

Original Article

Human Rights Issues in the Digital Era

Divya Sharma

HR Manager, Cognizant, India.

Received: 03-06-2021

Revised: 03-24-2021

Accepted: 04-01-2021

Published: 04-03-2021

ABSTRACT

The rapid growth of digital technologies such as the internet, artificial intelligence, social media, and big data has transformed modern societies, creating both opportunities and challenges for human rights. This study examines how digitalization affects fundamental rights including privacy, freedom of expression, access to information, equality, and non-discrimination. Key concerns include data surveillance, misuse of personal information, algorithmic bias, cyber harassment, misinformation, and the digital divide. Using a literature review and policy analysis approach, the research evaluates digital governance models and regulatory frameworks aimed at protecting digital rights. The findings show that while digital technologies promote transparency, communication, and civic participation, they also create new risks that require strong legal, ethical, and technological safeguards. The study emphasizes the need for international cooperation among governments, technology companies, and civil society to ensure accountability and protect human dignity in the digital age.

KEYWORDS

Digital Rights, Human Rights, Digital Privacy, Artificial Intelligence Ethics, Online Freedom Of Expression, Cyber Governance, Data Protection, Digital Inequality, Algorithmic Bias, Internet Regulation.

1. INTRODUCTION

1.1. Evolution of Digital Human Rights

The idea of the digital human rights can be traced back to the late twentieth century when the internet technologies began to grow rapidly and spread all over the world. During the internet infancy, the two issues that were greatly discussed were the right to access to information and safeguard of the freedom of expression in the online environment. With the further penetration of the digital technologies into the life, the environment of digital rights experienced the widening to encompass the issues of data privacy, cybersecurity, digital identity, and surveillance on the Internet. High penetration of social media sites, cloud computing systems, mobile technology, and analytics on big data have created wealth of intimate data available on the digital world, and injected fresh ethical and legal issues on how this data may be kept safe. To address these issues, governments, international agencies and regulators have embarked on creating laws and policy provisions that will be used to protect the rights of persons in the virtual world. Several laws and other measures have been enacted regarding data protection, legislations in digital privacy and cybersecurity measures in various countries to curb problems of unauthorized data mining, cybercrime and online surveillance. International efforts have also contributed to the necessity to advance human rights in the digital era through encouraging ethical technology management and open approaches to data management. Nonetheless, as much as these regulatory measures are being made, technology tends to keep accelerating ahead of policy and law enforcement. The recent technological advancements on artificial intelligence, biometric surveillance systems, and data analytics at large cannot cease to pose new challenges to the policymakers, legal institutions, and the technology developers. Consequently, the digital human rights development is a continuous process, which must be continually adjusted to guarantee that technological advancement promotes the key human rights and democratic principles.

1.2. Human Rights Issues in the Digital Era

The progress of digital technologies at a rather fast pace has changed the modern societies considerably, making a serious impact on the way people communicate, get access to information and engage in economic and social activities. As the digital innovation provided new platforms of growth and network, it has brought along with it intricate issues touching on the protection of human rights. Technological systems and digital platforms are taking over the most basic rights like privacy, freedom of speech, equality, and access to information in the digital age. The popularity of internet, artificial intelligence, social media network and big data analytics has transformed how human rights are exercised and guarded. With the digital technology gaining massive penetration in the sphere of governance, commerce, and ordinary life, there is the need to study the numerous human rights concerns emerging in the digital realm.

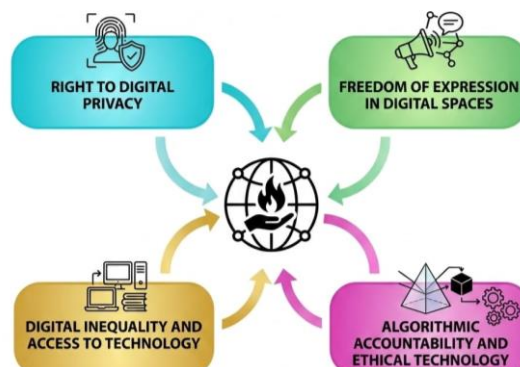


Fig 1- Human Rights Issues in the Digital Era

1.2.1. Right to Digital Privacy

The issues of the individual privacy preservation are taken as one of the most important human rights issues in the digital age. As the Internet based services, social networking sites, and computer applications develop, a great amount of personal information has been getting incessantly gathered, processed and stored. This information can be about personal identities, browser habits, geographical details, and records related to money. As much as the data collected in this way makes it possible to obtain personalized services as well as innovation in technology, it raises the chances of loss in privacy. Data sharing without permission, data breaches, as well as the intrusive surveillance, may undermine individual autonomy and personal security. The aspect of internet privacy should involve high data protection laws, open practice of data governance and responsible technological design that honors user privacy and consent.

1.2.2. Freedom of Expression in Digital Spaces

The digital space has widened the access of person in giving opinions and presenting ideas in addition to taking part in the global conversations. Civic engagement and open communication are available through social media networks, blogs and Internet forums. Nonetheless, these media are confronting the issue of balancing between freedom of expression and the necessity to regulate hate speech. Problems with misinformation, hate-based content, extremist statements, and online harassment are challenges to the regulators and policymakers in the platforms. Too much moderation and excessive regulation will curb legitimate speech whereas too little regulation will cause toxic content to become viral. Thus, there is a significant issue of balancing the right to free speech and the need to have responsible communication in the digital world as a key human rights issue.

1.2.3. Digital Inequality and Access to Technology

The other critical human rights concern in the digital era is the problem of digital inequality that means unequal access to digital technologies and the internet connection. People in most parts of the world, particularly those of the developing world and those in rural areas do not have access to the internet, digital equipment or training on how to entirely engage in digital society. Such digital divide has the potential to restrict access to education, economic engagement, as well as access to some of the most critical services, which are increasingly being distributed online. To redress digital inequality, it is important to invest in digital infrastructure, affordable internet services and learning programs that will foster the concept of digital literacy and inclusive engagement.

1.2.4. Algorithmic Accountability and Ethical Technology

An increasingly popular use of artificial intelligence and automated decision-making systems has also supported the question of algorithmic responsibility as well as ethical technological development. The decision making on fields like recruitment, credit scoring, healthcare services, and law enforcement are some of the fields where algorithms are gradually making decisions. These systems might however give biased or discriminatory results as long as they are based on biased data or lack transparency. This may tap into the rights of people to equality and fairness in the process of making decisions. The creation of ethical technology involves the following: transparency in designing the algorithm, accountability system, and routinely testing automated systems to avoid discrimination and safeguard human rights in the digital world.

1.3. Human Rights Issues in the Digital Era

The digital age has considerably changed the manner in which people communicate, interact, and access information, whereas it has raised a number of thorny and ambiguous human rights

issues. With the penetration of digital technologies including the internet, social media and artificial intelligence systems, as well as the large data systems in the daily life, the dependency and exercise of basic human rights is subject to an increased succession by the digital technology. The problem of data privacy is one of the most burning issues of the digital environment. Contemporary digital technologies gather users abundant personal data such as personal identities, browsing, location data and the online activities. Although such information promotes custom-made services and technological creativeness, it similarly brings up the issues of unauthorized data exchange, information attacks, and intrusive monitoring measures. The other relevant matter is the influence of digital platforms on the freedom of speech. On the one hand, online channels provide people with the possibility to express their opinions, take part in conversations, find various sources of information; on the other hand, they lead to the emergence of certain issues connected to the proliferation of false information, hate speech, and de-beneficial online content. Moderation of content to safeguard free expression and accountable control of content is one of the greatest concerns by policy makers and technology industries. Also, in some cases, algorithmic decision making machines that run on artificial intelligence may yield biased results when based on incomplete or discriminating data set. Algorithms can become biased, leading to unjust treatment of people in several fields like work, finances, and law enforcement, thus, an issue of equality and integrity in computer governance emerges. The other major problem is that of digital inequality, or more commonly known as the digital divide, whereby specific groups of people do not have sufficient access to digital infrastructure, the internet and lack of digital literacy skills. This disparity may hinder access to education, work and contribution into digital economies. Moreover, online bullying and cyber harassment is a widespread problem that impacts the mental health of people and makes them unwilling to engage in the digital environment. These concerns are pointing to the necessity to involve more extensive regulatory frameworks, ethical practices in the development of digital technologies, and raise awareness of people to make sure that digital technologies help and safeguard fundamental human rights in the world that becomes more connected.

2. LITERATURE SURVEY

The literature abounds with digital human rights studies as the digital technologies keep to gain influence over the social, economic and political life. There has been a scholarly discussion among the field of law, information technology, sociology, and public policy on the impact of emerging technologies on the basic human rights of privacy, equality and freedom of expression. The opportunities and the risks of digital transformation are mentioned in the literature. Although the digital media broadens access to information, communication, and civic engagement, it also brings new issues like surveillance, algorithmic discrimination, and the doing of harmful information. Scientists note that proportional regulations should be created, which would strike the balance between human rights and technological advancement. The subsections below present some of the key themes in the existing research with an emphasis on digital privacy and surveillance, bias in artificial intelligence systems, and the changing nature of freedom of expression on the Internet.

2.1. Digital Privacy and Surveillance

There has been a considerable amount of research on digital privacy issues and surveillance issues in the current technological environment. As the use of internet service, social media networks, cloud computing and mobile applications grow very fast, vast amount of individual information is continuously being collected, processed and stored by the government and corporations. Researchers say the bulk of data collected is highly questionable in terms of ethics and legal concern; specifically the autonomy and informed consent of an individual and the ownership of the data. Research has

revealed that surveillance systems which include facial recognition, biometric identification, location tracking, and predictive analytics have allowed institutions to monitor individuals in levels never seen before. Although these technologies can enhance security, safety in the larger society, and service, researchers caution that unrestrained surveillance can result in abuse of civil liberties, chilling the freedom of expression, and normalizing surveillance. The aspect of surveillance capitalism, in which companies glean and process user data to profit off of it, is also mentioned in several scholarly publications. To address these issues, the literature proposes more robust data protection systems, open governance institutions, and ethics in order to make sure that digital technologies do not violate basic privacy rights.

2.2. Artificial Intelligence and Algorithmic Bias

Stemming directly from the issues of digital human rights is another significant research topic, that of the ethics of artificial intelligence (AI) and the existence of algorithmic bias in automated decision-making processes. The field of artificial intelligence systems is being heavily applied in recruitment, credit rating, medical diagnosis, law enforcement, and legal decision support. Although AI systems are deemed to be efficient and objective, a significant body of research indicates that algorithm models may inadvertently replicate or exacerbate social inequality, which exists. Investigators point out that machine learning systems are very dependent on past data to train them and when such data has biased or incomplete information, the attained algorithms could generate discriminatory results. Indicatively, research studies have indicated that, in some instances, facial recognition systems have decreased accuracy in people with dark skin color or women because of disproportionate training information. On the same note, predictive policing algorithms can be biased against some communities in case the historical crime data is biased. According to scholars such prejudices are likely to jeopardize the value of fairness, equality and non-discrimination that form the foundation of human rights frameworks. As a result, the literature urges creating AI ethical principles, algorithm transparency, non-discriminatory data structure, and control components over algorithms to promote responsibility and adaptability in AI-based structures.

2.3. Freedom of Expression in Online Platforms

With the advent of digital communication platforms, there has been considerable change in how people are expressing their freedom of expression right. Internet forums, social media networks, and other digital publishing platforms help users to express opinions, access various perspectives and engage in a global discussion at ease than in the past. Researchers point out that such sites have bolstered democratic participation and citizen journalism as well as social movements as those that are locked out can be heard by more people. Nonetheless, the literature also states that there are a number of challenges related to the use of digital speech environments. Misinformation, disinformation struggles, hate speech, harassment, extremist content in online platforms are a common problem. These issues create some convoluted questions concerning the role of the technology companies in censoring the content and still maintaining the open conversation. Academics observe the moderate content moderation can limit the rightful expression, and the self-regulation can result in the evolution of illicit content and jeopardy society. Moreover, it has been questioned how strong the private technology companies are and can suppress the digital discussion by using obscure algorithms and policies of the platforms. Consequently, most scholars propose clear moderation processes, accountability systems among users and collaborative forms of government where governments, civil society and technology firms participate to ensure freedom of expression is upheld and deal with damaging online content.

3. METHODOLOGY

3.1. Research Design

This study uses research design that seeks to conduct an analytical study of problems emerging on the digital human rights in various sectors of technology, such as artificial intelligence, social media, and data governance systems. The research is performed using a qualitative and analytical research method, which includes theoretical analysis and the available scholarly publications and policy framework. The main aim of the research design would be to comprehend the effect of technological developments on such basic human rights like privacy, freedom of expression, equality, and the ability to access information. To realise this goal, the study explores the relationship of digital technologies and human rights principles in terms of a multidisciplinary model that involves information technology, legal studies, ethics, and public policy. The research design focuses on the discovery of the major problems including data surveillance, bias in algorithms, online censorship, and the dominance of privately owned technology firms in controlling online areas. By prioritizing these areas, the research has been trying to research on the opportunities as well as the threats of digital transformation in the modern societies. Comparative analysis of existing regulatory frameworks and governing models applied in various regions in creating protection of digital rights is also included in the design. Moreover, the paper examines the case study and the reported examples in the academic literature, institutional reports, and international bodies to demonstrate the practical consequences of copyright violations and the actions of the regulating bodies. This systematic research design will help the study to determine the implications of the existing technology systems regarding democratic principles and social justice in the online world. The design is also effective in determining weak points in the existing governance patterns and in noting the necessity of more ethical standards and principles, clear and transparent technological development practices, and inclusive policies regarding the digital. On the whole, it can be said that the research design is a detailed model of the study of the multifaceted relationship between technological innovation and human rights protection in the digital age and makes the analysis of the topic systematic, interdisciplinary, and purposeful.

3.2. Data Collection Methods

In the study, the qualitative data collection method is used and is based on the utilization of secondary data sources represented by reliable scholarly and institutional sources of information. These sources give detailed information on the issues of digital human rights, technology governance, and ethical issues surrounding the up-to-date digital systems. The obtained information is useful to examine the correlation of emerging technologies and basic human rights concepts.



Fig 2- Data Collection Methods

3.2.1. Academic Journals

In this study, academic journals will be a major source of academic information. Theoretical models, empirical studies, and critical commentaries on the subject of digital privacy, artificial intelligence ethics, algorithms bias, and freedom of expression in the digital space are offered on peer-reviewed journal articles. Such journals usually follow high-quality research techniques and proved conclusions thus can be depended upon as sources of academic research. The research examines several journal publications in the disciplines of information technology, law, social sciences, and communication studies, to compile varied views of the way digital technologies affect human rights in the modern societies.

3.2.2. Policy Reports

Government, research, and international policy think tanks policy reports were also significant sources of data. These reports present viable information on regulatory frameworks, regulatory policy programs, and strategic steps embraced by governments and other organizations to curb the problem of digital rights. The policy documents tend to assess the role of new technologies in governance, economic growth, and social welfare and prescribe policy to resolve the emerging technologies to promote ethical use of technology. By reviewing such reports, the study is in a position to know how policymakers respond to the various challenges that are facing them, including data protection, online misinformation and algorithmic accountability.

3.2.3. International Human Rights Documents

The international human rights documents play a significant role in understanding digital rights under a legal and ethical procedure. International organizations come up with documents indicating basic human rights principles such as privacy, freedom of expression and equality as elucidated by documents like the global declarations, international treaties and guidelines. These documents are the standards of normativity to which the digital technologies and practices of governance can be measured. The research will provide an analysis with standards of human rights and legal standards currently adopted by most countries in the world by looking at these international frameworks.

3.2.4. Technology Governance Frameworks

Another important source of data which has been utilized in this study is technology governance frameworks. These frameworks consist of regulatory frameworks, ethical standards, and governance models that governments, technology firms and international bodies have formulated to ensure that digital technologies are managed in a responsible manner. Data protection, accountability mechanisms, AI transparency, and responsible innovation are some of the issues they discuss. The examination of these frameworks aids the study to comprehend how various institutions are trying to control digital technologies without neglecting innovation and protection of human rights in the digital ecosystem.

3.3. Analytical Framework

The paradigm of analysis applied in this paper relies on the Digital Rights Protection Index (DRPI), which is utilised to assess the degree of protection under digital conditions of human rights. This framework proposes a systematic approach to the evaluation of the role of technological systems, governance mechanisms, and policy regulations in the provision of the fundamental digital rights protection. The model concentrates on four fundamental dimensions that are traditionally known as key elements of digital human rights, namely, the protection of privacy, freedom of expression, accessibility and security protection. These dimensions are the main spheres where

digital technology may foster or weaken the human rights based on their design, implementation, and regulation. These four components when analyzed collectively can enable the researcher to form a complex picture of the entire state in the technological ecosystems in terms of digital rights. Digital Rights Protection Index (DRPI) is obtained by summing up the results of the four dimensions and getting an overall average. Simply put, the DRPI is calculated as the result of the summation of the privacy protection, freedom of expression, accessibility, and security protection and divided by 4. The privacy protection can be defined as the level of security concerning the personal information of individuals that is not accessed, monitored, or used by organizations and governments without permission. Freedom of expression is a gauge used to gauge the freedom of individuals to access information and express their opinions online without needless restrictions and censorship. Accessibility aims towards the presence, as well as accessibility of digital technologies so that every person including the marginalized groups are equally given a chance to access the digital platforms and digital information hubs. Security protection is my evaluation of the efficiency of cybersecurity mechanisms created to keep the digital infrastructure and the user data safe against the cyber threat, hacking, and data breaches. Through this model of analysis, the study evaluates the performance of various technological landscapes and systems of governance in the safeguarding of digital rights in a systematic way. The DRPI framework also facilitates cross-comparative research of various technological industries in the form of artificial intelligence system, social media platforms, and digital data governance frameworks. Finally, this method of analysis allows defining the advantage and disadvantage of existing digital rights protection policies and offers clues to building a more robust set of ethical principles, policies, and regulatory measures that can assist human rights in the digital age.

4. RESULTS AND DISCUSSION

4.1. Analysis of Digital Human Rights Challenges

The overview of the problem of digital human rights suggests that violations of privacy, bias in algorithms, and the uncontrolled spread of misinformation are some of the most crucial threats to the individuals and societies in the digital age. With the ever-growing development of digital technologies, the accumulation of personal data is enormous, and governments, companies, and Internet resources process and store them. Although such a data-driven environment facilitates both technological creativity and better services, it makes more privacy abuses. Numerous digital platforms are based on massive data gathering activities, which are sometimes not clearly visible or informed. These acts may cause illegal data transfer, identity theft, and intrusive surveillance, thus compromising the very idea of privacy. Moreover, the increasing popularity of such surveillance technologies as facial recognition cameras, position-finding systems, and biometric identification are also a reason to worry about the fact that the personal information can be potentially abused, and the civil liberties can be lost. The other significant threat that was realized during the analysis is the existence of an algorithmic bias in artificial intelligence systems. The technology of AI is employed more and more to assist decision-making in the field of recruiting, financial services, healthcare, and law enforcement. But once trained using biased or incomplete data sets they can give discriminatory results that are disproportionately applicable to particular social groups. Algorithms bias may support the social inequalities that exist by disproportionately disadvantaging people due to race, sex, or socioeconomic status. This brings up serious ethical issues of fairness, accountability, and transparency in automated decision-making systems. More so, the fast proliferation of fake news and misinformation online has become an essential danger to democratic principles and deliberate communication among citizens. Social media networks allow the information to reach the global masses in a short period; yet also give the possibility of the dissemination of false or misleading

information over a wide area. Misinformation can also turn the opinion of people, bend the political mechanism and divide people socially. This issue is further aggravated by the absence of efficient content moderation tools as well as the contribution of automated algorithms in the propagation of sensational or deceptive information. Altogether, these issues underscore the necessity of more effective digital regulations structures, ethical methods of technologies development, and public awakening in order to get sure that technological advancement will not hurt the basic human rights.

4.2. Human Rights Challenges in Digital Platforms

The internet has revolutionized communication, access to information and socialization. Nevertheless, they also present a number of human rights issues that impact various individuals and societies in the rest of the world. The issues that are presented below are some of the most serious challenges that have been witnessed in the digital environment.

Table 1: Human Rights Challenges in Digital Platforms

Human Rights Issue	Percentage Impact (%)
Data Privacy Violations	32%
Online Hate Speech	18%
Algorithmic Bias	14%
Government Surveillance	12%
Misinformation	10%
Digital Inequality	8%
Cyber Harassment	6%

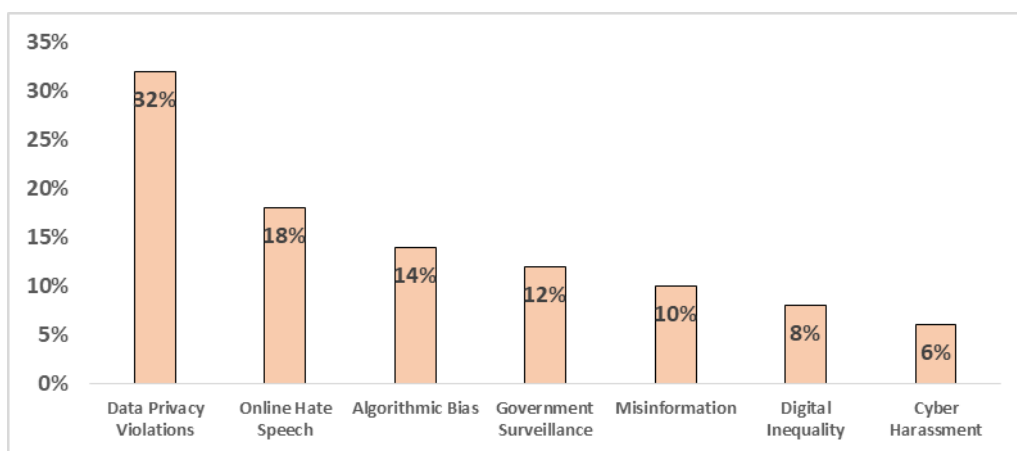


Fig 3 - Human Rights Challenges in Digital Platforms

4.2.1. Data Privacy Violations (32%)

Breach of data privacy is the greatest human rights issue with online platforms. As social media, mobile applications, and online services become widespread, they gathering a lot of personal information, such as location, browsing history, and preferences of the user. A large number of technology firms are also interpreting and selling this information to do targeted advertising and business analytics. Nevertheless, lack of adequate data protection systems and lack of clear consent terms and conditions tend to leave users vulnerable to unauthorized access or misuse of data or data leakages. These breaches are a threat to the privacy rights of individuals, and may result in identity theft, financial fraud, and loss of autonomy on the internet.

4.2.2. Online Hate Speech (18%)

Online hate speech has gained massive concern in the online platforms, especially in social media networks and discussion forums. Hate speech is the type of speech, which is rude and harmful, which is used to address a person or a group of people because of their race, religion, gender, ethnicity, or nationality. The fast proliferation of such content may lead to unfriendly online spaces, promotion of discrimination, and social polarization. Digital platforms are faced with a complicated dilemma of ensuring that harmful speech is controlled and yet freedom of expression is upheld. There should be proper moderation policies and user reporting systems to minimize the distribution of hateful and abusive content.

4.2.3. Algorithmic Bias (14%)

The outcome of the effort applied to automated decision-making processes is algorithmic bias, which can be either unfair or discriminatory because of biased training data or an incorrect algorithm design. Algorithms are used in many digital platforms to suggest content, filter information or predict user behavior. In case these algorithms are trained with datasets that are representative of historical inequalities or social biases, they will unintentionally perpetuate discrimination against a specific group of people. The problem of algorithmic bias brings up issues of fairness, transparency, and accountability to digital decision-making systems and points to the necessity of ethical development of AI and routine auditing of algorithm models.

4.2.4. Government Surveillance (12%)

Another important human right issue in the digital space is government surveillance. Online surveillance and facial recognition programs, message interception devices, among others are some of the digital technologies applied by many governments to improve national security and law enforcement operations. Although such technologies can be used to stop crime and keep people safe, in case of over-surveillance or unregulated surveillance, citizens can enjoy their right to privacy and freedom of speech. To the extent that people consider that they are being followed at all times, they will feel reluctant to voice their viewpoints and engage in social debates, and this undermines democratic involvement and civil freedoms.

4.2.5. Misinformation (10%)

Misinformation is defined as a dissemination of false or misleading information by use of digital mediums, in many instances without confirmation of accuracy. Social media sites enable information to be dispersed on a widespread level among a vast number of people and it may be challenging to regulate the dissemination of false or doctored information. The misinformation may falsify the knowledge of the people on issues of interest, affect elections, cause social panic, and erode institutional credibility. The solution to this dilemma will be more content verifying systems, better digital literacy among the audience and responsible sharing of information in online communities.

4.2.6. Digital Inequality (8%)

Digital inequity describes the unfair differences between the populations on accessing digital technologies, internet connectivity, and digital skills. In most of the parts, especially, in developing nations and rural territories, the inadequate technological infrastructure does not allow the populace to enjoy the full benefits of the digital economy and to tap into the information sources on the internet. Such inequality may expand the bureaucratic social and economic gaps, inhibiting education, business, and civic rights. To resolve the digital inequality, the digital infrastructure, low-cost access to the internet, and digital literacy program need to be invested in so that everyone has a chance to be included in the digital sphere.

4.2.7. Cyber Harassment (6%)

Online harassment is an emerging issue in the online platforms and encompasses online harassment characterized by the activities of internet bullying, threats, stalking, and harassment messages targeted at individuals. Cyber harassment may affect the subject, in most cases, emotionally, nervously and create a bad reputation. Such forms of online abuse are especially frequent in women, journalists, activists and minority groups. Anonymity of the digital platforms also has the potential to tempt an individual to do destructive acts without responsibility in some cases. To overcome cyber harassment, digital platforms should adopt more robust user protection regulations, reporting systems, and legal infrastructure that will deter abusive social behavior and safeguard users that are vulnerable.

5. CONCLUSION

The digital era has introduced ground-shifting transformations to the contemporary societies that greatly have transformed how people communicate, how they access information, how they do business as well as engage in the democratic processes. Information technologies (the internet, artificial intelligence, big data analysis, and social media systems) have provided an unprecedented chance of connecting globally, economic development, and sharing knowledge. The technologies have also allowed people to obtain educational materials, potentially enter the digital economies, and a space of dialogue at the cross of geographic borders. The role of government and other organizations heavily depend on the digital systems to provide their public services, enhance the efficiency in administration and boost development based on innovation. Through reforms, therefore, digitalization has come to be a major primary source of societal development and technological growth in the twenty-first century. Nonetheless, along with these advantages, the fast spread of digital technologies has also brought into circulation some serious complications when it comes to safeguarding the basic human rights. Problems with mass surveillance, abuses of personal information, algorithmic discrimination, and misinformation have become some of the issues that have posed serious ethical and legal issues. The mass gathering and processing of personal information by the government and other business entities have posed new threats of infringing on privacy and exploitation of information. Likewise, the application of artificial intelligence systems to make a decision can also reproduce the biases that exist in the historical data, which is not intentional and results in discriminatory actions that impact marginalized groups of people. Moreover, the digital space has turned into the place where dangerous content, cyber bullying, and fake news can be disseminated very quickly and to coordinate the devaluation of democratic principles and social credibility. These issues demonstrate a complicated nature of the connection between technological innovation and the preservation of human rights on the Internet. The way to deal with these concerns is to create wholesome legal and regulatory frameworks that can protect the rights of technology, and in the process promote the development of technology in a responsible manner. Cultures and governments need to put powerful data protection legislations, transparent monitoring provisions, and accountability measures in case of artificial intelligence system. Simultaneously, the role of the ethical design in technology firms should be embraced with the idea of the user privacy, equity, and transparency in the digital space. The other important participants in campaigning on digital rights, digital literacy, and carrying out research that can guide policymaking include the civil society and educational institutions. These stakeholders need to work together to develop mechanisms of governance that will strike a balance between the advancement of technology and the safeguarding of the basic rights. In the future, more studies are required to solve arising issues related to sophisticated technologies like artificial intelligence, blockchains systems and quantum computing. Such technologies can transform the digital infrastructures and establish new ethical issues

concerning security, ownership of data, and algorithmic governance. Researchers and policymakers need to collaborate in order to develop new regulatory models that look into these advancements in order to make sure that digital technologies are not in opposition to the human rights principles. Through technological development that incorporates the aspect of ethics and the ensuing framework of the importance of inclusive digital governance, communities can have assurance that digital transformation can make people experience dignity, equality, and social justice in an ever-reliant world.

REFERENCES

- [1] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY, USA: PublicAffairs, 2019.
- [2] D. J. Solove, *Understanding Privacy*. Cambridge, MA, USA: Harvard University Press, 2008.
- [3] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA, USA: Stanford University Press, 2010.
- [4] N. Kshetri, "Big data's role in expanding access to financial services in developing countries," *International Journal of Information Management*, vol. 37, no. 6, pp. 466–472, 2017.
- [5] C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York, NY, USA: Crown Publishing, 2016.
- [6] F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA, USA: Harvard University Press, 2015.
- [7] V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY, USA: St. Martin's Press, 2018.
- [8] J. Angwin, J. Larson, S. Mattu, and L. Kirchner, "Machine bias: There's software used across the country to predict future criminals," *ProPublica*, 2016.
- [9] K. Crawford and R. Calo, "There is a blind spot in AI research," *Nature*, vol. 538, pp. 311–313, Oct. 2016.
- [10] A. Narayanan, "Translation tutorial: 21 fairness definitions and their politics," in *Proc. ACM Conf. Fairness, Accountability and Transparency*, 2018.
- [11] T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, CT, USA: Yale University Press, 2018.
- [12] Z. Tufekci, "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency," *Colorado Technology Law Journal*, vol. 13, pp. 203–218, 2015.
- [13] J. Balkin, "Free speech in the algorithmic society: Big data, private governance, and new school speech regulation," *University of California Davis Law Review*, vol. 51, pp. 1149–1210, 2018.
- [14] L. Floridi et al., "AI4People – An ethical framework for a good AI society," *Minds and Machines*, vol. 28, no. 4, pp. 689–707, 2018.
- [15] R. Kitchin, "Big data, new epistemologies and paradigm shifts," *Big Data & Society*, vol. 1, no. 1, pp. 1–12, 2014.