Delhi Metropolitan Education
Affiliated to GGSIP University, New Delhi & Approved by Bar Council of India

RESEARCH ARTICLE TYPE
doi: 10.53361/dmejc.v6i02.02

Navigating Digital Rights in the Recent Era: Promoting the Freedom and Safety

G Sanjay Guru, Dhivyabharathi K

Student, Bharath Institute of Law, Selaiyur, Chennai-600073

Abstract

The paper establishes a practical view against privacy that violates human rights. The disputes that arise due to trouble are faced in the technology that is used by the recent generation. Digital rights are closely linked to the use and publication in digital media, freedom of speech and expression, right to privacy, even the right to access the computer and other electronics and communication networks. Most of the technologies that are beneficial to use such expansive knowledge in the digital mode. Why are digital technologies that harmful to every individual? Because the people are unaware of problems faced by them while sharing their details. It is the broader way to calculate the significance by using digital technology. Digital rights are very useful by implementing many talents to the world. More ways restrict the rights of an individual to showcase their skills in the pandemic world. There are infinity methods that restrict digital rights such as copyrights, data privacy, basic human rights, etc. Violation of another kind of right is not that reckless, but violating the rights of individual privacy digitally is in the place of insecurity. More disadvantages that affect the advantages of using the source, like mobile phones, computers, palm tops, etc. The wrong way of using their data may create a bad impression of the technology development. If people get fear of using resources like private data to log in to some source, then how is digital mode utilized properly? The laws that protect against this confusion are implemented in the Information Technology Act, cybercrime, cybersecurity agencies, etc., that is, to help individuals while their data is in an unsafe position. We, the users of technology, should be aware of overusing our details in common ways. Should not normalize the things of sharing their data on all kinds of unauthorized websites or links that provide on mobile phones. Nowadays, people are knowingly and unknowingly using their private data to be ejected without their consent. Why is privacy stolen repeatedly? Even laws are being set up to secure the people from scamming and hacking. How can the technology also protect the private data? Through the apps and services licensed by the Government that help to keep your information secure, such as privacy score, disconnect, safe shepherd, cocoon, Anchor Free hotspot shield, LBE privacy guard, and Burn Notes. Encourage and recommend technologies which enhance privacy and security such as encryptions and protection of communication tools.

ARTICLE INFO

***Correspondence:**
bharathidhivya876@gmail.com
Student, Bharath Institute of Law, Selaiyur, Chennai-600073

Dates:
Received: 28-07-2025
Accepted: 22-09-2025
Published: 31-12-2025

Keywords:
Cyber Terrorism, privacy Breach, Electronic Trespass, Data Protection.

How to Cite:
Guru, G.S., Dhivyabharathi, K . (2025) Navigating Digital Rights in the Recent Era: Promoting the Freedom and Safety. MediaSpace: DME Journal of Communication, 6(2), 11-16. doi: 10.53361/dmejc.v6i02.02

Introduction

Digital world, often involves protection against cyber criminals or hackers of personal data. Privacy as the right to manage personal information and

MediaSpace:
DME Journal of Communication
e-ISSN: 2583-035X

secure the information. Both are equally important to cyber safety. As per the title, 'NAVIGATING DIGITAL RIGHTS IN RECENT ERA'', that ensure the individuals protection of data requires a combination of technology tools, proactive measures to protect personal information and legal awareness which the security must stronger than before because of the technology reaching higher than we think. Making of update in the laws that should equals to the technology upgrade. The laws that allow the digital rights is also a human right used by the common people and get remedies through these statutes universal declaration of human rights (UDHR), International convent on civil and political right (ICCPR), European convention on human rights (ECHR), and Indian connotational law. New technologies have deeply penetrated in the present legal environment which this not only implementing new paths of analysing the human rights, but also introducing new right and freedoms that evolves in constitutional and regulations by the government. In our article, we frequently recommend the importance of raising public awareness about the their secure or protection of personal data and those most affected by digital transformation. These clearly determines how nowadays its crucial to renovate the principle of human rights in experienced society.

Aim

The aim is to educate individuals about their digital rights and to secure their privacy in the current world. Looking into the recent challenges connected to security of data and personal privacy. Whatever the things that happens in their digital world to make a practice of sharing. Encourage the extension and application of effective policies and statutes that prevents digital rights and privacy. Cheer and encourage practices that intensify for privacy protection in both personal and professional manner. Overall, the aim is to bring up the respect to their personals and each one of them should aware of their rights and how to get rid of the problem faced in it.

Issues Faced

- Date breaches can lead to financial loss, leaking of sensitive information, personal data theft, reputational damage that leads to hacking, security flaws, spamming, morphing which can be rectified by changing their passwords, encryptions, step-by-step verification and informing to relevant institutions and platforms to seek support.
- Even many companies and governments operating and tracking the individual's data that can infringe on right to privacy and freedom of speech.
- Harassment could be in the form of cyberbullying, stalking in online, doxing, trolling, threats, impersonation and sexual harassments are the various form of abusive behaviour in digital platform.
- Insufficient privacy laws and statutes can create loopholes in the legal framework that may create unauthorised use of personal data and blocks execution of digital rights.
- Even outdated loss are failed to perform their role in the modern generation.
- Various practices of privacy laws and statutes across various countries that may complicated and challenging to protect a private data.
- Unfair treatment of individuals or groups that discriminated digitally in various ways and can results in biased decision-making, unequal opportunity in digital resources, inequitable discrimination in social media platform and privacy concerns.

Hypothesis

Digital privacy is the perception that individuals have the right to survive unreservedly on the network, and that unnecessary information should not restrict them.

What Happen, If It Happens

If the Government and corporate surveillance measures for security purpose then people may feel that their data collection can lead to privacy erosion without their clear consent or knowledge. If unauthorised use of links and websites send by the unauthorised person or companies then the privacy of individuals like photos, contacts, personal data are be theft and hacked. In this case, the privacy lost to the person become helpless by the Government

because the details filled by them in that particular website link or with the consent of that person.

If the individual become influenced in social media such as Instagram, snapchat, Facebook, WhatsApp, etc. over addiction to these sources then that may violate their digital right without knowing to them. This may cause less harm compared to the online games. If the financial based online games like rummy circle, winzo, dream 11 etc... are the apps which may cause financial loss over to their addiction. these type of licensed apps through which the loss acquired; the Government become numb to help the people who financially lost in the online games because of consent given by installing them. Even though, they have the right to use the technology but the grievance faced in this is very serious and harmful. If the digital harassment and occur through different online channels like social media, e-mail receiving threatens, messaging apps, public forums, gaming platform that addresses and rectified by primary evidence like screen shot, block the contact, report to certain platform, seek support form family & friends, then these can protect the individual by using the digital platforms.

Legal Frames

Data protection laws: Statutes such as the general data protection regulation (GDPR) in the European union. That protects for personal data and privacy and regulates how the data of an individual is collected, stored and accessed.

- Even California grants the statutes for privacy protection, the California consumer privacy act (CCPR) in the United States.
- Several countries deal with the digital rights management and copyrights disputes such as the digital millennium copy right act (DMCA) in the united state.
- Agreements and treaties between the countries like European union- united states (EU-U.S.) privacy shield framework for data privacy, convention on cybercrime, combating cybercrime on a global scale.
- Court makes a decision on judicial ruling and some digital rights and privacy cases dispose legal precedent that impact how laws are explained and applied in the digital domain.
- Cyber security laws: laws related to cybersecurity must take into an account by the organisation. To protect data form cyberattacks and data breaches these laws measures and report the breaches the private data.
- Under 19 of the Universal Declaration of Human Rights (UDHR) deals with protection of the rights to freedom of opinion and freedom of expression including freedom of speech online and access to information is the primary digital rights.
- Under article 19 of the International Covenant on Civil and Political Rights (ICCPR) is similar to the UDHR, which proclaims the right to freedom of expression, that elongates to digital information and communications.
- The article 10 under European Convention on Human Rights (ECHR) guarantees to the right to freedom of expression that includes freedom in online speed and access to information.

Human Rights And Digital Rights

Human rights and digital rights are closely intersecting but human freedom and dignity views in different aspects in the modern world. Human right recognised in international level whereas digital rights are the sub-right which is under basic human right. The first-generation right are civil and political rights that is the basic rights to freedom of speech, the right to fair trial and the right to privacy. On the other hand, rights and freedoms that use of digital technology and the internet. Second generation right are economic, social and culture right such as the right to work, the right to religion, the right to trade, the right to education and the right to an adequate standard of living. The right to prevent one's personal data in online, freedom of sharing information through digital platforms, the right to access technology and right to protect against cyber threats that also pertains human rights. The protection of human rights in the digital world that involves individuals' dignity, safeguarding individuals' sovereignty, freedom, liberty and self-governance. Most of the risk that taken in the digital world which manifest us from the real technological world. Infringement of digital right is very crucial compared to the violation of human

rights in this generation. Most important thing in this generation is the technology upgrading that may protect and harmful to individuals using the data via online. Even there is a violation of human rights in the digital platform, the people are urge to utilize the technology even through it become dangerous to use. If the digital development were restricted, the modern technology development cannot be utilized properly even there is an upgradation. Technological and professional education shall be equally accessible.

Challenges

Why does data privacy is important in marketing

Marketers regularly use customer's personal data as their strategies. That must secure the information in the proper manner. So, they obey with privacy laws and the business can be trusted by the customers. If the data leaks in the marketing sector becomes more critical.

Data protection and why is it important

Data protection is the technologies or policies which used to safe guard the sensitive data or private information from unauthorized use, Theft, loss or breach or access and these have been restricted by involving such measure like encryption backups and secure access control.

It plays in several important reasons

- Privacy – purpose of keeping the personal information or sensitive information confidential.
- Trust – securing the personal data and maintain them will make the customers comfortable and trust the organisation.
- Risk – Risk of management helps to prevent data breaches and financial losses and protect the reputation damage.

Regulation Approval – Many statutes, such as California Department of Pesticide Regulation (CDPR) and Central Consumer Protection Authority (CCPA) requires managements to secure personal data and ignore legal penalties.

Is AI playing a role in privacy breach?

YES, AI plays an obvious role in privacy breach. Artificial Intelligence (AI) analyse the personal data leads to unauthorized access or misuse of personal information. Exploitation of vulnerabilities can be harder to detect that the details were misused. Artificial intelligence (AI) handling data might not be always perfectly protected.

Pros And Cons

PROS

There is tool that ensure privacy benefits in digital way,

- Protecting sensitive data or information of an individual from Unauthorised access and data theft.
- Users can control and manage their personal data and who and how it is accessed.
- Make a confidence in service through online when the customers feel secure by sharing their data to the organisation.
- Private data can track the person, in case of any fraudulent activity done by the person.
- Encourages to express their opinion through freedom of speech and expression without any fright.
- Security against data theft and cybercrime by giving guidance to the private data.
- Organisations with robust privacy practices enhance trust between the customers and encourage them with their loyalty.
- Make lesser the amount of personal data and lowers the chance of misuse.
- If you want to find any authorities related to any research under your profession, here internal privacy becomes an important role that secure about to research the data can be exploited to cause harm.
- There is more security in the Information Technology (IT) components such as Application security, mobile security, Network security and internal security.

CONS

- For some privacy measures can complicate user practice such as using too many passwords or verification.

- Privacy measures can block lawful investigations into crime and terrorism, it is harder to gather evidence for the authorities.
- Limited data sharing required for research and development in the professionals like Technology and Healthcare.
- Misuse of the person's sensitive information without the consent of the users of particular technology which still breaches the data.
- Governments and corporations, breach the privacy sill occur ever there is a law to protect them.
- More free online services, due to data construction and may lead to discontinuation in the connection of internet.
- The main cons of digital privacy can lead to pessimistic behaviour in online like child abuse, harassment.

Social Media Issues

Beginning in late 2022, for the data privacy concerns provoked U.S. State and federal agencies ban employees from using TikTok on the devices of Government -owned. Because TikTok is possessed by U.S. Government may use TikTok to know about the confidential information through these devices.

Being a government can take, for their confidential matters. Even to the common users of all the technologies developed in their generation want some laws and same agencies so that the people need not fear about the data theft and hacking.

The deadly game has spread over all the country and in India has their reports of children hurting themselves and even committing suicides which the game named as blue whale challenge. Although the Government has asked companies such as google, Facebook, WhatsApp, Instagram, micro soft and yahoo to instantly block any links that leads to the deadly games.

Here, there is no security for the children to assess the smartphones and the players of this game cannot be stopped playing because of the blackmail and cyberbullying to complete the task given in that game. Teachers in the school should ensure the children about the pros and cons of the internet and should look for the social behaviour of the students.

Dubsmash: In December 2018, Dabsmash New York-based video messaging service had 162 million email addresses, password hashes, usernames and other personal data such as dates of birth etc... Dubsmash accepted the breach and sale of data and gave recommendation to change their password.

Here, there should be any extra authentication for the individual's protection of their personal data, theft through the way of password breach which loss the trust in the Apps that used for their particular purpose.

Bay: An online market place breach on eBay between late February and early March 2014 revealed sensitive private information of an approximately 145 million user accounts. Cybercriminals got access to eBay's system and hacked the employee's sensitive information including encrypted passwords, email address, mailing addresses, dates of birth and phone numbers. Financial information like data and PayPal accounts through there is no breach and affected. In the incident of cybercriminals attack, eBay requested to the user to reset passwords.

These types of financial information theft may affect the people to use of E-Banking method. These financial cybercriminals should be punished and more security should provide by the Government in the ways which money is transferred. Like this online marketing should secure their customer details with proper responsibilities.

Uber data breach: In 2016, uber suffered a data breach that exhibited the personal data of 57 million users of the uber and drivers. Rather that the breach, Uber paid the Hackers $ 100,000 to delete the data and keep breach quiet. This shows a clear violation of data ethics, and damage of Uber's reputation.

Thus, these breaches not only do such violation the personal privacy and trust, but they can lead to loss their financial data and reputational damage, if the companies involved. Certain principles should be handled by the company's side which makes the users to trust and believe creating things.

Case Laws

K.S. Puttaswamy vs Union of India (2017)

This supreme court case held that right to privacy is a fundamental part of the right to life and personal

liberty under article 21 of the constitution of India. Everyone or any person should not suffer for not getting the Aadhaar card. The Aadhaar project was connected with different welfare schemes. The judgement held that the want for a data protection law in the dominion of parliament to legislate on the subject.

Rout vs State of Odisha (2020)

Through this case, the high court justice S.K.Panigrahi noticed that the right to be forgotten. The accused vigorously engage in sexual intercourse with his classmate and put on record that incident and posted it to Facebook with a fake ID of the victim. After caught by the police, he deleted the videos. For the proper order, the victim & prosecution may approach the court to remove the objectionable content from their database.

Jorawar Singh Mundy vs Union of India (2022)

In India, the new Delhi high court directed in the Jorawar Singh Mundy vs Union of India (2022) judgement that the online legal database such as Indian kanoon and other in their websites removed the judgement titled custom vs Jorawar Singh Mundy (2013) in which the petitioner's name approached. The Delhi high court justice M. Pratibha Singh noticed rights such as rights to privacy, the right to information of the public and the maintenance of transparency. Petitioner loss his social life and career prospects, the case name from the database by Indian kanoon and block result showing from research in google similar search sources.

Shreya Singhal vs Union of India (2015)

This case dealt with the dispute of online freedom of speech and constitutionality of section 66A of the international technology act, which criminalized such type of online speech. The supreme court held that section 66A infringe the right to freedom of speech and expression under article 19(10)(a) of the constitution of India and thus it is unconstitutional.

Conclusion

It is high time for the general approach to digital rights that will take into account the challenges of technology and society. Special attention should be paid to edation concerning the privacy policies as it helps to enhance the users' decision-making process. Promoting transparent data practices play an important role of establishing trust between organizations and users. There is the need to enhance sound legislation as a means of protection of the right of the users from being exploited in the use of social networks and other online platforms. Companies should ensure security of their data while at the same time ensuring they respect the freedom of their employees as well as the freedom of the people on the social media platforms. This also includes development of informative tools that the users can use to enhance their awareness of their rights and obligations in cyberspace. Controlling the consent mechanism is very important in order to ensure users are well informed on how their data is being used and shared. Thus, responding to online posts regarding the effects of digital surveillance may be useful for increasing the awareness of people and collective actions for digital rights' protection. The four principles of accountability and transparency will enable us to make the digital environment safer for everyone.

Reference

Information technology act, 2000

Human rights Law, 1st Edition 2012, Dr. S.R. Myneni

IndianKanoon, https://indiankanoon.org/search/?formInput=cases%20on%20right%20to%20privacy (last accessed on 23/09/2024)

Legal Service India, https://www.legalserviceindia.com/legal/article-10664-right-to-privacy-and-data-protection-era.html, (last accessed on 23/09/2024)

ipleaders Blog, https://blog.ipleaders.in/different-aspects-of-right-to-privacy-under-article-21/, (last accessed on 23/09/2024)

Atlan, https://atlan.com/data-ethics-examples/ , (last accessed on 24/09/2024)