NAVIGATING HUMAN RIGHTS IN THE AGE OF TECHNOLOGY

Zaree Shahnaz*

INTRODUCTION

The digital age has brought phenomenal changes to the understanding, protection, and challenging of human rights. As societies and their economies increasingly rely on the use of digital technologies, some fundamental rights like privacy and freedom of expression have become pillars for both unmeasured promotion and unmeasured threat to citizens. The interaction displayed through artificial intelligence, big data, and digital surveillance is changing the interaction among an individual, corporations, and government, raising the ethical and legal influence on the shielding of civil liberties in cyberspace.

Privilege status: This is one of the most widely discussed social issues in this age of digital technologies. The issue of privacy becomes a major source of concern when governments and other private organizations engage in mass surveillance, data breaches, and abuse of personal data. The setting up of powerful data protection acts, such as the General Data Protection Regulation within the EU, further emphasizes that there should exist a minimum law that would provide protection to a person from the exploitation of persons in the world of digital information. Digital freedom of speech articulates itself differently today. Social media platforms have created political discourses, activism, and dissent; however, the growing tide of false information, censorship online, and algorithmic biases led to debate over the need to regulate free speech to prevent undermining democratic values. The moderating influence of technological companies and the growing influence of AI in public narratives add complexity to the world of digital rights. Another very critical aspect of human rights in the digital world is equitable access to technology. "The digital divide most poignantly affects marginalized communities; this division remains an assault on opportunities for education, economics, and civic engagement." Thus, any initiatives such as widening the scope of internet infrastructure

*BBA LLB, SECOND YEAR, MODEL INSTITUTE OF ENGINEERING AND TECHNOLOGY(MIET) JAMMU.

and improving digital literacy are still key to inspiring technology to be an enabler, not a barrier, to human rights.

Equitable access to technology is one of the other vital aspects of human rights in the digital age. The digital divide most heavily affects marginalized communities; this division remains an assault on opportunities for education, economics, and civic engagement. Hence, any initiatives such as widening the scope of internet infrastructure and improving digital literacy are still key to inspiring technology to be an enabler, not a barrier, to human rights.

Privacy Rights and Data Protection in the Digital Age

A. Privacy pursuant to Applicable Laws

The right to privacy is said to be among the most important human rights which are endowed protection by both international and some national laws. The Universal Declaration of Human Rights contemplates the right to protection from arbitrary interference with privacy, family, home, or correspondence in Article 12. Likewise, the International Covenant on Civil and Political Rights conceptually seeks to protect the individual from arbitrary interference within his or her private life through Article 17. Such protections were framed on the premise of the idea of privacy in the physical, yet now the digital age has broadened this to incorporate one involving digital data and information.

The legal frameworks often lag behind when it comes to technological advancement. Personal data can be captured without consent through the digital footprints generated. With this, privacy in data issues is significant in many countries with laws that include the General Data Protection Regulation implemented in the European Union. Overall, legal standards for data protection and privacy still vary across jurisdictional lines.

GDPR: A LEGAL FRAMEWORK FOR DATA PRIVACY ADDRESSANCE

The GDPR (2018) is a landmark legislation designed to address data privacy issues in our digital world. This policy brings forth three basic principles: transparency, accountability, and consent. These principles require businesses to inform individuals about their data collection practices and to obtain explicit consent before processing personal information. In addition, the right to be forgotten and data portability provisions empower individuals over their own data.

However, the scope of the GDPR is mainly limited to the European Union, although extraterritorial provisions do affect companies outside the EU if they process data related to EU citizens. This situation poses substantial enforcement issues when data is transferred to jurisdictions that have weaker data protection laws (such as the United States). In 2020, the European Court of Justice's Schrems II decision declared the EU-U.S. Privacy Shield refers to the limited protection of the data of EU citizens under US regulations. The ruling speaks to the challenges of generalization of data protection standards because the landscape is in constant flux.

Legal Analysis:

Despite the solidity of the base upon which data protection stands, the extraterritorial limits have capped the effectiveness of the GDPR at an international level. Moreover, provisions never dealt adequately with issues connected to government surveillance and corporate appropriation of personal information. Legal analysts say that such laws need to be much broader and involve much larger constituencies, such as international organizations and tech behemoths, if an international consensus on digital privacy is to be arrived at.

FREEDOM OF EXPRESSION IN THE DIGITAL ERA

A. The Role of the Internet in Promoting Free Speech

The internet has become a very important tool whereby the freedom of expression, guaranteed under Article 19 of the UDHR and ICCPR, which pertains to the right of seeking, receiving, as well as imparting any information and ideas through any media and any other media, is exercised. This is exactly where the democratization of communication happens. Here is where the internet allows persons to express themselves, seek facts, and partake in global discourse.

The right to free speech is a precious freedom; it is, however, not without limits.

It is not always possible for every country to protect online content to prevent hate speech, terrorism, and cyberbullying. As such, it becomes quite difficult to deal with this complex legal challenge: this conflict between protecting individuals from such harmful content and protecting the right to free speech. The use of online hate speech and misinformation

campaigns has driven the widespread call for increased regulations of digital media, especially companies operating on social media.

B. Legal Challenges in Content Regulation

Sites like Facebook, Twitter, and YouTube are frequently criticized for taking down content they believe is harmful to society. Legal standards surrounding internet content are divergent and vastly different depending on the jurisdiction. In the United States, the Communications Decency Act (CDA) Section 230 provides a defence against holding the provider liable for the user-generated material, yet continues to make it challenging to hold the platform responsible for the harmful content it hosts.

In contrast, the European Union's Digital Services Act (DSA) and the Digital Markets Act (DMA) try to bring online platforms closer to regulation in a more frontal manner, being stricter on matters of content moderation, transparency, and accountability. These laws hope to balance freedom of expression as a right while holding the obligation of platforms over preventing harm.

Legal Analysis

Freedom of speech is a natural right, and the legal concerns in regulating digital content are multifaceted: Proportionality is a key legal principle in content regulation, ensuring that any restriction on speech does not exceed what is necessary to protect other rights. The application of international human rights law to digital platforms remains a complex issue, as tech companies operate globally, and local laws often conflict with international norms. Freedom of expression and control over content content should be correctly balanced through additional harmonization between the laws within the digital atmosphere.

DIGITAL MONITORING AND HUMAN RIGHTS

A. Expansion of the scope of monitoring

Surveys and data recovery are utilizing advanced technologies, with government agencies increasingly using mass surveillance tools in the fight against terrorism, cybercrime, and social unrest. Facial recognition, geolocation tracking, and internet monitoring have been the major areas of concern as they can breed privacy invasion and possible human rights violations.

Governments consider it necessary for national security; however, adequate oversight or transparency does not exist.

B. Legal Framework of Surveillance

Legislation on surveillance powers, carried in powers narrow and broad, is on most crimes in mosting have sworn such as Walczuch. These executive utterances have introduced questioning of proper course and redress thereof under the various heads under international and domestic jurisdictions has undoubtedly polarized public opinion. For instance, in the USA, the USA Patriot Act and Foreign Intelligence Surveillance Act grant the executive powers to conduct warrantless surveillance under various circumstances. In the UK, the Investigatory Powers Act permits mass surveillance and data collection by intelligence agencies. Even if some of these laws are justified under arguments of national security, the overreach of these laws raises debate as to whether mass surveillance is permissible, and if there is a proper targeting of particular groups in question-for instance, activists, journalists, or minorities.

Legal Issues:

Most contentious issues surrounding digital surveillance relate to proportionality and necessity; the surveillance measures ought to be necessary and the least intrusive means of achieving the same goals. International human rights law, especially the ICCPR, requires that any interference with privacy should be lawful, necessary, and proportionate. The ECHR has ruled in cases like Szabo v. Hungary (2016) that clear legal safeguards are needed to avoid overreach in surveillance activities.

The increasing deployment of digital surveillance technologies, not least by illiberal regimes, threatens to engulf individual rights. Legal solutions must be designed that provide sufficient safeguards against arbitrary interference with privacy and that offer redress for its violation of human lives.

ACCESS TO INFORMATION AND DIGITAL INCLUSION

A. Legal Right to Get Information

Getting information is a basic human right that allows people to join in democratic processes and use other rights, like schooling and jobs. The UN Declaration on Human Rights sees getting information as part of the right to join in cultural life and public matters. But, the gap

between those who have digital access and those who don't is still one of the This right faces big roadblocks in less developed countries where internet access is scarce.

B. Legal Instruments for Digital Inclusion

The International Covenant on Economic, Social, and Cultural Rights emphasizes the equal right to access information and education that has become highly dependent on digital technology. With this, various countries and international organizations have started developing programs of digital inclusion where disadvantaged communities will be assured internet and digital technology access.

Legal Analysis:

National and international laws should guarantee that money doesn't stop people from getting information. Making sure everyone knows how to use computers and can afford the internet needs to be a top priority to bridge the gap between those who have digital access and those who don't. Countries that have signed the ICESCR need to have legal systems that help people get information from those who are at a disadvantage. If there's no solid legal backing to include everyone in the digital world, a big chunk of society won't get chances in school, healthcare, and jobs.

CONCLUSION

The legal landscape around human rights in the digital era is complex and in constant evolution. International human rights frameworks, such as the UDHR and ICCPR, form a foundational base for the protection of fundamental rights, but these must be adapted to deal with the special challenges posed by digital technologies. Such critical issues as privacy, freedom of expression, surveillance, and information access require an approach that takes into account balancing individual rights while providing for governments' and companies' legitimate interests. Global cooperation, comprehensive legislation, and strong enforcement mechanisms should be the hallmarks of such a protection effort for human rights in the information age.

REFERENCES

1. Universal Declaration of Human Rights (UDHR), Article 12.

2. International Covenant on Civil and Political Rights (ICCPR), Article 17.

3. United Nations, "Guidelines for the Regulation of Computerized Data Files," UN Doc. A/RES/45/95 (1990)

4. European Union, "General Data Protection Regulation," (EU) 2016/679.