

**LAWFOYER INTERNATIONAL**  
**JOURNAL OF DOCTRINAL LEGAL**  
**RESEARCH**  
**(ISSN: 2583-7753)**

---

---

Volume 2 | Issue 1

---

---

2024

© 2024 *LawFoyer International Journal of Doctrinal Legal Research*

Follow this and additional research works at: [www.lijdlr.com](http://www.lijdlr.com)  
Under the Platform of LawFoyer – [www.lawfoyer.in](http://www.lawfoyer.in)

---

---

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of **any suggestions or complaints**, kindly contact [info.lijdlr@gmail.com](mailto:info.lijdlr@gmail.com)

---

**To submit your Manuscript** for Publication in the **LawFoyer International Journal of Doctrinal Legal Research**, To submit your Manuscript [Click here](#)

---

# PRIVACY UNPLUGGED: BALANCING TECHNOLOGY AND HUMAN RIGHTS

---

Ekshitha Gutta<sup>1</sup>

## I. INTRODUCTION

The fine line between fundamental human rights and technological breakthroughs has become increasingly important in an increasingly linked society. The convergence of fundamental human rights and technological advancement has become a crucial focus point in today's digitally driven society. As we navigate the enormous terrain of the digital world, protecting privacy is crucial to maximizing the advantages of technology. This blog sets out to explore the complex relationship between technology and human rights, analyzing the obstacles and possible solutions for finding a careful balance between the two.

### A. WHAT IS TECHNOLOGY?

In today's world, technology is the result of the dynamic interaction of scientific understanding, useful instruments, and creative processes. It includes a wide range of innovations that impact our day-to-day activities, from the tangible devices we use to the intangible algorithms controlling our online interactions. Every aspect of our lives is impacted by technology, whether it is the smartphone we carry around in our pockets, the artificial intelligence that analyses data, or the infrastructure that facilitates international communication.

Fundamentally, technology stands for advancement—the never-ending search for answers to problems, big or little. It gives us the ability to accomplish previously unthinkable things, but it also presents moral conundrums. We must balance this dual responsibility as we examine the complex link between technology and human rights preserving individual liberty while maximizing its advantages. Some of the Key Aspects

---

<sup>1</sup> BA LLB Hons. 2nd year 4th semester.

of Technology are Innovation, Tools & Machines, Automation, Information and Communication, and Data Processing.

For Example, technological innovation propels development and provides answers to societal problems. But if innovation isn't sufficiently controlled, it may also be dangerous for people's right to privacy. Establishing strong frameworks that promote advancement while preserving individual liberties is necessary to strike a balance between privacy issues and innovation. Also, the availability, sharing, and communication of information has been completely transformed by the digital age. Technology makes it easier to connect people around the world and share ideas, but it also raises concerns about data security and privacy. Robust data protection protocols and communication platform openness are necessary to strike a balance between the right to privacy and the free flow of information.

## **B. What are Human Rights?**

Human rights are essential privileges that every person has only by existing. All people are entitled to these rights, which are unalienable and universal, irrespective of their race, nationality, religion, or any other attribute. Achieving a balance between protecting individual rights and technical progress becomes crucial in the context of technology and privacy.

- 1. Right to Privacy:** A fundamental component of human rights is the right to privacy. It includes the freedom of an individual to control their private life, communications, and personal information. This right confronts hitherto unheard-of difficulties in the digital age because of the widespread use of technology. It's critical to strike a balance between the advantages of technical progress and the requirement to preserve privacy. For Example, the General Data Protection Regulation (GDPR) of the European Union sets tight requirements for how businesses and organizations doing business inside the EU should handle personal data. The GDPR regulates the

gathering, storing, and use of personal data to uphold people's rights to privacy in the digital era.

- 2. Freedom of Expression:** One of the fundamental rights of individuals is the ability to freely express one's thoughts, ideas, and knowledge as well as to take part in public conversation. Global communication has made this right even more possible thanks to technology. To strike a balance, though, requires tackling problems that might restrict this freedom, such as hate speech and disinformation on the internet and spying. The UN's attempts to counteract online censorship and advance internet freedom, such as the UN Special Rapporteur on the promotion and protection of the right to freedom of thought and expression, are a practical illustration of this right in action. These campaigns aim to protect people's freedom of expression online from censorship or fear of retaliation.
- 3. Right to Data Protection:** People have the right to decide how their information is used, especially when technology gathers enormous volumes of personal data. By promoting data-driven innovations while protecting privacy, data protection laws and regulations seek to achieve a balance. To achieve this balance, transparency, consent, and accountability are essential. The historic Schrems II case serves as a noteworthy illustration of the legal system in action. In this case, the Court of Justice of the European Union invalidated the EU-US Privacy Shield agreement because it did not adequately safeguard EU individuals' data from US government monitoring.
- 4. Right to Access Information:** People now have never-before-seen access to information thanks to technology, which enables them to study, participate, and make wise decisions. However, equitable access may be hampered by the digital divide. Technology balancing entails closing this gap and making sure that everyone takes use of the possibilities and information

that the digital world has to offer. Through open data efforts and transparency measures, governments may increase public access to information by participating in the Open Government Partnership (OGP), an international project. The OGP seeks to enable people to hold their governments responsible and take part in decision-making processes by encouraging open access to government data and information.

5. **Right to Anonymity:** The freedom to express oneself without worrying about retaliation is facilitated by anonymity. Technology balancing is protecting anonymity while addressing issues with cyberbullying, online abuse, and illegal activity made possible by anonymity. The process of protecting communications from monitoring and interception by using encryption technologies. The conflict between ensuring security and upholding people's right to privacy and anonymity is brought to light by the continuous discussion over encryption policy, particularly about law enforcement's access to encrypted material.
6. **Right to Security:** People are entitled to both physical and digital security. Through cybersecurity, monitoring, and encryption, technology improves security. Finding a balance between maintaining public safety and avoiding overzealous surveillance that violates people's right to privacy is necessary, nevertheless. The Budapest Convention on Cybercrime is one worldwide attempt to tackle cybersecurity risks. Its goals are to improve international collaboration in combatting cybercrime and harmonize national legislation.
7. **The Right to Be Free from Discrimination:** Technology must not support prejudice against people based on their gender, race, religion, or any other attribute. Promoting inclusion, preventing prejudice in algorithms, and guaranteeing equitable opportunity for all are all part of balancing technology. Discrimination on the basis of gender, race, disability, and other grounds is prohibited by international human rights instruments like

the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) and the Convention on the Rights of Persons with Disabilities (CRPD).

## **II. HISTORICAL ASPECT**

From early inventions to contemporary technologies, privacy concerns and technological advancements have always coincided. For instance, the telegraph made instantaneous long-distance communication possible but also gave rise to concerns regarding the confidentiality of messages sent. Similar privacy concerns were brought about by the telephone due to wiretapping and eavesdropping. Considerable advancements in technology for surveillance, particularly in the course of World War II, spurred discussions about how to reconcile security and privacy. The 1970s saw the rise in awareness of data privacy due to personal computers and databases, which in turn changed the dynamics of privacy. In the 1980s, encryption technologies became available to people, allowing them to safeguard their digital correspondence.

Public internet access in the 1990s contributed to an increase in privacy concerns as a result of the boom in online activity. The distinction between private and public information became more hazy in the 2000s with the proliferation of social networking sites and mobile devices. The privacy problems raised by contemporary technology such as biometrics, artificial intelligence, and security cameras make it difficult to strike a balance between technical growth and individual rights.

In a similar vein, human rights history is extensive and varied. The path towards acknowledging fundamental human rights has been a long and complex one, spanning from the Middle Ages' Magna Carta, which guaranteed protections against arbitrary arrest, to Enlightenment philosophers like Voltaire and John Locke, who promoted individual rights. Following World War II, the United Nations adopted the Universal Declaration of Human Rights in 1948, which affirmed the significance of fundamental rights for every person, including the right to privacy as stated in Article 12. Additionally,

privacy rights are expressly guaranteed in Articles 8 and 17 of the International Covenant on Civil and Political Rights and the European Convention on Human Rights, respectively. These significant events highlight the continued international effort to protect individual rights in the face of changing social norms and technological advancements.

### **III. ADVANCEMENTS IN TECHNOLOGY**

In our globalized society, technology profoundly shapes our daily lives, revolutionizing how we connect, communicate, and work. From smartphones to smart cities, innovations abound, ushering in unprecedented efficiency and convenience. However, this rapid progress raises a pressing question: how do we safeguard privacy while upholding human rights in the digital age? The dilemma inherent in technological advancement becomes apparent as personal information is continuously collected, analyzed, and exploited. Tools for surveillance, employed by both businesses and governments for law enforcement and national security purposes, introduce a conflict between innovation and privacy. While technologies like location monitoring, biometrics, and facial recognition are invaluable, their indiscriminate use risks infringing on individuals' right to privacy.

Policies such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) underscore the importance of responsibility, transparency, and user consent in data handling. These regulations strive to strike a balance between protecting individual rights and fostering technological innovation. Messaging apps like Signal and WhatsApp utilize end-to-end encryption to safeguard conversations, limiting access to intended recipients and enhancing privacy. Similarly, the Tor network facilitates anonymous browsing by routing internet traffic through multiple servers, shielding users' identities from surveillance.

Blockchain technology offers decentralized, immutable data storage, empowering users with control over their personal information and potentially revolutionizing identity

management. Projects like Solid envision a decentralized web, where users retain ownership of the data they share with applications and services.

While fingerprint and facial recognition technologies streamline device access and transactions, concerns persist regarding their potential for abuse and privacy violations. Ensuring fairness and transparency in AI systems is essential to shield individuals from bias and uphold human rights. Engineers and designers must prioritize privacy considerations from the outset, integrating privacy protections into default settings to empower consumers to make informed decisions. Education about privacy risks and best practices empowers users to demand technology that respects their privacy rights, ensuring a more equitable and rights-respecting technological landscape.

#### **IV. HINDRANCE TO HUMAN RIGHTS**

While there is no denying that technological improvements have made many areas of our life easier, they also present serious threats to human rights. Here are three key areas, along with relevant instances and reliable sources, where technology affects human rights.

- 1. Privacy and Surveillance:** Serious questions concerning the right to privacy have been highlighted by the widespread use of surveillance technology. For example, the United Nations report on privacy in the digital age emphasizes how contemporary networked digital technologies are posing increasing risks to human rights and privacy. These technologies, like the controversial "Pegasus" software, may turn cell phones into constant monitoring tools that allow hackers to obtain personal information and use it as a weapon to spy on people's lives. These instruments have been employed for unlawful purposes, such as suppressing journalists, human rights advocates, and opposing viewpoints.
- 2. Artificial Intelligence (AI) Bias and Discrimination:** AI systems have the potential to reinforce preexisting prejudices, which might result in discrimination in important domains including lending, employment, and criminal justice.



Examples from the real world include AI systems in the medical field that have given African-American patients less accurate findings than White ones. In a similar vein, AI-powered resume screening programs have the potential to unfairly exclude applicants from underrepresented groups, exacerbating already-existing social inequalities.

- 3. Digital Divide and Technology Access:** With large segments of the population without access to technology, the digital divide continues to be a barrier to equality. Data highlights the huge disparity in digital access, with around 3.6 billion people still living without internet access<sup>5</sup>. Low-income countries (LICs) are disadvantaged in terms of cost, speed, and performance due to the greater lack of contemporary data infrastructure in these countries.

## V. NATIONAL POLICIES

### 1. Right to Privacy

National constitutions or legal frameworks should expressly recognize the right to privacy as a basic human right. With this acknowledgment, people are guaranteed legal protection from unauthorized access to their private life. It should be illegal for governments and other organizations to conduct widespread monitoring without a valid reason. It is crucial to strike a balance between the demands of individual privacy rights and national security. To stop arbitrary surveillance, there should be legal protections in place, including warrants.

### 2. Transparency and Accountability

Companies that gather personal information are required to be open and honest about their data policies. Users should be informed about data collection, processing, and storage through their succinct and unambiguous privacy policies. Organizations should be held responsible for data breaches. It is vital to have reporting guidelines and sanctions for improper handling of personal data. Trust between users and data controllers is strengthened by transparency.

### **3. Biometric Data Regulation**

The usage of biometric information such as DNA, fingerprints, and face recognition – for identification and verification is growing. Policies ought to balance the needs of individual privacy protection with those of technical innovation. Biometric data should be collected, stored, and used following regulations. Before having their biometric information gathered, people must give their informed consent. Countries should explicit policies regarding the usage and security of this data.

### **4. Cross-border data flows**

Maintaining uniform privacy rules is critical when data moves across national borders. Cross-border data transfers should be covered by national policies. Sufficient security measures have to be implemented to preserve private data even during its transit outside the nation.

### **5. Ethical use of AI and Surveillance Technologies**

The ethical ramifications of surveillance technology and artificial intelligence (AI) should be addressed by policy. It is difficult yet vital to strike a balance between the demands for privacy protection and security. Privacy rights should be protected when surveillance technologies, such as CCTV cameras, are used, according to policies. It's crucial to have explicit policies on data access, retention, and supervision.

### **6. Collaboration with International Bodies**

Participating in international organizations enables nations to work together on global privacy standards. A strong privacy framework may be established by exchanging best practices and learning from one another. Involvement in privacy standards debates helps to guarantee that national regulations follow international trends.

## **VI. INTERNATIONAL LAW**

### **1. UN Report on Spyware and Surveillance**

The United Nations (UN) has drawn attention to the risks that contemporary networked digital technologies pose to human rights and privacy. These technologies may be oppressive even if they are effective instruments for monitoring and controlling people. The necessity of effective regulation founded on international human rights legislation and norms is emphasized in the study. It concentrates on three important areas: State agencies frequently misuse spyware programs, and convert cell phones into round-the-clock monitoring apparatuses. To stop spyware from spreading, immediate action is required.

This includes calling for a ban on using and selling spyware until sufficient security measures are in place. Strong encryption techniques are essential for safeguarding online human rights. States should refrain from utilizing techniques like backdoors or routine device scanning to erode encryption. Extensive monitoring is made possible by digital identification systems, biometric databases, and large-scale automated data collecting and processing. Governments are required to prevent the misuse of surveillance instruments and to notify the public about surveillance operations.

## **2. OHCHR Reports on AI and Privacy**

One of the most important organizations in the UN system, the Office of the High Commissioner for Human Rights (OHCHR) is tasked with advancing and defending human rights around the world. It is significant when considering human rights and international law. The wide-ranging effects of artificial intelligence (AI) on privacy and related rights have been investigated by the UN Human Rights Office (OHCHR). The papers emphasize how urgently sufficient protections must be put in place before AI technologies that pose major dangers to human rights may be sold or used. AI programs that violate international human rights legislation ought to be prohibited.

## **VII. CONCLUSION**

In conclusion, it is becoming more and more important to protect human rights in the context of technological innovation as we negotiate the intricacies of our digitally linked

society. We need to stand out for privacy and make sure that it is included into technology advancements rather than being treated as an afterthought. Strong ethical foundations, strict accountability procedures, and unflinching openness are required to pave the way forward. Among the Principal Suggestions are Tighten up privacy regulations to counteract the intrusive aspects of surveillance technology. In order to reduce algorithmic prejudice and advance impartial AI systems, include a variety of datasets and viewpoints. By giving everyone in society fair access to technology, we can close the digital divide. Together, let's work to build a future in which technology is a source of empowerment rather than an instrument of oppression. A future in which privacy is essential to the advancement of technology and where each person's rights are respected and safeguarded. By working together, we can direct innovation in the direction of a future that upholds and expands upon our fundamental rights. Let this be our steadfast dedication and our common vision.

## VIII. REFERENCES

1. How are today's biggest tech trends affecting our human rights?, *available at:* <https://www.weforum.org/agenda/2017/12/how-are-today-s-biggest-tech-trends-affecting-human-rights/> (Last Visited on April 14, 2024).
2. Technological Advancements affect the future of Human rights, *available at:* <https://www.hks.harvard.edu/centers/carr/programs/technology-human-rights> (Last Visited on April 14, 2024).
3. The Promise and Peril of Human Rights Technology, *available at:* [https://www.cambridge.org/core/services/aop-cambridge-core/content/view/17A00746377B91341F684D4F28D48221/9781107179639c1\\_120.pdf/the-promise-and-peril-of-human-rights-technology.pdf](https://www.cambridge.org/core/services/aop-cambridge-core/content/view/17A00746377B91341F684D4F28D48221/9781107179639c1_120.pdf/the-promise-and-peril-of-human-rights-technology.pdf) (Last Visited on April 14, 2024).
4. Technology and Human Rights, *available at:* <https://www.openglobalrights.org/technology/> (Last Visited on April 14, 2024).
5. Introduction to International Human Rights Law, *available at:* <https://humanrightsconnected.org/international-human-rights-law/> (Last Visited on April 14, 2024).

6. A Brief Primer on International Law and Cyber Space, *available at:* <https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763> (Last Visited on April 14, 2024).
7. International Law Handbook, *available at:* [https://legal.un.org/avl/studymaterials/handbook/english/book\\_1.pdf](https://legal.un.org/avl/studymaterials/handbook/english/book_1.pdf) (Last Visited on April 14, 2024).
8. Universal Declaration of Human Rights, *available at:* <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (Last Visited on April 14, 2024).
9. International Bill of Human Rights, *available at:* <https://www.ohchr.org/en/what-are-human-rights/international-bill-human-rights> (Last Visited on April 14, 2024).
10. Human Rights, *available at:* <https://www.britannica.com/topic/human-rights> (Last Visited on April 14, 2024).