# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

# DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

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

# BALANCING SECURITY AND FREEDOM: CYBERSECURITY IN THE AGE OF HUMAN RIGHTS.

AUTHORED BY - PATEL HARSHALI SHAILESHBHAI,
PATEL DEVYANSHI UMESH, TISHA MADATBHAI PANJWANI
& PATEL DEVANSHI MUKESH

## ABSTRACT

The rapid growth of digital technologies in India has transformed communication, governance, and economic activities, but it has also raised critical challenges for both cybersecurity and human rights. Cybersecurity ensures the protection of information, networks, and critical infrastructure, while human rights safeguard individual freedoms such as privacy, freedom of expression, and access to information. In India, the rise of cybercrime, surveillance practices, and data breaches has led to significant concerns about the balance between security and civil liberties. The implementation of laws such as the Information Technology Act, 2000, and recent initiatives like the Digital Personal Data Protection Act, 2023, demonstrate the state's attempt to secure cyberspace. However, questions remain about state surveillance, digital censorship, and the potential infringement of fundamental rights under the Indian Constitution, especially Article 19 (freedom of speech) and Article 21 (right to life and privacy). This paper explores the intersection of cybersecurity and human rights in India, analyzing legal frameworks, emerging challenges, and the need for a rights-based approach to digital security.

## Keywords

Cybersecurity, Human Rights, Privacy, Freedom of Expression, Data Protection, Cyber Laws in India, Digital Rights, Surveillance, Cybercrime, Information Technology Act, Constitution of India.

## Introduction

The rapid advancement of digital technologies has transformed the way individuals interact, communicate, and conduct business. However, alongside these benefits, the growth of cyberspace has also given rise to new forms of criminal activity, commonly referred to as cybercrime. Cybercrime includes offenses such as identity theft, hacking, phishing,

ISSN: 2582-6433

cyberstalking, financial fraud, and the spread of harmful or extremist content. These crimes not only threaten national security and economic stability but also pose significant challenges to the protection of fundamental human rights.

Human rights—such as the right to privacy, freedom of expression, access to information, and the right to security—are increasingly vulnerable in the digital era. For example, unlawful surveillance and data breaches compromise privacy rights, while online harassment and hate speech can undermine the dignity and equality of individuals. At the same time, governments face the challenge of balancing the enforcement of cybercrime laws with the protection of rights like freedom of speech.

Thus, the study of cybercrime and human rights highlights the need for robust legal frameworks, international cooperation, and rights-based approaches to cybersecurity. It underlines the importance of ensuring that technological growth does not come at the cost of fundamental freedoms.

It's a digital dilemma with no easy answers. We live in a world where our lives are increasingly online, and this has created a fundamental conflict between our desire to be safe and our need to be free.

On one side, you have the "safety first" crowd. They argue that in the face of cyberattacks on power grids, identity theft, and online terrorism, we have to give authorities the tools they need to protect us. This means giving governments the power to monitor our communications and collect our data. It’s a trade-off: we sacrifice a little bit of our privacy for a lot more security.

But this trade-off comes at a steep price. When governments have these broad powers, our human rights are at risk. Our privacy vanishes as our every click and search is potentially tracked. Our freedom of speech is threatened when governments can shut down websites or prosecute people for online dissent, often under the guise of fighting "fake news." Our right to assemble is also at stake, as people might be too afraid to join online groups or movements if they know they're being watched.

On the other side are the "freedom first" champions. They believe that an open, uncensored internet is vital for a healthy society. It’s how we hold power accountable, how we share ideas,

ISSN: 2582-6433

and how we empower marginalized voices. But they acknowledge that this freedom can be abused. The very tools that protect a journalist's source—like strong encryption—can also be used by criminals to hide their activities. The open nature of the internet, which allows for a free flow of information, also allows for the spread of propaganda and misinformation.

So, where do we go from here? The solution isn't to simply choose one side over the other. It's about finding a middle ground. We're currently trying to do this in a few ways:

Smarter Laws: Governments are trying to write new rules that give them the power they need to fight crime, but with strict oversight from judges to protect our rights.

Smarter Tech: Companies are developing technologies that can both protect user privacy (like end-to-end encryption) and help identify threats without compromising personal data.

Teamwork: This isn't just a government problem. It requires tech companies, civil society groups, and international organizations all working together to create a global set of principles for how we govern the internet.

The rise of new technologies like artificial intelligence and biometrics only makes this debate more complicated. They offer incredible new ways to enhance security but also new ways to conduct surveillance on an unprecedented scale. The fight over whether companies should be forced to create "backdoors" into our encrypted devices perfectly captures the deep divide between those who prioritize safety and those who champion privacy.

Ultimately, this is a never-ending negotiation. It’s a dynamic and evolving challenge that will shape the future of our digital lives, constantly requiring us to re-evaluate the balance between staying safe and staying free.

## International Collaboration

Growing importance:

India is central to global cyber governance due to its large digital population, IT sector, and strategic role in geopolitics.

Cybersecurity cooperation intersects with human rights, especially privacy, freedom of expression, and access to information.

ISSN: 2582-6433

Bilateral cooperation:

India collaborates with the United States, European Union, Japan, Australia, and Israel on cyber capacity building, information sharing, and incident response.

Agreements often include commitments on combating cybercrime and protecting critical infrastructure.

Multilateral engagement:

Active participant in UN dialogues, G20 processes, BRICS, and ASEAN cyber initiatives.

Contributes to global debates on responsible state behavior in cyberspace.

Platforms provide opportunities to integrate human-rights safeguards into cybersecurity frameworks.

Operational mechanisms:

CERT-In partners with international Computer Emergency Response Teams for threat intelligence and cyber incident cooperation.

India also engages in joint exercises, training programs, and technical capacity building with foreign agencies.

Human rights challenges:

India's Digital Personal Data Protection Act (2023) and surveillance powers raise concerns about government discretion, data sharing, and individual remedies.

Civil society groups warn against misuse of cybersecurity laws for surveillance or censorship.

## Monitoring and Evaluation

Establishment of Oversight Bodies:

Create independent bodies to monitor the implementation of cybersecurity policies and assess their impact on human rights.

Regular Audits and Assessments: Conduct periodic audits of cybersecurity initiatives to identify gaps, challenges, and areas for improvement.

Feedback Mechanisms: Implement channels for citizens to report grievances and provide feedback on cybersecurity policies and practices.

ISSN: 2582-6433

**Some of the leading case laws relating to Cyber Security and Human Rights are as follows:**

1." Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)" — Right to Privacy

Brief: A nine-judge bench held that privacy is a fundamental right under Articles 14, 19, and 21. Any intrusion (such as surveillance, data collection, or cybersecurity regulations) must pass the tests of legality, necessity, and proportionality.

Relevance to cybersecurity: Sets the constitutional foundation for evaluating state surveillance, digital data processing, and cyber laws.

2. Shreya Singhal v. Union of India (2015) — Online Free Speech

Brief: The Court struck down Section 66A of the IT Act for being vague and overbroad, as it chilled free expression online. It also clarified limits of intermediary liability (under Section 79).

Relevance to cybersecurity: Protects digital freedom of expression and establishes that cyber laws must be precise, proportionate, and not suppress lawful online activity.

3. Anuradha Bhasin v. Union of India (2020) — Internet Shutdowns

Brief: The Court held that indefinite internet shutdowns are unconstitutional. Any restriction must satisfy tests of legality, necessity, proportionality, and must be subject to periodic review. Internet access was recognised as integral to free speech and trade.

Relevance to cybersecurity: Limits government powers to suspend internet services — a key safeguard for human rights in the digital age.

## Conclusion

Balancing cybersecurity and human rights in India is not merely a policy imperative but a moral and constitutional obligation. By adopting a holistic approach that integrates legal reforms, institutional strengthening, technological advancements, and human rights considerations, India can create a secure and inclusive digital ecosystem that serves the interests of all its citizens. This roadmap provides a strategic framework to navigate the complexities of this balance, ensuring that the nation's digital future is both secure and rights-respecting.

ISSN: 2582-6433

## References

•United Nations Office on Drugs and Crime (UNODC). The Global Programme on Cybercrime. (UNODC, 2021).

•Council of Europe. Convention on Cybercrime (Budapest Convention), 2001.

•Human Rights Council, United Nations. The Right to Privacy in the Digital Age. A/HRC/RES/34/7, 2017.

• Bhatia, G. (2017). Offend,

. Neutral: Freedom of speech as guaranteed by the Indian Constitution

• Oxford University Press.

Kshetri, N. (2010). The

global cybercrime industry:

Economic, institutional and strategic perspectives. Springer.

Mathur, N. (2021).

"Cybersecurity and Human Rights in India: Challenges and

Prospects." Indian Journal of Law and Technology, 17(2), 45-62.

• Singh, P., & Singh, R.

(2019). "Data protection and privacy issues in India."

International Journal of Cyber Criminology, 13(1), 1-15.

• The Information

Technology Act, 2000, Government of India.

• India’s Digital Personal Data Protection Act (2023)

• Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., (2017) 10 SCC 1.

• Shreya Singhal v. Union of India AIR 2015 SC 1523

• Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.