INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN:2582-6433

DISCLAIMER

 ISSN:2582-6433

EDITORIALTEAM

EDITORS

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

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

 ISSN:2582-6433

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.

 ISSN:2582-6433

SURVEILLANCE OF CYBER SECURITY AND HUMAN RIGHTS

AUTHORED BY - SOHAIR AHMED SHAIKH

ABSTRACT:

The relationship between cybersecurity and human rights has grown in importance in our evolving digitalized society. The hazards to privacy, freedom of expression, and security have increased as people, businesses, and governments now depend more on digital technologies for communication, trade, and governance. Human rights are significantly impacted by cybersecurity, which is typically concerned with defending networks, systems, and data against online attacks. This is especially true when it comes to preserving fundamental liberties.

The escalation of cyberattacks, data breaches, and spying directly jeopardizes basic rights including freedom of speech and privacy. Concerns regarding abuse, illegal access, and the possibility of mass monitoring are raised by the frequent collection of enormous volumes of personal data by governments and businesses. Cybersecurity methods are occasionally employed to monitor and stifle opposition in authoritarian governments. Thus, the freedoms of assembly and expression are violated. On the other hand, strong cybersecurity regulations can strengthen citizens' rights to engage in the digital sphere without worrying about reprisals by guaranteeing safe communication, safe access to information, and protection from cyberthreats.

The Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights are two examples of international law and human rights frameworks that offer a basis for striking a balance between rights and security in the digital age. However, there are difficulties with regulation and enforcement due to the quick speed of technical advancement. There is a growing demand for legal frameworks that protect human rights while addressing cybersecurity, making sure that laws don't unduly restrict freedoms or violate privacy in the name of security.

This paper explores the complexities of cybersecurity in the context of human rights, emphasizing the need for a balanced approach that promotes both security and the protection of fundamental freedoms. It underscores the importance of international cooperation, legal

 ISSN:2582-6433

reform, and responsible corporate practices in creating a cyberspace that respects human dignity and rights.

KEYWORDS: Data Protection, Cyber Security, Cyber Attacks, Digital Governance, Human Rights, Cyber Laws, Digital Justice.

INTRODUCTION:

Cybersecurity refers to the strategies, tools, and practices used to protect against online threats, such as data breaches, cyberattacks, and system vulnerabilities. It is crucial for individuals, businesses, and governments to safeguard sensitive information and ensure the integrity of digital services. [1]Cybersecurity involves defending against a wide range of potential threats from hackers, nation-states, and cybercriminals. Its importance lies in preventing data loss, system damage, and the disruption of services.

Human rights, on the other hand, are the fundamental freedoms and protections that belong to all individuals, regardless of their nationality, race, religion, or other characteristics. These rights are enshrined in international law and include the right to life, freedom, personal security, freedom of expression, religious practice, and participation in cultural activities, among others. As the internet and digital technologies become increasingly essential to the exercise of many human rights, the relationship between cybersecurity and human rights becomes more complex.

The intersection of cybersecurity and human rights involves both the need for security and the protection of individual freedoms. The internet and digital technologies are integral to the realization of numerous human rights, such as access to information, freedom of expression, and the ability to participate in public life. However, the protection of these rights can be compromised by cyber threats like surveillance, data breaches, and censorship. Therefore, it is critical to maintain a balance between ensuring cybersecurity and upholding fundamental human rights.

[1] **Human Rights and the Digital Age**: U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (June 30, 2014), https://www.ohchr.org/en/issues/opinion/pages/opinionindex.aspx.

 ISSN:2582-6433

As digital technologies continue to evolve, the responsibility of governments, businesses, and individuals to safeguard both cybersecurity and human rights becomes even more vital. Policies must be developed to protect digital security without infringing upon privacy, freedom of expression, or other basic human rights. This growing interdependence calls for comprehensive legal frameworks, international cooperation, and ethical cybersecurity practices to ensure that the digital landscape supports both security and human dignity.

THREATS FOR THE CYBER SECURITY:

Cybercrime encompasses illegal activities that utilize computers, networks, or digital technologies. This category of crime includes various offenses such as hacking, identity theft, online fraud, cyberbullying, data breaches, and the dissemination of malicious software (malware). Targets of cybercrime can range from individuals to organizations and governments, with perpetrators engaging in actions like stealing personal data, inflicting financial damage, disrupting services, or propagating harmful online content. As technological advancements progress, the prevalence of cybercrime has emerged as a significant global issue, necessitating specialized law enforcement efforts and international collaboration to address it effectively.

2Cybercrimes are becoming increasingly common in the contemporary digital landscape. Several notable cybercrimes associated with video calls and video leaks include: 1. Video Call Extortion (Blackmail) This crime entails an individual being pressured to pay money or divulge sensitive information to avert the release of compromising video footage or personal images captured during private video calls. Often, perpetrators threaten to disclose intimate or private video content unless their demands are met. 2. Unauthorized Sharing of Personal Videos Private video calls can be surreptitiously recorded and subsequently shared or published online without the consent of the individual being filmed. Such actions typically involve private moments or content that the victim believed would remain confidential, resulting in considerable personal and professional repercussions. 3. Sexual Extortion and "Sextortion" This type of cybercrime involves leveraging intimate or explicit video material to extort money, Favors, or additional explicit content from the victim. It may commence with a video call or online interaction where explicit content is solicited, and once acquired, it is used for blackmail

[2] **General Cybercrime Threats and Legal Frameworks**: *National Institute of Standards & Technology*, Cybersecurity Framework, NIST (last visited Dec. 26, 2024), https://www.nist.gov/cyberframework.

 ISSN:2582-6433

purposes. 4. Non-Consensual Video Recording Certain cybercriminals engage in recording video calls without the knowledge or consent of the individual being filmed. This practice can be part of a larger scheme to exploit the footage for malicious intents, such as blackmail or damaging someone's reputation. 5. Cyberstalking via Video Calls In some instances, individuals may utilize video calls as a method to stalk or harass another person. This may involve persistent unwanted video calls, manipulation, or threats made during the calls, resulting in emotional distress or harm to the victim.

3Cybersecurity refers to the strategies and protocols implemented to safeguard computer systems, networks, and information from unauthorized access, damage, or theft. In the contemporary digital landscape, where technology is intricately woven into daily life, this field has become increasingly vital. The principles of cybersecurity include several key elements, such as: 1) Confidentiality: Protecting sensitive information to ensure it is accessible solely to authorized users or systems. 2) Integrity: Preserving the accuracy and reliability of data by preventing unauthorized alterations or tampering. 3) Availability: Guaranteeing that systems and data are accessible when required and safeguarded against interruptions or outages. 4) Authentication: Confirming the identity of users or systems seeking access to resources. 5) Authorization: Assigning appropriate access rights to verified individuals or systems based on established roles or permissions. 6) Encryption: Transforming data into a secure format to shield it from unauthorized access during transmission or storage.

CYBER LAWS:

Cyber laws in India encompass a series of regulations and legal frameworks designed to combat cybercrime, facilitate electronic commerce, safeguard digital privacy, and enhance information security. These laws establish a comprehensive structure to oversee online activities, protect individuals, businesses, and governmental bodies from cyber threats, and ensure the security of online transactions.

Prominent Cyber Laws and Acts in India:4 Information Technology Act, 2000 (IT Act, 2000) This is the principal legislation governing cyber activities within India. It addresses issues

[3] **Cybercrime** **Definition**: *Cybersecurity & Infrastructure Security Agency*, Cybersecurity: What is Cybersecurity? CISA (last visited Dec. 26, 2024), https://www.cisa.gov

[4] **India**, *Information Technology Act, 2000*, No. 21 of 2000, § 1, 2000, https://www.indiacode.nic.in/handle/123456789/1998?view_type=advanced&sam_handle=123456789/1362.

related to cybercrime, digital signatures, electronic contracts, and e-governance. The Act includes provisions concerning cyber offenses (such as hacking and identity theft), data protection, electronic evidence, and e-commerce. It introduced the concept of cybersecurity and defined the roles of Certifying Authorities and the Controller of Certifying Authorities. An amendment in 2008 introduced more stringent measures against cyberterrorism and online child pornography.

Indian Penal Code (IPC) - Amendments Certain sections of the IPC are applicable for prosecuting cyber offenses, including: 5Section 66: Pertaining to hacking and unauthorized access to computer systems. Section 66A (repealed in 2015): Related to the transmission of offensive messages through communication devices. 6Section 469: Concerning forgery in relation to digital documents or electronic records. Section 500: Addressing defamation, which can extend to online content.

The Copyright Act, 1957 This Act addresses issues of digital piracy and the infringement of intellectual property rights in the digital realm. It offers protection for digital content, including software, music, and various forms of online media.7

8 The Data Protection Law (Proposed - Personal Data Protection Bill) This proposed legislation seeks to regulate the collection, storage, and utilization of personal data. It mandates that organizations obtain consent prior to processing personal data and guarantees individual rights concerning their personal information. The law includes provisions for addressing data breaches, imposing penalties, and establishing a Data Protection Authority of India (DPAI). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 These rules govern the practices related to the protection of sensitive personal data and information.

---

[5] **Section 66 (Hacking and Unauthorized Access)**: *Indian Penal Code* (IPC), No. 45 of 1860, § 66, (India), https://www.indiacode.nic.in/handle/123456789/2267?view_type=advanced&sam_handle=123456789/1362.

[6] **Section 469 (Forgery of Digital Documents)**: *Indian Penal Code* (IPC), No. 45 of 1860, § 469, (India), https://www.indiacode.nic.in/handle/123456789/2267?view_type=advanced&sam_handle=123456789/1362.

[7] **India**, *Copyright Act, 1957*, No. 14 of 1957, § 1, 1957, https://www.indiacode.nic.in/handle/123456789/2263?view_type=advanced&sam_handle=123456789/1362.

[8] **Personal Data Protection Bill (Proposed)**: *India, Personal Data Protection Bill, 2019*, Bill No. 373 of 2019, § 1, 2019, https://www.prsindia.org/billtrack/personal-data-protection-bill-2019.

 ISSN:2582-6433

INTERPLAY BETWEEN CYBERSECURITY AND HUMAN RIGHTS:

The relationship between cybersecurity and human rights represents a multifaceted and dynamic area of concern. While the primary objective of cybersecurity is to safeguard computer systems and data from cyber threats, it is imperative to ensure that this objective does not come at the expense of human rights and fundamental freedoms. The following points illustrate the connection between these two domains:

Right to Privacy: (Article 21 of the Constitution of India) Cybersecurity initiatives, including data collection and surveillance, may encroach upon individuals' right to privacy. It is essential to find an appropriate equilibrium to ensure that cybersecurity practices do not unduly infringe upon privacy rights.

Freedom of Expression: (Article 19 of the Constitution of India) Cybersecurity protocols should not serve as a justification for curtailing freedom of expression. Governments and organizations must refrain from utilizing cybersecurity as a rationale for censorship or suppressing dissenting opinions.

Access to Information: Although cybersecurity is vital for safeguarding information, overly stringent security measures can hinder access to information, thereby obstructing individuals' rights to seek, receive, and disseminate information. It is necessary to balance security with accessibility to prevent unwarranted restrictions on this right.

Due Process and Rule of Law: In the quest for enhanced cybersecurity, it is crucial to ensure that law enforcement and intelligence agencies operate within the framework of the rule of law. All measures should be subject to legal scrutiny, and individuals' rights to due process, fair trials, and the presumption of innocence must be maintained.

Protection of Vulnerable Groups: Individuals or groups that are vulnerable may encounter distinct challenges in the digital landscape, such as online harassment or targeted cyberattacks. Cybersecurity strategies should address their specific needs and safeguard them from discrimination and harm.

Cybersecurity and Economic, Social, and Cultural Rights: The accessibility and affordability of secure digital infrastructure are vital for the fulfilment of economic, social, and cultural rights. Robust cybersecurity measures should be implemented to ensure the protection of these

 ISSN:2582-6433

rights.

INTERNATIONAL STANDARDS AND BOUNDARIES:

International legal frameworks and standards are essential in tackling the challenges posed by cybersecurity and human rights on a global scale. They offer guidance, norms, and principles for governments, organizations, and individuals to safeguard rights and security in the digital era. The following are some significant frameworks and standards:9 1) Universal Declaration of Human Rights (UDHR): Ratified by the United Nations (UN) General Assembly, the UDHR outlines the fundamental human rights and freedoms that are universally applicable. It serves as the cornerstone of international human rights law and provides principles relevant to the digital landscape. 2) 10International Covenant on Civil and Political Rights (ICCPR): This treaty safeguards civil and political rights, including the right to privacy, freedom of expression, and due process. It is applicable to the online environment and offers guidance on reconciling security with human rights. 3) Convention on Cybercrime (Budapest Convention): Developed by the Council of Europe, the Budapest Convention seeks to harmonize national laws and bolster international cooperation in combating cybercrime. It addresses issues such as hacking, data breaches, and cyber-related offenses while ensuring the protection of human rights. 4) General Data Protection Regulation (GDPR): Enforced by the European Union (EU), the GDPR establishes comprehensive standards for data protection and privacy. It sets forth requirements for organizations that handle personal data, including consent, transparency, and the rights of individuals. 5) United Nations Guiding Principles on Business and Human Rights: These principles offer a framework for businesses to uphold human rights within their operations, particularly in the digital domain. They stress the obligation of companies to prevent and address human rights violations, including those associated with cybersecurity. 6) National Cybersecurity Strategies: India has developed and implemented its National Cybersecurity Strategy to confront the increasing challenges in cyberspace.

[9] **Universal Declaration of Human Rights (UDHR)**: *Universal Declaration of Human Rights*, G.A. Res. 217 A (III), U.N. GAOR, 3rd Sess., U.N. Doc. A/810, at 71 (Dec. 10, 1948), https://www.un.org/en/universal-declaration-human-rights/.

[10] **International Covenant on Civil and Political Rights (ICCPR)**: *International Covenant on Civil and Political Rights*, G.A. Res. 2200A (XXI), U.N. GAOR, 21st Sess., U.N. Doc. A/6316 (Dec. 16, 1966), https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

 ISSN:2582-6433

CONCLUSION:

The convergence of cybersecurity and human rights represents a significant issue in the contemporary digital landscape, where online engagement is essential to personal, social, and economic activities. While the implementation of cybersecurity is crucial for safeguarding sensitive information, infrastructure, and mitigating cyber threats, it is imperative that these measures do not compromise human rights, such as privacy, freedom of expression, and access to information. On one side, robust cybersecurity protocols are necessary to thwart cybercrimes, identity theft, and hacking, thereby ensuring the safety of individuals and nations from digital vulnerabilities. Conversely, overly intrusive or inadequately structured cybersecurity initiatives can encroach upon essential rights. For instance, broad surveillance practices or stringent data collection measures may infringe upon the right to privacy, while censorship or the restriction of free speech can threaten the principle of freedom of expression. A comprehensive approach that includes various stakeholders—such as governments, civil society, the private sector, and technical experts—is essential for balancing security with human rights. It is imperative to ensure transparency, accountability, and the integration of human rights considerations in the development and execution of cybersecurity strategies. As technological advancements continue and cyber threats become more sophisticated, it is vital to revise and enhance these frameworks to effectively tackle new challenges. By fostering collaboration, upholding human rights, and complying with international standards, we can successfully navigate the digital environment while safeguarding both security and fundamental rights in the contemporary digital era.

REFERNCES:

[1] Kulesza, Joanna & Balleste, Roy. (2015), Cybersecurity and Human Rights in the Age of Cyberviolence, Rowman Littlefield Publishers

[2] Godwin, Mike. (2003), Cyber Rights: Defending Free speech in the Digital Age (The MIT Press), CBS PUBLISHERS & DISTRIBUTORS PVT. LTD

[3] BARE ACT OF INDIAN PENAL CODE (ACT NO.45 OF 1860).

[4] BARE ACT OF CONSTITUITON OF INDIA.

[5] https://eicta.iitk.ac.in/knowledge-hub/cyber-security/cybersecurity-an-introduction-to-threats-risks-and-best-practices/

[6] https://www.javatpoint.com/what-is-cyber-securit