ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1618

Law Technology and Human Dignity: Shaping Rights Respecting Digital future

Sunil L Kalagi[1]; Renuka S Gubbewad[2]; Ritika Sahu[3]; Shikha Dubey[4]

[1]Advocate and Legal Researcher, Kalaburgi, Karnataka
[2]Assistant Professor, Central University, Kalaburgi, Karnataka
[3]Assistant Professor, Kalinga University, Chhattisgarh
[4]Associate Professor, Indore Institute of Law, Madhya Pradesh

Publication Date: 2025/05/30

Abstract: The swift progression of technology has significantly altered civilizations, offering both unparalleled potential and substantial challenges to human rights. This article examines the complex interplay between law, technology, and human rights, highlighting the historical evolution of legal frameworks in response to technological advancements and the necessity for ongoing adaptation. It investigates significant technology advancements—such as digital surveillance, artificial intelligence, social media, biometric systems, and the Internet of Things—and evaluates their effects on essential rights including privacy, freedom of expression, equality, and security. The article emphasizes urgent human rights issues in the digital era, including extensive data gathering, algorithmic prejudice, online censorship, and digital disparity, demonstrating how technology advancements may both empower individuals and jeopardize their liberties. It also examines current international and regional legal instruments, ethical standards, and the existing gaps, emphasizing the necessity for adaptive, inclusive, and enforced frameworks. The paper emphasizes the necessity of proactive regulation, responsible innovation, and international collaboration to mitigate the rising threats linked to technologies such as blockchain, quantum computing, and deepfakes. It ultimately endorses a rights-based strategy that harmonizes innovation with the protecting and advancement of human dignity, underscoring that the protection of human rights in the digital age is crucial for cultivating a just, transparent, and inclusive future.

Keywords: *Human Rights, Digital Technology, Privacy, Legal frameworks, International law.*

How to cite: Sunil L Kalagi; Renuka S Gubbewad; Ritika Sahu; Shikha Dubey; (2025) Law Technology and Human Dignity: Shaping Rights Respecting Digital future. *International Journal of Innovative Science and Research Technology*, 10(5), 2519-2525. https://doi.org/10.38124/ijisrt/25may1618

I. INTRODUCTION

In the swiftly changing realm of Human Civilization, Technology has emerged as both a driver of advancement and a source of intricate legal and ethical dilemmas. Technological developments, from the invention of the printing press to the emergence of the internet and artificial intelligence, consistently transform society, economies, and individual rights. As these breakthroughs grow integral to daily life, they raise urgent problems regarding the adaptation of laws to evolving technology and the assurance that innovation respects human dignity, privacy, and freedom.

The convergence of law, technology, and human rights is a vital area that requires focused consideration. The law establishes a framework to govern technology advancement and its implementation, protecting fundamental rights from possible violations. Conversely, technological advancements threaten established legal frameworks, compelling communities to reevaluate concepts of privacy, freedom of expression, equality, and security.

The study aims to investigate the adaptation of laws to the digital era, assess the significant effects of technology on human rights, analyze contemporary challenges and case studies, and recommend strategies to ensure that technological advancement is consistent with human dignity and justice. The interplay between legislation and technical advancement is not novel. Historically, disruptive inventions have required legal responses to manage dangers and seize possibilities. Comprehending this historical backdrop enhances our appreciation of the persistent challenges and the necessity for flexible legal systems.

Johannes Gutenberg invented the printing press in the 1400s, which changed the way knowledge was shared. It questioned the power of the church and the government by letting ideas spread without being controlled by the church or the government. Legally, this time period led to rules about censorship and the right to free speech, which are still being debated today when it comes to rules about digital material. In the 18th and 19th centuries, industries grew quickly, changing economies and societies. Labor rules were made to

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1618

protect workers' rights, make workplaces safer, and stop child labor. To deal with new industry hazards and economic imbalances, legal systems had to change quickly. This shows how legal frameworks change in response to changes in society and technology.

In the late 20th and early 21st centuries, the emergence of personal computers, the internet, and mobile devices has marked the beginning of a new era of unparalleled connectivity. The globalized nature of online content, the rise of cybercrimes, and digital privacy concerns are all unique challenges that this technological advance presents. Since then, governments and international organizations have been attempting to establish legislation that strikes a balance between human rights, security, and innovation.

During these periods the technical advancements have frequently surpassed legal answers, resulting in discrepancies and discussions. The digital revolution persistently challenges conventional legal concepts, especially on privacy, free expression, and sovereignty. Legislators confront the challenge of formulating laws that promote innovation while safeguarding individual rights. In the internet era, jurisdictional difficulties impede cross-border law enforcement. Likewise, nascent technologies like artificial intelligence necessitate policies that are both progressive and ethically sound.

This chronological progression highlights a basic fact: the relationship between technology and law is intrinsic, and legal systems are dynamic in nature, constantly adapting to new situations. In order to guarantee that technology advancement benefits humanity in an ethical and equitable manner, it is crucial to comprehend this interaction, as we are learning more about this subject.

II. THE ROLE OF LAW IN REGULATING TECHNOLOGY

Governments, international organizations, and private companies have faced substantial regulatory issues due to the rapid expansion of technology advancements. By laying down rules, holding people to account, and safeguarding their rights, the law is crucial in molding these changes. Problems with effective regulation arise, however, when dealing with technology due to its inherent volatility, which in turn raises important concerns of jurisdiction, flexibility, and prediction.

A. International Legal Frameworks:

A lot of international agreements and rules are meant to protect human rights as technology changes. Even as new digital tools come out, these laws understand how important it is to protect privacy, freedom of speech, dignity, and equality.

The UDHR, or Universal Declaration of Human Rights, was made official in 1948. Some of the most important rights in the UDHR are privacy (Article 12), freedom of speech (Article 19), and equality (Article 1). Even though it's not legally binding, it sets the tone for future deals that are. Articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR) law protect freedoms that are important to human rights in the digital age. These include the right to privacy. When a country ratifies the ICCPR, it promises to protect these rights, even if there are problems with technology.

The Budapest Convention on Cybercrime is the first worldwide agreement to deal with crimes that happen on the internet, like hacking, content-related crimes, and getting into someone else's data without permission. It sets formal guidelines for countries to work together, but it also makes people worry about privacy and overreach. Guiding Principles on Business and Human Rights from the UN: This framework stresses that companies must protect human rights when making and using technology, which shows how important it is to think about what is right.

The General Data Protection Regulation (GDPR) is a law that applies to the whole of Europe, but it has had an impact on privacy, consent, and user rights around the world. It shows how the law can change how businesses act and give people more power over their data.

B. Domestic Laws and Policies:

Nations develop their own legal frameworks reflecting specific societal values, economic interests, and technological landscapes. Some countries have enacted comprehensive data protection laws, cybersecurity regulations, and digital rights legislation.

United States: No single comprehensive data privacy law exists but rather sector-specific laws such as the California Consumer Privacy Act (CCPA). The U.S. legal approach emphasizes free market principles, with ongoing debates about striking a balance between security and privacy.

For European Union (EU, the GDPR is a landmark regulation providing robust protections for individuals' data privacy, jurisdiction over global companies, and strong enforcement mechanisms. In China, The Cybersecurity Law and subsequent regulations emphasize state control, data localization, and surveillance capabilities, exemplifying a techno-authoritarian approach that raises human rights concerns. In India the proposed Personal Data Protection Bill aims to mirror GDPR standards, emphasizing individual rights and data security but faces implementation challenges.

C. Challenges in Legal Regulation:

Despite the existence of laws and treaties, several obstacles hinder effective regulation in the digital era:

Jurisdictional Difficulties: Cyber activities cross borders effortlessly, complicating enforcement. For example, a data breach in one country can impact users worldwide, creating diplomatic and legal conflicts regarding responsibility.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1618

Speed of Innovation: Laws often lag behind technological developments. For example, biometric and AI-based systems evolve rapidly, and legal mechanisms struggle to keep pace.

Governments encounter challenges such as balancing security and privacy. Enforcing security policies poses difficulties without encroaching upon civil liberties. Discussions over data retention, surveillance initiatives, and encryption illustrate this conflict. Global inequities, such as gaps in technical access and legal safeguards, can result in human rights breaches, exemplified by digital colonialism, wherein dominant nations impose their norms on weaker states. Legislation is occasionally insufficient to resolve the ethical quandaries presented by modern technology, including autonomous weaponry and AI decision-making.

Toward Adaptive and Inclusive Legal Frameworks: To address the difficulties of the digital era, legislation must be adaptable and able to evolve in accordance with emerging technical realities. It must be inclusive: Considering diverse perspectives, particularly those of underprivileged people and developing nations. Additionally, collaborative efforts facilitate international cooperation and the harmonization of standards. Should be Principle-Oriented, Rooted in fundamental rights and ethical values rather than unilateral regulations.

Hence the Law serves as both a safeguard and a regulator in the technological landscape. Its effectiveness depends on the ability to anticipate developments, incorporate human rights considerations, and foster international consensuS.

III. KEY TECHNOLOGIES IMPACTING HUMAN RIGHTS

Technological innovation continues at an astonishing pace, transforming every facet of daily life. While many of these advances offer vast benefits—such as improved communication, healthcare, and economic opportunities—they also pose significant challenges to human rights. Below, we examine some of the most influential technologies impacting fundamental rights and freedoms.

Digital Surveillance and Privacy: Digital surveillance involves the collection, analysis, and use of data to monitor individuals and populations. Governments and corporations deploy surveillance tools for security, marketing, or control, but these practices often threaten privacy, autonomy, and freedom.

Implications for Human Rights: Right to Privacy: Enshrined in Article 12 of the UDHR and protected under various national laws, privacy is fundamental to personal autonomy and freedom. Mass surveillance programs, such as those revealed by Edward Snowden in 2013, exposed the extent of government monitoring, sparking global debates.

Violation of Free Expression, Widespread monitoring discourages dissent, activism, and criticism, undermining democratic participation. Data Exploitation: Corporate data collection, often without explicit consent, enables profiling, targeted advertising, and potentially discriminatory practices. Challenges are like Lack of transparency and accountability, Disproportionate impact on vulnerable groups and use of surveillance for political repression, especially in authoritarian regimes.

Artificial Intelligence and Automation: Artificial Intelligence (AI) encompasses algorithms and systems capable of learning, decision-making, and automating complex tasks. Its integration into policing, hiring, credit scoring, and judicial processes has raised critical human rights concerns.

Deepfake technology, which entails the manipulation or creation of realistic yet fabricated visuals and sounds, presents substantial threats to human rights. It can be exploited for misinformation, defamation, privacy infringements, and political manipulation, adversely affecting individuals' reputation, privacy, and safety. Deepfake technology has significant implications for human rights, including the right to privacy, the right to reputation, and freedom of expression. In 2019, a deepfake video of Nancy Pelosi circulated widely, eliciting apprehensions around misinformation. No formal legal case exists; however, it has prompted regulatory deliberations. Deepfakes connected to Indonesia's elections: Authorities examined deceptive videos intended to sway voters, resulting in demands for more stringent legislation. Indian superstars such as Rashmika Mandanna, Aamir Khan, Ranveer Singh, Sachin Tendulkar, and Virat Kohli have all been targeted by deepfakes. These instances evoke significant apprehensions regarding privacy, manipulation, and reputation. Although India has not established specific case law on deepfakes as a breach of human rights, current legislation on privacy, defamation, and cyber harassment is becoming increasingly pertinent.

Implications for Human Right are like Bias and Discrimination. AI systems trained on biased data perpetuate stereotypes, leading to unfair treatment in employment, law enforcement, and access to services.

Right to Explanation: When AI influences vital decisions—such as bail or parole—the right to understanding and contesting those decisions becomes crucial. Current opaque models challenge accountability.

Job Displacement: Automation threatens economic rights by replacing human labor, exacerbating inequality and marginalization.

➢ *Following are the Challenges:*

- Lack of regulation ensuring fairness, transparency, and non-discrimination.
- Ethical dilemmas around autonomous weapons and lethal decision-making.
- Concentration of power in tech corporations.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1618

Social Media and Freedom of Speech: Social networking channels have democratized communication, facilitating unparalleled involvement and mobilization. However, they also face challenges related to censorship, misinformation, and platform responsibility.

Consequences for human rights include breaches of freedom of expression, content moderation, and the increase of hate speech and misinformation. The issues to be addressed include balancing free expression with public safety, algorithmic prejudice and the amplification of polarizing content, as well as the complexities of jurisdiction and enforcement due to worldwide reach. Biometric technology, including facial recognition, fingerprint scanning, and retinal imaging, are progressively employed for security, identification and access control.

Concerns for Human Rights: Right to Privacy and Data Protection: Biometric data is sensitive and irreversible; its abuse or theft poses threats to persons. Potential for Widespread Surveillance and Repression: Governments utilize facial recognition technology in public areas, occasionally to observe and stifle opposition.

Incorrect identification and Bias: Facial recognition systems frequently demonstrate racial and gender biases, resulting in false positives and possible harassment. Challenges include the absence of comprehensive regulation, the necessity for truth and impartiality, and the ethical use of informed consent.

Internet of Things (IoT) and Smart Devices:IoT refers to networks of interconnected devices—smartphones, wearables, home appliances—that collect and exchange data.

Implications for Human Rights: Privacy and Data Security: Continuous data collection can be intrusive, enabling profiling and behavioral tracking. Excessive surveillance can erode personal autonomy and the right to be left alone. Vulnerabilities in IoT devices create security risks, including potential for hacking and misuse.

Challenges include establishing stringent security requirements, implementing transparent data procedures, and addressing digital disparities about access and management. Technologies include surveillance systems, artificial intelligence, social media, biometric instruments, and the Internet of Things possess transformative capabilities; nevertheless, they also present significant threats to privacy, equality, freedom of expression, and security. Policymakers, technologists, and civil society must collaborate to avoid these dangers by setting norms that respect rights, fostering transparency, and ensuring inclusive access.

IV. HUMAN RIGHTS CHALLENGES IN DIGITAL AGE

The rapid advancement of technology has introduced distinct obstacles in safeguarding and advancing human rights. Although technology provides opportunities for empowerment and accessibility, it also presents threats of exploitation, discrimination, and violations. The report examines significant human rights challenges presented by the digital age.

A. Privacy and Data Protection:

The right to privacy is central to human dignity, autonomy, and freedom. Articles 12 of the UDHR and 17 of the ICCPR affirm this right, emphasizing that individuals should control their personal information and be protected against arbitrary interferences.

Governments and corporations collect massive amounts of personal data, frequently without explicit agreement, raising concerns about misuse and spying. The growing number of hacking instances reveals sensitive personal information, endangering people's safety and privacy. Data-driven profiling can lead to unfair practices in employment, credit, and legal matters. Many governments have weak data protection regulations, making citizens exposed to abuse.

Case Examples like ‘The Cambridge Analytica scandal’ revealed how data harvested from Facebook was used to influence elections and manipulate public opinion. ‘Public debates over government surveillance in the U.S., China, and beyond highlight tensions between security and privacy rights.

B. Freedom of Expression and Speech:

Freedom of expression, as guaranteed by Article 19 of the Universal Declaration of Human Rights, is essential for a functioning democracy since it allows people to express themselves, critique authority, and obtain information. Censorship, content moderation, hate speech and misinformation, and platform liability are all issues that must be addressed. Some of the disagreements occur between journalists and activists in authoritarian nations, where they are frequently subjected to internet repression. Content bans on social media during civil movements, such as those in Myanmar and Iran, show how digital tools are utilized to suppress.

C. The Right to Equality and Non-Discrimination:

Regardless of race, gender, nationality, or socioeconomic status, the digital realm must uphold the principle of equality. Algorithmic bias in AI systems, derived from skewed datasets, perpetuates prejudices and leads in discriminatory outcomes. Restricted access to technology intensifies pre-existing disparities, such as the Digital Divide, marginalizing poor populations and depriving them of possibilities. Online harassment and gender-based violence are pervasive, particularly affecting women and marginalized groups.

Case examples demonstrate that facial recognition systems misidentify individuals of color more frequently than their white counterparts. The absence of internet connectivity in rural or economically disadvantaged regions excludes many from the digital economy.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1618

D. Access to Information and Digital Inclusion:

The Right to Information includes Access to reliable information is crucial for informed decision-making, education, and participation.

Challenges like Censorship and Filtering where Governments may block or restrict access to certain information. Poverty and Infrastructure Gaps like Economic barriers, illiteracy, and geographic remoteness hinder access, deepening social inequalities. Language Barriers like Digital content often favors dominant languages, limiting information access for minority language speakers.

E. Security and Safety:

Protection in the Digital Sphere While technology enhances security, it also introduces new vulnerabilities. Challenges like Cybercrimes, Identity theft, hacking, and fraud threaten individual and institutional security. Cyberwarfare and Digital Conflicts: State-sponsored attacks undermine sovereignty and human security. Digital Repression and Violence: Governments and groups can use digital tools to monitor, intimidate, or harm individuals.

Case Examples like Ransomware attacks on critical infrastructure and State-sponsored hacking campaigns targeting political opponents.

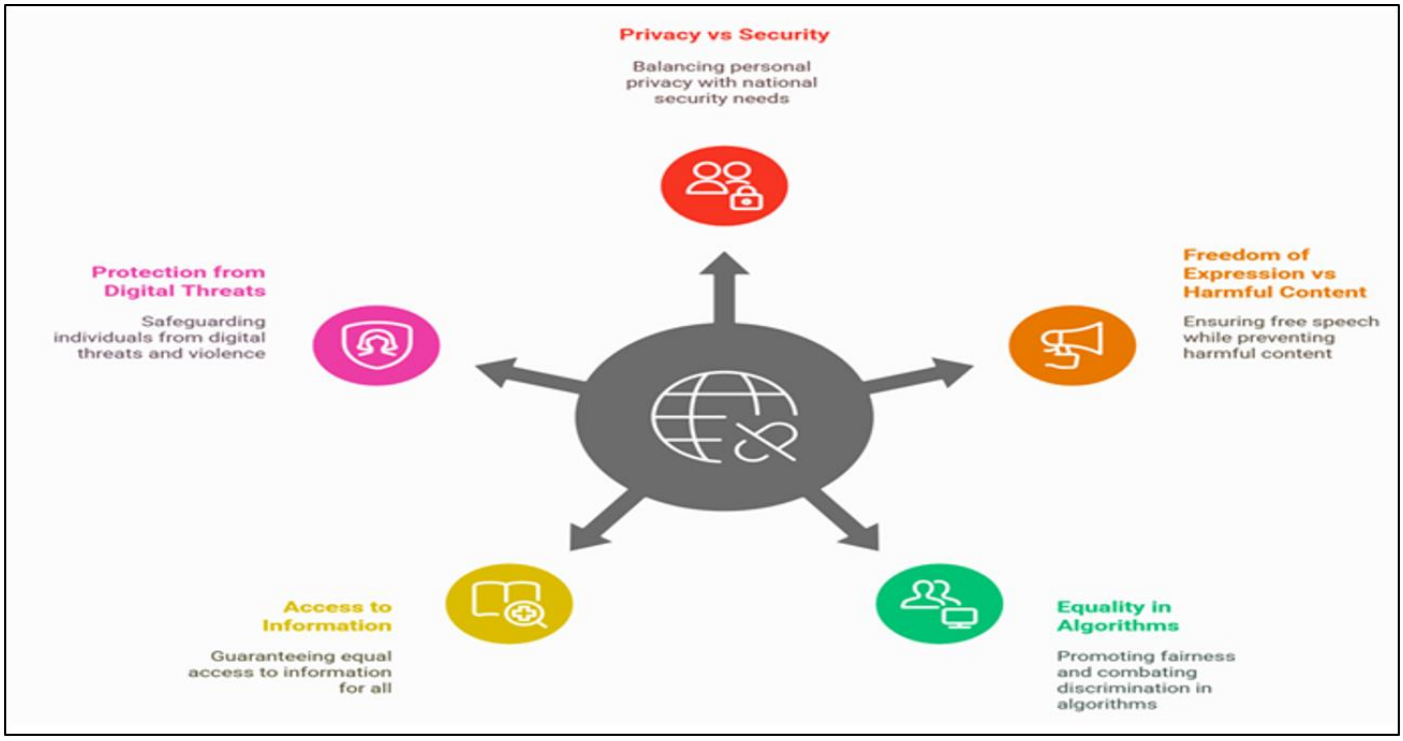

Fig 1 The Digital Age Presents a complex web of Human Rights challenges.

Addressing these challenges requires multilateral cooperation, robust legal protections, ethical development of technologies, and active civic engagement.

V. LEGAL AND ETHICAL FRAMEWORKS

Confronting the human rights issues presented by digital technologies necessitates stringent legal norms and ethical values. These frameworks aim to direct stakeholders—such as governments, corporations, technologists, and civil society—in cultivating an environment where innovation is consistent with human dignity and justice.

A. International Treaties and Instruments:

International law establishes fundamental concepts that support the safeguarding of human rights in the digital realm. Although existing treaties were frequently formulated prior to the digital age, their concepts are progressively interpreted and broadened to address modern concerns.

United Nations Guiding Principles on Business and Human Rights (UNGPs): These establish an expectation that firms must uphold human rights in their activities, including technological advancement. They underscore due diligence, openness, and redress. The Universal Declaration of Human Rights (UDHR) functions as a moral guide, compelling nations and corporations to safeguard privacy, free expression, and equality, including in digital environments.

The European Convention on Human Rights (ECHR), despite its age, has been construed to encompass digital rights, thereby establishing legal benchmarks for privacy and freedom of expression. The Budapest Convention of the Council of Europe: Concentrates on cybercrime, establishing a legal framework for international collaboration and tackling concerns such as hacking and identity theft.

The Global Digital Compact: Proposed by the UN to formulate common principles for digital cooperation, encompassing rights, ethics, and inclusive growth.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1618

B. Regional and National Legislation:

Many nations have established legislation that specifically pertain to digital human rights.

The European Union's General Data Protection Regulation (GDPR) is an extensive legislative framework that mandates data privacy, consent, access rights, and data portability for persons within the EU, possessing extraterritorial applicability. United States of America: A mosaic of regulations (e.g., CCPA, HIPAA) governing certain sectors, such as healthcare and consumer data, yet devoid of overarching federal privacy legislation. Brazil's 'Lei Geral de Proteção de Dados' (LGPD) is analogous to the GDPR, emphasizing data protection and privacy rights. China has instituted stringent data governance, official surveillance, and control measures, frequently at odds with international privacy standards.

C. Emerging Ethical Standards:

In addition to legal requirements, ethical standards are essential, particularly for technology such as AI, whose legislation may still be incomplete.

Responsible AI development is essential for fostering openness, fairness, and accountability in AI systems to uphold human rights. Human-Centric Design: Prioritizing human needs, inclusivity, and dignity in technical innovation. Principles of Non-Maleficence and Justice: Directing developers and policymakers to avert damage and foster equitable advantages. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems establishes standards to direct ethically aligned design and implementation.

D. Challenges in Legal and Ethical Regulation:

Although frameworks are established, numerous challenges hinder their efficacy. Accelerated Technological Advancement: Legislation frequently trails developments, resulting in regulatory voids. Cross-Border Jurisdiction: Digital actions surpass geographical boundaries, complicating enforcement and accountability. Reconciling Rights and Interests: Achieving a balance among privacy, security, innovation, and free expression is intricate. Corporate Accountability: Numerous algorithms and platforms are regulated by corporate rules that do not consistently adhere to human rights standards. Insufficient Enforcement: Even meticulously crafted laws can experience inadequate enforcement or oversight deficiencies.

Advancing a Digital Future that Upholds Rights: To foster a technological environment that promotes human rights, techniques such as Collaborative Multiparty Engagements involving governments, civil society, and corporations are essential. They must collaborate to set unified standards.

Requirement for a legal framework and standards to incorporate human rights in technological design, including the integration of ethical issues from the outset. International Governance Frameworks: International organizations ought to promote collaboration, establish standards, and resolve disputes. Accountability and Remedies: Comprehensive processes must be established for victims of rights abuses, facilitating remedies and sanctions.

VI. CITIZENS DUTIES AND RESPONSIBILITIES

- People also have important duties and obligations when it comes to protecting human rights and public safety from technological risks. Here is a summary of Citizens' Duties:
- Stay Informed: They should learn how innovations affect their rights, privacy, and safety. Stay up to date on the latest laws, rules, and best practices for digital rights and safety.
- Get digitally literate: learn how to use technology in a safe and smart way. Learn how to spot false information, scams, and other bad things that are happening.
- Respect the rights of others: Behave morally when using technology by keeping others' privacy, not bothering them, and not cyberbullying or sharing hate speech.
- Take part in democratic processes: make policy, talk about issues in public, and speak out to change the rules that guide how technology is used. Help projects that fight for digital rights and equal access.
- Report Threats and Violations: Tell the right people or sites about cybercrime, harassment, false information, or security holes. Notify the right people about bad uses of technology that could hurt people or groups.
- Keep personal information safe: use strong passwords, turn on two-factor authentication, and be careful about giving out private information online.
- Make the case for ethical technology use: back groups and rules that encourage the safe creation and use of technology that respects human rights.

- *Liabilities of Citizens:*

- Legal Duty: Do not do anything illegal, like hacking, accessing data without permission, or spreading harmful material. Follow any age limits and material rules that the law or the platform's rules set.
- Being Responsible for Misinformation: You should be responsible for the truth of the information you share and not spread harmful false or misleading information.
- Ethical Use of Technology: Be aware of how your digital activities might affect the rights and safety of others. Do not take part in activities that could hurt human rights, like abuse, harassment, or breaking people's privacy.
- Community Support: Help make the internet a safe and polite place by helping people who have been victims of hacking and false information.

One well-known example is Germany, which makes its people follow certain rules when they use digital technology to protect human rights and keep the system safe.

Germany's NetzDG (Network Enforcement Act) says that social media sites must quickly remove any illegal content. This law mostly targets platform owners, but it also encourages responsible behavior among citizens by telling them to watch out for and report illegal online content.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1618

The German 'Bundesdatenschutzgesetz' (BDSG) is a Federal Data Protection Act and following the General Data Protection Regulation (GDPR) stress that each person is responsible for protecting their own data. This means that people have a duty to keep their personal information safe.

People are encouraged to report material that is harmful or illegal to authorities or platforms, like cyberbullying, hate speech, or false information. Digital literacy campaigns run by the government teach people how to behave responsibly online. People are responsible for following data privacy rules, like making sure they use strong passwords and are careful about sharing personal information.

The NetzDG law says that people can be sued if they intentionally share illegal content like hate speech or slander, especially if they don't report or delete the content after knowing about it.

VII. CONCLUSION

One of the most important challenges for the Twenty First -21st century is how to balance law, science, and human rights. Technological progress has a lot of good effects on health, education, and economic growth, but it also has a lot of bad effects on privacy, freedom, equality, and safety. Guaranteeing that forthcoming technological advancements respect human rights necessitates a proactive, interdisciplinary strategy encompassing law, ethics, technology, and civil society. The objective should be to establish an inclusive, equitable, and rights-respecting digital ecosystem.

Although governments and organizations bear considerable duties, citizens also significantly contribute to alleviating technological risks. Their responsibilities encompass remaining aware, exercising responsible usage, honoring rights, and engaging actively in social initiatives to promote a secure and equitable digital landscape. Individuals are accountable for unlawful or immoral conduct online, and their activities can profoundly impact the technological landscape's adherence to human rights and security.The legal system in Germany shows how a country can make its people responsible for using technology in an honest and legal way. People are expected to help keep the internet safe, report violations, and protect privacy. By doing these things, they help achieve the larger goal of protecting human rights in online.

To deal with these problems, we need flexible law systems, high moral standards, global cooperation, and active participation in government to achieve Sustainable Development Goals (SDGs). The decisions we make today will determine whether the digital world is a place where people are empowered or a place where people are abused. In the end, to get the most out of technology while protecting everyone's basic rights, we need a rights-based approach built openness, responsibility, acceptance, and respect for human dignity.

REFERENCES

[1]. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Off J Eur Union. 2016;L119:1-88

[2]. United Nations Human Rights Office of the High Commissioner. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. 2011.

[3]. Singh R. Blockchain technology and its implications for Indian legal system. J Indian Law. 2021;9(3):78-90.

[4]. Verma P. Challenges to implementing data protection laws in India. Int J Cyber Law. 2020;14(1):45-59.

[5]. Das G. The impact of the Information Technology Act, 2000 on privacy rights in India. Law J India. 2018;18(2):210-225.

[6]. Pillai K, Menon R. Biometric systems and privacy concerns in India. India J Info Sec. 2019;5(3):78-85.

[7]. Sharma S. Regulation of social media in India: A human rights perspective. Sci Tech Soc. 2022;27(1):45-63.

[8]. Kuner C, Bygrave LA, Docksey C, editors. The GDPR: A Commentary. Oxford: Oxford University Press; 2017.

[9]. Shannon C, Weaver W. The Mathematical Theory of Communication. Urbana: University of Illinois Press; 1949.

[10]. Schneier B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton & Company; 2015.

[11]. Gagliardi F. Blockchain technology and human rights: An analysis of challenges and opportunities. J Digital Law Policy. 2019;4(2):45–67.

[12]. Gagliardi F. Blockchain technology and human rights: An analysis of challenges and opportunities. J Digital Law Policy. 2019;4(2):45–67.

[13]. Mann S, Ferenbok J. New media and the paparazzi: The politics of digital surveillance. Media Cult Soc. 2013;35(1):37–54.

[14]. Bryson JJ. Artificial Intelligence and Human Rights. In: The Oxford Handbook of Ethics of Artificial Intelligence. Oxford: Oxford University Press; 2018.

[15]. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs; 2019.

[16]. Kumar P. Data privacy and protection law in India: Challenges and opportunities. Int J Law Management. 2020;62(3):233-248.

[17]. Sinha A. Digital surveillance and privacy rights in India. Indian J Law. 2021;12(4):145-160.

[18]. Reddy M. Artificial intelligence and human rights: An Indian perspective. J Tech Law Policy. 2019;24(2):101-118.

[19]. Council of Europe. European Convention on Human Rights. 1950. Available from: https://www.echr.coe.int/documents/convention_eng.pdf