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

RESEARCH ARTICLE
doi: 10.53361/dmejm.v5i02.05

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

G Sanjay guru, K Dhivyabharathi

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 publishing of digital media, rights even access computers and other electronics and communication networks. Most of the technologies that are beneficial to beings use such expansive knowledge in the digital mode. Why are digital technologies 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 to restrict the rights of an individual to showcase their skills in the pandemic world. There are infinite 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 a place of insecurity. More disadvantages 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 are provided 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 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 that 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: 15-10-2024
Accepted: 20-11-2024
Published: 30-12-2024

Keywords:
Cyber terrorism, Privacy breach, Electronic trespass, Data protection

How to Cite:
Authors. (2024) Navigating Digital Rights in the Recent Era: Promoting the Freedom and Safety. DME Journal of Management, 5(2), 38-43.
doi: 10.53361/dmejm.v5i02.05

Introduction

The digital world often involves protection against cyber criminals or hackers. Privacy is managing personal information and secure information. Both are equally important to cyber safety. As per the title, 'Navigating Digital Rights in

DME
Journal of Management
e-ISSN: 2582-9432

Recent Era'', ensuring the individual's protection of data requires a combination of technology tools, proactive measures to protect personal information and legal awareness which the security must be stronger than before because of the technology reaching higher than we think. Making updates in the laws that should equal the technology upgrade. The laws that allow digital rights are also human rights used by the common people and get remedies through (UDHR), convent (ICCPR), rights (ECHR), and Indian connotational law. New technologies have deeply penetrated the present legal environment which this not only implementing new paths of analyzing human rights but also introducing new right and freedoms that evolves in the constitution and regulations by the government. In our articles, we frequently recommend the importance of raising public awareness about the security or protection of personal data and those most affected by digital transformation. These clearly determine how nowadays it's crucial to renovate the principle of human rights in an 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 the security of data and personal privacy. Whatever things happen in their digital world make a practice of sharing. Encourage the extension and application of effective policies and statutes that prevent digital rights and privacy. Cheer and encourage practices that intensify privacy protection in both a personal and professional manner. Overall, the aim is to bring up respect to their personals and each one of them should be aware of their rights and how to get rid of the problems faced in it.

Issues Faced

- Date breaches can lead to financial loss, leaking of sensitive information, personal data theft, and reputational damage that leads to hacking, security flaws, spamming, and 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 can infringe on the right to privacy and freedom of speech.
- Harassment could be in the form of cyberbullying, stalking online, doxing, trolling, threats, impersonation and sexual harassment are the various forms of abusive behavior on digital platforms.
- Insufficient privacy laws and statutes can create loopholes in the legal framework that may create unauthorized use of personal data and block the execution of digital rights.
- Even outdated loss failed to perform their role in the modern generation.
- Various practices of privacy laws and statutes across various countries may be complicated and challenging to protect private data.
- Unfair treatment of individuals or groups that discriminate digitally in various ways and can result in biased decision-making, unequal opportunity in digital resources, inequitable discrimination in social media platforms 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 be restricted to them.

What Happens, If It Happens

If the Government and corporate surveillance measures for security purposes then people may feel that their data collection can lead to privacy erosion without their clear consent or knowledge. If unauthorized use of links and websites is sent by unauthorized persons or companies then the privacy of individuals like photos, contacts, and personal data will be theft and hacked. In this case, the privacy lost to the person becomes 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 becomes influenced by 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 online games. If financial-based online games like Rummy Circle, Winzo, dream 11, etc... are the apps that may cause financial loss over to their addiction. These types of licensed apps through which the loss is acquired; the Government becomes numb to help the people who are 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 digital harassment and occurs through different online channels like social media, e-mail receiving threats, messaging apps, public forums, or gaming platforms addressed and rectified by primary evidence like a screenshot, blocking the contact, reporting to certain platforms, seeking support from family & friends, then these can protect the individual by using the digital platforms.

Legal Frames

Data protection laws

Statutes

That is for personal data 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 digital rights management and copyright disputes such as the Digital Millennium Copyright Act (DMCA) in the United States.

Agreements and treaties between countries like for data privacy, conventions on cybercrime, and combating cybercrime on a global scale.

Court makes a decision on judicial rulings and some digital rights and privacy cases dispose of legal precedents that impact how laws are explained and applied in the digital domain.

Cybersecurity laws

laws related to cybersecurity must be taken into account by the organization. To protect data from cyberattacks and data breaches these laws measure and report the breaches the private data.

- Under deals with rights freedom of including freedom speech online and access to information is the primary digital rights.
- Under the which proclaims that elongates digital communications.
- The under to that in the online speed access information.

Human Rights Digital Rights

And closely intersecting freedom and dignity views in different aspects of the modern world. Human rights are recognised at the international level whereas digital rights are the sub-right which is under basic human rights. Right, that is a basic right to a fair trial. On the other hand, rights and freedoms that use digital technology and the internet. Second-generation rights are cultural rights religion, trade, education right to protect one's personal data online, freedom of sharing information through digital platforms, access to technology protection against cyber that also pertains to protection digital world that involves individuals' dignity, safeguarding individuals' sovereignty, freedom, liberty and self-governance. Most of the risks that are taken in the digital world manifest in the real technological world. The infringement of digital rights is very crucial compared to the violation of human rights in this generation. The most important thing in this generation is the technology upgrading that may protect and harmful to individuals using the data online. Even if there is a violation of human rights in the digital platform, people are urged to utilize the technology even though it becomes dangerous to use. If digital development were restricted, modern technology development cannot be utilized properly even if there is an upgrade. Technological and professional education shall be equally accessible.

Challenges

1. 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 privacy laws and the business can be trusted by the customers. If the data leaks in the marketing sector becomes more critical.

2. Data protection and why is it important?

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

It plays in several important reasons:

Privacy

the purpose of keeping personal information or sensitive information confidential.

Trust

securing personal data and maintaining them will make the customers comfortable and trust the organization.

Risk

Risk management helps to prevent data breaches and financial losses and protect the reputation damage.

Regulation Approval

Many statutes, such as the California Department of Pesticide Regulation (CDPR) and the Central Consumer Protection Authority (CCPA) require management to secure personal data and ignore legal penalties.

3. Is AI playing a role in privacy breaches?

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

Pros and Cons

PROS

There is a tool that digitally ensures privacy benefits,

- Protecting sensitive data or information of an individual from unauthorized access and data theft.
- Users can control and manage their personal data and who and how it is accessed.
- Make confidence in service online when the customers feel secure by sharing their data to the organization.
- 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 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 lower 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 secures 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 the internet.
- The main cons of digital privacy can lead to pessimistic behavior in online like child abuse, and harassment.

Social Media Issues

V For the provoked, the devices of the possessed U.S. know them through these devices.

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

v The deadly game has spread over all the country and in India, there have their reports of children hurting themselves and even committing suicide which the game named as blue whale challenge. The Government has asked companies such as Microsoft to instantly block any that leads to the deadly games.

Here, there is no security for the children to access 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 teach the children about the pros and cons of the internet and should look at the social behavior of students.

v Dabsmash password hashes, etc... Dubsmash accepted the breach and sale of data and recommended changing their password. Here, there should be extra authentication for the individual's protection of their data, theft through the way of password breaches which lose the trust in the Apps that are used for their particular purpose.

v eBay: An online marketplace breach revealed a private approximately got system and hacked the employees' addresses, dates of birth phone numbers and although there is no breach and affected. In the incident of cybercriminals attack, eBay requested 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 be provided by the Government in the ways in which money is transferred. Like this online marketing should secure their customer details with proper responsibilities.

v Exhibited Uber shows the damage to Uber's reputation. Thus, these breaches violate the loss of their data if certain principles should be handled by the company's side which makes the users to trust and believe in creating things.

Case Laws

K S Puttaswamy case

Everyone or any person should not suffer for not getting an Aadhaar card. The Aadhaar project was connected with different welfare schemes. The judgment held that the a 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 engaged 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 being 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 directed the (2022) judgment that online legal databases such as Indian Kanoon and others in their websites removed the judgment 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, of maintenance of transparency. The petitioner lost his social life and career prospects, the case name from the database by Indian Kanoon, and the 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 the constitutionality of international type The Supreme Court held that infringed on India and thus it is unconstitutional.

Conclusion

It is high time for a general approach to digital rights that will take into account the challenges of technology and society. Special attention should be paid to education concerning privacy policies as it helps to enhance the users' decision-making

process. Promoting transparent data practices plays an important role in establishing trust between organizations and users. There is a need to enhance sound legislation as a means of protecting the rights of users from being exploited in the use of social networks and other online platforms. Companies should ensure the 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 social media platforms. This also includes the 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 well-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.

References

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)