.

In India, most shutdowns involve cutting off access to the internet on mobile phones within a certain area. But this translates into an internet blackout for most of the population within this area, because 96 percent of internet subscribers in India use their mobile devices to access the internet, while only 4 percent have access to fixed line internet. Mobile connectivity is even more critical in rural areas, as 94 percent of fixed line connections were concentrated in urban areas. As such, these shutdowns especially harm people who cannot pay for fixed line internet, as well as those living in rural and remote areas where there is little to no access to fixed line internet[7].

However, as the government has moved to digitize NREGA, including its attendance checks and wage payments, adequate access to the internet has become essential for people's ability to receive these vital benefits. Network coverage is already poor in remote areas covered by the program, causing serious challenges and setting back progress on poverty reduction, but shutdowns that cut off internet access only make the situation worse. Apart from harming the government's efforts to ensure the right to livelihood, as enshrined in the Indian constitution, internet shutdowns also impact a key social protection policy to provide subsidized food grains under the National Food Security Act through a targeted public distribution system.

Propaganda, misinformation and fake news

Massive digital misinformation is becoming pervasive in online social media to the extent that it has been listed by the World Economic Forum as one of the main threats to our society[8]. The spread of false information and disinformation online can have serious consequences for democratic processes and public discourse. Addressing this issue while respecting freedom of expression is a delicate balance. Since information and communication technology is so central to the life nowadays, young people are particularly vulnerable to propaganda, misinformation and fake news. Young people spend a significant amount of their time watching television, playing online games, chatting, blogging, listening to music, posting photos of themselves and searching for other people with whom to communicate online. They rely heavily on information circulated online for their knowledge of the world and how they perceive really[9]. Online hate speech and disinformation are circulating at an accelerated pace. Journalists, politicians and human rights defenders face constant surveillance and are subject to frequent online attacks.

Systemic Cyber Vulnerability and Digital Insecurity

In a context where everything is being digitally connected and links between the physical world and the cyber realm are expanding, society-wide digital insecurity and cyber vulnerability may be the biggest systemic threat of all. As more sectors of society have been digitized, the Internet has become the backbone of all infrastructures. While that interconnectivity and interdependence certainly has its upsides, one of the biggest risks is an exponential increase in cyber vulnerability to which all sectors of society are now subject. Cases of cybercrimes particularly of financial digital frauds are reporting more frequently. According to the recent NCRB data nearly 66 thousand cases of cybercrime was reported in year 2022, which is 24 percent more than the year before[10].

Digitalisation induced centralisation

As digital technology integrates governance and the central government holds most data, centralisation can cause discord between the central and the state. It becomes more relevant when specific standards are prescribed by the Central government for data sharing as a precondition to financial assistance.

Online Harassment

Online harassment, cyberbullying, and other forms of digital abuse can have severe consequences for individuals' mental and emotional well-being. Digital human rights advocate for the protection of individuals from such harm and the establishment of mechanisms to address and prevent online harassment.

INTERNATIONAL AND NATIONAL FRAMEWORK OF DIGITAL HUMAN RIGHTS

- International Framework of Digital Human Rights
- International Covenant on Civil and Political Rights
- International Telecommunication Union (ITU)
- The United Nations Human Rights Council
- Regional and national approaches of digital governance

At the international level, several key documents and organizations are instrumental in upholding digital human rights:

The Universal Declaration of Human Rights, adopted by the United Nations General Assembly in 1948, sets out the fundamental human rights that apply to all people, regardless of their nationality, race, gender, or other characteristics. Many of the principles articulated in this declaration, such as the right to privacy, freedom of expression, and the prohibition of discrimination, are highly relevant in the digital age.

The International Covenant on Civil and Political Rights (ICCPR) is another core international treaty that affirms the importance of civil and political rights, including freedom of expression, freedom of assembly, and the right to privacy. The ICCPR has been interpreted in ways that apply these rights to the digital domain.

International Telecommunication Union (ITU), a specialized United Nations agency, addresses issues related to information and communication technologies. It plays a role in setting international standards and policies that impact digital access and telecommunications infrastructure.

The United Nations Human Rights Council is responsible for addressing human rights issues on a global scale. It has explored various aspects of digital human rights in its work, including the appointment of a Special Rapporteur on the right to privacy in the digital age.

Regional and national approaches

Many regions and countries have taken steps to recognize and protect digital human rights through laws, regulations, and national policies. Here are a few examples:

The European Union (EU): The European Union has been a leader in data protection and privacy rights. The General Data Protection Regulation (GDPR), which came into effect in 2018, is one of the most comprehensive data protection regulations globally. It establishes strict rules for data collection, processing, and the rights of individuals to control their data.

The United States: The United States has a unique approach to digital human rights, with a strong emphasis on the First Amendment and freedom of expression. USA internet governance model prioritize openness, innovation, and inclusion. It preserve global network security, interoperability, and stability as well as promote multi-stakeholder processes and increased global stakeholder participation in internet governance discussions. The debate over net neutrality has been prominent, and there are ongoing discussions about the regulation of tech companies and their impact on freedom of expression and privacy.

China: China, on the other hand, has a distinct approach to digital human rights, with significant internet censorship and surveillance measures. The "Great Firewall" restricts access to certain websites and platforms, and extensive surveillance systems monitor online activities. It's important to note that the recognition and protection of digital human rights can vary widely even within regions and nations. The balance between individual freedoms and national security, cultural norms, and political ideologies can significantly influence how digital rights are upheld.

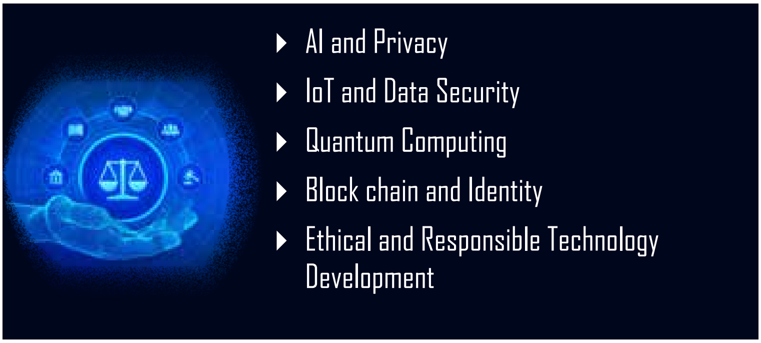
India: India is one of the biggest markets by user base for several technology corporations. It has its own "independent" path to governing the digital economy, elevating the risks for a fragmented internet. The Digital Personal Data Protection Act (DPDA) 2023 is India's first data protection act, and it establishes a framework for the processing of personal data in India. This Act now stands as a crucial component alongside the Digital India Act addressing the governance of personal data in India. Collectively, these legislative efforts represent a significant stride towards bolstering data protection in the country's swiftly evolving digital landscape[11]. Digital India Act (DIA) is companion legislation of DPDA which sets to replace 22 years old IT Act. The Digital India Act will deal with the whole ecosystem of technology[12]. The skeleton of the DIA is the legal framework and principles intact and the core constituents of the DIA are online safety, trust and accountability, open internet, and regulations of new age technologies like artificial intelligence and blockchain technologies[13].

At its core, the DPDP Act aims to establish a higher level of accountability and responsibility for entities operating within India, including internet companies, mobile apps, and businesses involved in the collection, storage, and processing of citizens' data. With a strong emphasis on the "Right to Privacy," this legislation seeks to ensure that these entities operate transparently and are answerable when it comes to handling personal data, thus prioritizing the privacy and data protection rights of Indian citizens. The DPDP Act's scope extends beyond the borders of India, encompassing digital personal data processing activities abroad. This extension applies specifically to organizations offering goods or services to individuals in India or engaging in the profiling of Indian citizens. In doing so, the Act fortifies data protection measures not only within India but also concerning Indian citizens' data handled abroad.

The DPDA Act grants certain rights to individuals including the right to obtain information, seek correction and erasure, and grievance redressal. The central government may exempt government agencies from the application of provisions of the Act in the interest of specified grounds such as security of the state, public order, and prevention of offences. The central government will establish the Data Protection Board of India to adjudicate on non-compliance with the provisions of the Bill.

Exemptions to data processing by the State on grounds such as national security may lead to data collection, processing, and retention beyond what is necessary. This may violate the fundamental right to privacy. The Act does not regulate risks of harms arising from processing of personal data. It does not grant the right to data portability and the right to be forgotten to the data principal. The Act allows transfer of personal data outside India, except to countries notified by the central government. This mechanism may not ensure adequate evaluation of data protection standards in the countries where transfer of personal data is allowed. The members of the Data Protection Board of India will be appointed for two years and will be eligible for re-appointment. The short term with scope for re-appointment may affect the independent functioning of the Board[14].

FUTURE OF DIGITAL HUMAN RIGHTS, THREATS AND WAY OUT



- AI and Privacy
- IoT and Data Security
- Quantum Computing
- Block chain and Identity
- Ethical and Responsible Technology Development

The future of digital human rights is a dynamic and evolving landscape that will be shaped by various factors, including technological advancements, legal and regulatory frameworks, international cooperation, advocacy and activism, and the development of ethical and responsible technology. Here's an expansion on what the future holds for digital human rights:

Technological Advancements

Technological advancements are a driving force in shaping the future of digital human rights. Emerging technologies like artificial intelligence (AI), the Internet of Things (IoT), quantum computing, and blockchain will introduce new challenges and opportunities for the protection of digital rights:

AI and Privacy: Artificial intelligence, or AI, is technology that enables computers and machines to simulate human intelligence and problem-solving capabilities. AI, in its broadest sense, is intelligence exhibited by machines, particularly computer systems, as opposed to the natural intelligence of living beings. As AI becomes more integrated into our daily lives, there will be concerns about how AI systems handle personal data and make decisions. Digital human rights will need to adapt to ensure that individuals' privacy and data rights are upheld in AI-driven environments.

IoT and Data Security: The Internet of things describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. The Internet of things encompasses electronics, communication, and computer science engineeringThe proliferation of IoT devices raises concerns about data security and personal privacy. Ensuring the security of these devices and the data they collect will be vital for protecting digital rights.

Quantum Computing: It is a new approach to calculation that uses principles of fundamental physics to solve extremely complex problems very quickly. Quantum computing has the potential to break current encryption standards, which could impact the privacy and security of digital communications. The future will involve developing new cryptographic techniques to safeguard digital rights in a post-quantum world.

Blockchain and Identity: Blockchain technology offers opportunities for secure and self-sovereign digital identity. This can enhance privacy and control over personal data, aligning with the principles of digital human rights.

International Cooperation

International cooperation will play a crucial role in shaping the future of digital human rights. As digital rights transcend national boundaries, it is imperative that countries work together to establish a global framework:

Multilateral Agreements: The development of multilateral agreements and conventions addressing digital rights will be essential. These agreements can set common standards for the protection of privacy, freedom of expression, and digital security.

Global Data Protection Standards: There may be a move towards harmonizing data protection standards at a global level, reducing disparities in data privacy regulations across regions.

Cybersecurity Collaborations: International cooperation in addressing cybersecurity threats will strengthen digital security and protect individuals from cyberattacks.

Legal and Regulatory Frameworks

Countries and regions will continue to develop and adapt legal and regulatory frameworks to address digital human rights. Some key developments may include:

Updates to Data Protection Laws: Governments will update and refine data protection laws to address new challenges, such as those posed by AI and IoT. These laws will ensure individuals have greater control over their personal data.

Digital Bill of Rights: Some countries or regions might consider enacting a digital bill of rights to codify the protection of fundamental digital freedoms, similar to constitutional rights.

Regulation of Tech Giants: There will likely be increased scrutiny and regulation of technology companies to ensure that they respect digital rights while addressing concerns about their market dominance and influence

Ethical and Responsible Technology Development

The technology industry is increasingly recognizing the importance of ethical and responsible technology development. Key trends in this area include:

Privacy by Design: Tech companies are integrating privacy protections into the design of their products and services from the outset.

Algorithmic Transparency: There will be a push for transparency in algorithmic decision-making to ensure that AI systems do not discriminate or infringe on individual rights.

Ethical AI: The development of ethical AI frameworks will ensure that AI technologies respect human rights and do not perpetuate bias or discrimination.

ROLE OF CIVIL SOCIETY IN DIGITAL HUMAN RIGHTS

- Public Awareness
- Lobbying and Policy Advocacy
- Legal Challenges:
- Watchdog

Civil Society organisations at the grassroots are well placed to support communities with issues of digital literacy and access, given their close relationship with people at the last mile and understanding of community networks. CSOs can play better role in awareness, raising digital literacy, facilitating people to avail the digital human rights. And most importantly keeping the watch of violations of digital human rights. CSOs are important stakeholder in promoting and protecting the human rights. It is true in the case of digital human rights also.

However, few organisations are actively engaging with digital rights today. Organizations are still lagging behind to understand the integral value of digital in every aspect of life today. We need to figure out how to make civil society understand that digital rights are no different from any other development issue. In fact, if digital is integrated into programming, everything will be much faster and better in the long run. And in any case, there is no future without digital. It's just a matter of time to make it contextually relevant.

The role of CSOs can also extend beyond their own programmes to overseeing policy implementation at the grassroots. CSOs can make sure that schemes reach the people who need them the most. The challenge in fulfilling this role at scale, however, is that the number of actors in this field is limited. Civil society organizations, activists, and individuals will continue to play a significant role in shaping the future of digital human rights:

A. Public Awareness

CSOs can play better role in awareness, raising digital literacy, facilitating people to avail the digital human rights. Advocacy and education campaigns will raise public awareness about digital rights, ensuring that individuals are informed and engaged in the protection of their own digital freedoms.

B. Lobbying and Policy Advocacy

Advocacy groups will push for changes in policy and corporate behavior, holding governments and tech companies accountable for respecting digital rights.

C. Legal Challenges

Legal challenges to protect digital rights, such as challenging government surveillance practices, will continue to be an important tool in upholding digital freedoms.

D. Watchdog

Most importantly CSOs will keep the watch of violations of digital human rights. CSOs are important stakeholder in promoting and protecting the human rights. It is true in the case of digital human rights also. Grassroots initiatives, such as the fight for net neutrality, will play a vital role in shaping policy and holding stakeholders accountable

CONCLUSION

In sum, we are in the midst of a massive digital transformation that has affected every aspect of society. Digital technology has brought many challenges to the enjoyment of human rights, to security, and to governance. The test for governments, private sector actors, members of civil society, and the technology community is whether through multi-stakeholder collaboration they can develop proactive and holistic policies that ensure that technology is used to increase both freedom and security, and that the benefits of digital technology is spread to people around the globe.

Digital human right is a critical component of the digital age, ensuring that individuals can navigate the digital world with dignity, privacy, and freedom. The protection of digital human rights is a multifaceted challenge, involving governments, international organizations, tech companies, civil society, and individuals. Balancing the ever-evolving technological landscape with fundamental freedoms is a complex task, but it is essential for a just and equitable digital society. The future of digital human rights lies in our ability to adapt to technological change while upholding the principles and protections that have been at the core of human rights for generations. As we continue to shape the digital world, it is imperative that we do so in a way that safeguards the inherent dignity and rights of all individuals, both online and offline.

States is responsible to uphold human rights, including in the online sphere, and we need to hold them accountable. Functional democratic processes require a free flow of information. Keeping free, pluralistic, independent information accessible to all, and allowing journalists and human rights defenders to perform their work, is paramount to the protection of human rights. Let's ensure we are taking those steps and advancing towards a world where we are protected from the dangers of attacks online, and where freedom of expression and the right to participate are unhindered for all. It is time for policymakers to be more proactive and holistic, and to advance practical solutions to several priority global human rights challenges.

In pushing digital indiscriminately, we are failing to understand how societies work, how communities work, and how we facilitate them with their rights, given the new means of serving them. We therefore need to place greater emphasis on intersectionality; in today's world, we cannot address issues of sanitation, gender, health, and rights without providing equitable access to technology with adequate safeguards for people's data. Ultimately, the larger challenge in the years to come will be to make digital literacy materials around digital rights much more inclusive and participative for all Indians.

These examples raise alarm bells about how both human rights protections and the human rights governance framework are being threatened in the digital context. There is a pressing need to find a way to capitalize on the upsides of digital technology while reducing the human rights risks. A core question is: How do we reinforce the international human rights law framework that already exists, but make it more relevant and potent in the digital context? In effect, we are in a rhetorical battle for the dominant narrative of the 21st century. How do we meet this challenge and reinforce the relevance of human rights principles in the global digital governance ecosystem?

★★

Reference:

1. https://idronline.org/article/rights/data-protection-and-digital-rights-in-india
2. https://www.drishtiias.com/daily-updates/daily-news-editorials/citizen-centric-digital-revolution
3. https://www.livemint.com/opinion/online-views/india-must-lead-the-creation-of-a-citizen-centric-digital-economy-11667409066158.html
4. https://www.hrw.org/news/2016/03/25/digital-disruption-human-rights
5. https://www.oxfamindia.org/knowledgehub/workingpaper/india-inequality-report-2022-digital-divide?psafe_param=1&gad_source=1&gclid=Cj0KCQjw2a6wBhCVARIsABPeH1vRdt4L-IBgE-NcuWS8-PP7zXGLSu_31t-O0D_B_ocpwusUxgNUeFoaAuuOEALw_wcB
6. https://economictimes.indiatimes.com/news/india/indias-recurrent-internet-shutdowns-threaten-its-own-flagship-digital-initiative-hurt-the-vulnerables/articleshow/100982550.cms?from
7. https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic
8. https://www.pnas.org/doi/10.1073/pnas.1517441113
9. https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/dealing-with-propaganda-misinformation-and-fake-news
10. https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/#:~:text=(NCRB)%20Sunday.-,According%20to%20the%20report%20’Crime%20in%20India’%2C%2065%2C893%20cases,2021%20to%204.8%20in%202022.
11. https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/
12. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1948357
13. https://vidhilegalpolicy.in/blog/explained-the-digital-india-act-2023/
14. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

Pairvi

Public Advocacy Initiatives for Rights and Values in India (PAIRVI) is a capacity building and advocacy support organization working at the intersections of rights, development and sustainability. It works with small grassroots organizations and community based groups to enhance their understanding on development discourse and capacity to respond appropriately.
PAIRVI also works with a pan Indian coalition on climate and environmental justice, MAUSAM (Movement for Advancing Understanding on Sustainability and Mutuality), previously Beyond Copenhagen.

Visit: www.pairvi.org Contact: pairvidelhi1@gmail.com, info@pairvi.org