INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | July 2023
ISSN: 2582-6433

ADDRESSING DIGITAL SECURITY FOR ESTABLISHING HUMAN RIGHTS

AUTHORED BY - DR. NEWAL CHAUDHARY [1]

Abstract:

In today's rapidly advancing digital age, the significance of safeguarding the right to digital security has become paramount for individuals and communities worldwide. As cyber-attacks and hacking attempts continue to surge, preserving this fundamental human right has become more complex than ever before. This article delves into the crucially of digital security as an essential human right and explores strategies to safeguard and uphold it in the face of evolving cyber threats. Examining both the legal and ethical aspects, we navigate the intricate landscape of digital security. We analyze the implications of government surveillance and scrutinize the responsibilities that technology companies bear in protecting users' data and privacy. Acknowledging the multifaceted nature of this issue, we aim to foster a comprehensive understanding of the challenges and opportunities surrounding digital security. In today's digital age, the right to digital security is becoming increasingly important for individuals and communities around the world. However, with the rise of cyber-attacks and hacking attempts, protecting this right is becoming more challenging than ever before. This article will examine the importance of digital security as a fundamental human right, and the ways in which this right can be protected and upheld in the face of evolving cyber threats. We will explore the legal and ethical considerations involved in digital security, as well as the impact of government surveillance and the responsibilities of technology companies in protecting users' data and privacy. Finally, we will discuss potential solutions for improving digital security, including increased education and awareness, improved digital infrastructure, and stronger international norms and agreements. By exploring these issues, we hope to shed light on the importance of the right to digital security and the challenges and opportunities involved in protecting this right in the 21st century.

Keywords: Digital security, Human rights, Privacy, Cyber threats, Hackers.

[1] Advocate, Supreme Court of Nepal ; Assistant Professor , Nepal Law campus, Tribhuvan University, Exhibition Road, Kathmandu, Nepal.

ISSN: 2582-6433

I. Introduction:

The digital age has brought unprecedented access to information and connectivity for individuals and communities around the world. However, with this increased access has come a heightened risk of cyber-attacks, hacking attempts, and breaches of digital security. As more and more aspects of our lives move online, from financial transactions to healthcare records, the need for robust digital security measures has become increasingly important. In this article, we will explore the right to digital security as a fundamental human right, and the ways in which this right can be protected and upheld in the face of evolving cyber threats. Digital security has become increasingly crucial in the modern era, where cyber threats like hacking, identity theft, and malware attacks pose a significant risk to individuals' privacy, financial security, and physical safety. Beyond the protection of personal information, digital security is a fundamental human right, and it is essential for safeguarding freedom of expression and other civil liberties. In general sense, digital security lies on cyber security and cyber security lies on protection of digital privacy. The importance of digital security is underpinned by international human rights treaties that recognize the right to privacy as a fundamental right. Without digital security, individuals' personal information could easily be accessed by hackers or other malicious actors, resulting in identity theft, financial fraud, and other forms of harm. Moreover, concerns about government surveillance pose significant legal and ethical considerations. While governments have a responsibility to protect citizens from cyber threats, mass surveillance risks undermining trust in democratic institutions and eroding civil liberties. The role of technology companies is also critical in protecting users' data and privacy. However, companies have often failed to live up to this responsibility, putting users' personal information at risk. This trend towards mass surveillance and failure to prioritize user privacy and security underscores the need for stronger digital security measures. There are several potential solutions for improving digital security, including increased education and awareness campaigns, improved digital infrastructure, and stronger international norms and agreements. Through education and awareness campaigns, individuals can better understand the risks associated with digital security and how to protect themselves. Robust digital infrastructure, such as stronger encryption standards and more secure networks, can help prevent cyber threats from occurring. Moreover, stronger international norms and agreements can help ensure that governments and technology companies are held accountable for protecting users' digital security.

ISSN: 2582-6433

II. The Importance of Digital Security as a Human Right:

The right to digital security can be seen as an extension of the right to privacy, which is enshrined in international law and recognized as a fundamental human right. Digital security is a term used to describe the economic and social aspects of cyber security, in contrast to the technical aspects or those related to criminal law enforcement and national or international security. The word "digital" is often used in conjunction with expressions such as digital economy, digital transformation, and digital technologies. This terminology provides a foundation for constructive international dialogue among stakeholders who aim to establish trust and maximize opportunities for information and communication technologies (ICTs)[2]. Digital security is essential for protecting individual's personal information, financial data, and other sensitive information from cyber-attacks and hacking attempts. Furthermore, the right to digital security is essential for protecting freedom of expression and other civil liberties, as individuals who feel their digital security is compromised may be less likely to speak out on sensitive issues or engage in other forms of online activism. Digital security is more than just a tool to protect personal information or prevent cyber-attacks; it is a fundamental human right that supports privacy, freedom of expression, and other civil liberties. International human rights treaties, such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Convention on Human Rights, have enshrined the right to privacy. This right protects individuals from arbitrary or unlawful interference with their privacy, family, home, or correspondence. In the digital age, the right to privacy includes the protection of personal data, such as an individual's online activities, communication history, and location data. The absence of digital security puts individuals' personal information at risk of being accessed by hackers or other malicious actors, resulting in identity theft, financial fraud, and other forms of harm. In addition, concerns about government surveillance pose significant legal and ethical considerations. While governments have a duty to protect citizens from cyber threats, mass surveillance risks undermining trust in democratic institutions and eroding civil liberties. Over the years, there have been several cases of government surveillance and data breaches that have highlighted the need for stronger digital security measures. For instance, in 2013, Edward Snowden, a former contractor for the US National Security Agency, revealed the extent of the

[2]OECD, Digital Security, https://www.oecd.org/digital/digital-security/ (last visited Apr. 13, 2023).

ISSN: 2582-6433

agency's surveillance activities, both in the US and abroad[3]. The disclosure sparked widespread debate about the balance between national security and individual privacy. Similarly, the Cambridge Analytica scandal in 2018 demonstrated the risks associated with the collection and use of personal data by technology companies. The scandal involved the unauthorized collection of data from millions of Facebook users, which was used to influence political campaigns. The scandal highlighted the importance of digital security measures to safeguard individuals' privacy and civil liberties. In the digital age, technology has become an essential tool for individuals to express their opinions, access information, and participate in public discourse. However, without digital security, these activities could be compromised by surveillance or censorship. Governments have a responsibility to protect the right to freedom of expression online while also safeguarding individuals from cyber threats. Balancing these responsibilities can be challenging, but it is essential to protect both fundamental human rights. Furthermore, technology companies must play their part in protecting users' digital security and ensuring that their platforms are not used to facilitate censorship or human rights violations.

Nepal and India both have laws that address digital security concerns. In Nepal, the Electronic Transaction Act 2063 provides a legal framework for regulating electronic transactions and protecting sensitive data. The act covers areas such as data privacy, electronic signatures, and cybercrime[4]. Similarly, in India, the Information Technology Act 2000 establishes the legal framework for regulating electronic transactions, including data privacy, digital signatures, and cybercrime. However, despite having legal frameworks in place, both Nepal and India face challenges in enforcing their digital security laws. For example, the lack of resources and trained personnel can hinder the effective implementation of these laws. Additionally, the absence of strong data protection laws and regulatory bodies to oversee the implementation of these laws can be a significant challenge. In contrast, some countries have more robust legal frameworks and regulatory bodies to address digital security concerns. For example, the European Union's General Data Protection Regulation (GDPR) sets strict rules for companies that process personal data of EU citizens. The regulation requires companies to obtain explicit consent from individuals and implement appropriate measures to protect their data. Failure to comply with these rules can result in significant fines. Similarly, in the United States, there are several federal and state laws that address digital security concerns. The Health Insurance Portability and Accountability Act

[3] BBC News, Edward Snowden profile: Who is the former NSA contractor? , (June 11, 2013, 9:18 AM), https://www.bbc.com/news/world-us-canada-23123964 (last visited Apr. 13, 2023).
[4] Electronic Transaction Act, (2063).

ISSN: 2582-6433

(HIPAA) regulates the collection and storage of personal health information, while the Children's Online Privacy Protection Act (COPPA) sets strict rules for websites and online services that collect data from children under 13 years old. Apart from legal considerations, ethical considerations also play a significant role in digital security. For example, the use of surveillance technologies can raise ethical concerns about privacy and civil liberties. In many countries, the use of facial recognition technology by law enforcement agencies has come under scrutiny due to concerns about the accuracy of the technology and the potential for abuse. In contrast, some countries have taken a more proactive approach to address ethical considerations in digital security. For example, the Canadian government has established a national consultation process to develop guidelines for the ethical use of artificial intelligence (AI). The guidelines are intended to ensure that AI is used in a way that respects human rights, avoids bias, and promotes transparency.

III. The Legal and Ethical Considerations of Digital Security:

One potential application of digital security is safeguarding one's personal information against misuse and commercial exploitation by corporations[5]. Protecting the right to digital security involves navigating a complex web of legal and ethical considerations. For example, governments have a responsibility to protect their citizens from cyber threats, but this must be balanced against concerns about government surveillance and the potential for abuse of power. Similarly, technology companies have a responsibility to protect users' data and privacy, but this must be balanced against the need for businesses to collect and use data for legitimate purposes. In today's digital age, digital security has become a critical concern for individuals, governments, and businesses alike. The increasing dependence on digital technology, coupled with the rising sophistication of cyber threats, has created an urgent need to safeguard sensitive data and protect privacy. However, the pursuit of digital security raises a range of legal and ethical considerations, which must be carefully balanced against the need to prevent cyber threats and maintain national security. One of the most pressing legal considerations surrounding digital security is the issue of data privacy. As more personal information is shared and stored digitally, the potential for data breaches and identity theft becomes a significant concern. In response, governments around the

[5] Security.org, Digital Safety, https://www.security.org/digital-safety/ (last visited Apr. 13, 2023).

ISSN: 2582-6433

world have enacted laws to regulate the collection, storage, and use of personal data. For example, the European Union's General Data Protection Regulation (GDPR) establishes strict rules for companies that process personal data of EU citizens, requiring them to obtain explicit consent from individuals and implement appropriate measures to protect their data. Similarly, in the United States, the California Consumer Privacy Act of 2018 (CCPA) grants consumers the right to know what personal information is being collected about them and how it is being used, as well as the right to request deletion of their data. These laws reflect a growing recognition of the importance of data privacy and the need to hold companies accountable for protecting individuals' personal information. Another key legal consideration in digital security is the use of encryption technology. Encryption is a method of protecting data by encoding it so that it can only be read by authorized parties who possess the decryption key. While encryption can provide valuable protection against cyber threats, it can also create challenges for law enforcement and national security agencies. For example, encrypted communications can be used by terrorists and other criminals to plan attacks without detection. In response, some governments have sought to weaken encryption standards to allow law enforcement agencies to access encrypted data when necessary. However, this approach raises significant ethical concerns. Weakening encryption could make it easier for hackers and other malicious actors to access sensitive data, potentially exposing individuals to harm. Moreover, undermining encryption standards could have a chilling effect on free speech and privacy rights. It is essential to strike a balance between the need for digital security and the need to protect civil liberties. Another ethical consideration in digital security is the use of surveillance technologies by governments and law enforcement agencies. Surveillance technologies, such as facial recognition software and location tracking, can provide valuable tools for detecting and preventing criminal activity. However, their use also raises concerns about privacy and civil liberties. Without appropriate safeguards and oversight, surveillance technologies can be used to monitor individuals' activities without their knowledge or consent, potentially infringing on their rights. To address these concerns, governments must establish clear legal frameworks and oversight mechanisms to regulate the use of surveillance technologies. Moreover, technology companies must prioritize user privacy and security in the design and development of their products.

ISSN: 2582-6433

IV. The Impact of Government Surveillance:

One of the biggest threats to the right to digital security is government surveillance. In recent years, we have seen an increasing trend towards mass surveillance by governments around the world, often justified in the name of national security or counterterrorism. However, such surveillance can have a chilling effect on freedom of expression and other civil liberties, and can undermine trust in government and democratic institutions.

In the United States, the National Security Agency (NSA) came under scrutiny in 2013 after former contractor Edward Snowden leaked classified documents revealing the extent of the agency's surveillance programs. The leaked documents showed that the NSA was collecting data on millions of Americans without their knowledge or consent. This led to widespread public outrage and calls for greater transparency and accountability.

The impact of government surveillance on digital security is significant. When individuals believe that their activities are being monitored, they may be less likely to express their opinions or engage in activities that could be considered controversial. This can have a chilling effect on free speech and lead to self-censorship.

Furthermore, government surveillance can also lead to a lack of trust in digital security systems. If individuals believe that their personal data is not secure, they may be less likely to use online services or engage in electronic transactions. This can have a significant impact on e-commerce and digital economies.

V. The Role of Technology Companies in Protecting Digital Security:

Technology companies have a responsibility to protect users' data and privacy, and to ensure that their products and services are secure from cyber threats. However, in many cases, companies have failed to live up to this responsibility, either through negligence or a desire to collect and monetize user data. This has led to a series of high-profile data breaches and other incidents, which have eroded trust in technology companies and underscored the need for stronger digital security measures.

ISSN: 2582-6433

One significant role of technology companies is to ensure that their products and services are secure by design. This means that security is integrated into every aspect of product development, from design to deployment. This approach helps to prevent vulnerabilities and reduce the risk of cyber-attacks. Technology companies also play a critical role in educating users about digital security best practices. For example, companies can provide users with guidance on creating strong passwords, avoiding phishing scams, and updating software regularly. This can help to prevent common security breaches and protect user data. In addition to improving their own digital security practices, technology companies also have a responsibility to protect user data from government surveillance. In recent years, there have been numerous cases where technology companies have been asked to provide user data to governments for national security or law enforcement purposes. In some cases, technology companies have challenged these requests in court, arguing that they violate user privacy rights. Another way technology companies can protect digital security is by promoting open standards and interoperability. Open standards allow different technology systems to communicate with each other, which can help to prevent lock-in and create a more competitive market. Interoperability can also help to prevent vendor lock-in and promote innovation in digital security. However, technology companies also face ethical considerations in the collection and use of user data. In recent years, there have been numerous cases of technology companies collecting and using user data in ways that violate user privacy rights. For example, companies have been criticized for using user data to target advertising, or for selling user data to third-party companies without user consent. To address these ethical considerations, technology companies can implement clear privacy policies and obtain informed consent from users before collecting and using their data. They can also be transparent about their data collection and use practices and provide users with tools to control their data.

VI. Solutions for Improving Digital Security:

There are a number of potential solutions for improving digital security, including increased education and awareness, improved digital infrastructure, and stronger international norms and agreements. For example, education and awareness campaigns can help individuals and communities better understand the risks and challenges involved in protecting digital security, while improved infrastructure can make it easier to implement effective security measures. Stronger international norms and agreements can help establish clear standards for responsible behavior in cyberspace, and can provide a framework for international cooperation on digital security issues.

ISSN: 2582-6433

One technology solution for improving digital security is the use of encryption. Encryption is the process of encoding information so that it can only be accessed by authorized users. Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography[6]. This can help to protect sensitive information from cyber threats, such as data breaches and hacking attempts. Many technology companies have implemented encryption in their products and services, and encryption has become a standard practice in digital security. Another technology solution for improving digital security is the use of multi-factor authentication. Multi-factor authentication is the process of using more than one method of authentication to verify a user's identity. For example, a user may need to enter a password and provide a fingerprint or facial recognition scan. This can help to prevent unauthorized access to user accounts and protect against phishing attacks. Policy solutions can also help to improve digital security. For example, governments can pass laws that require companies to implement strong digital security practices, such as encryption and multi-factor authentication. Governments can also fund research into new digital security technologies and provide resources for user education. User education is also an essential component of improving digital security. Many cyber threats are the result of user behavior, such as using weak passwords or falling for phishing scams. By educating users about digital security best practices, such as creating strong passwords and avoiding suspicious emails, users can become more aware of potential threats and take steps to protect themselves. In addition to these solutions, it is also essential to prioritize collaboration and information sharing among different stakeholders. Governments, technology companies, and users all have a role to play in improving digital security. By working together and sharing information about digital threats and best practices, we can create a more secure and resilient digital landscape.

VII. Conclusion:

The right to digital security is an essential human right that is becoming increasingly important in the digital age. Protecting this right involves navigating a complex web of legal and ethical considerations, and requires collaboration and cooperation between governments, technology companies, and civil society organizations. By working together to strengthen digital security measures and protect users' data and privacy, we can ensure that the right to digital security is

[6] TechTarget, Encryption Definition, SearchSecurity (TechTarget, last updated May 2020), https://www.techtarget.com/searchsecurity/definition/encryption (accessed: April 13, 2023).

ISSN: 2582-6433

upheld and protected for generations to come.

It is clear that improving digital security requires a multi-faceted approach that involves collaboration and information sharing among different stakeholders. By prioritizing digital security and working together to implement strong digital security practices, we can create a more secure and ethical digital landscape for all. The right to digital security is a critical component of our human rights, and it is essential that we protect it. By taking steps to improve digital security, we can ensure that individuals and organizations are protected from cyber threats and that the digital world remains a safe and secure place for all.