Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rishikesh Dave; Publisher – Ayush Pandey

A Holistic Overview of Cyber Laws Pertaining in India

Divyanjali Rathore[a] Anmol Kuldeep Tyagi[b]

[a]Rajiv Gandhi National University of Law, Patiala, India [b]Rajiv Gandhi National University of Law, Patiala, India

Received 18 January 2023; *Accepted* 03 February 2023; *Published* 06 February 2023

When about 4.66 billion people use internet services in a world of about 7.83 billion population, where an ever-increasing number of people all over the world engage with internet databases and use them, it becomes really important to look into their proper functioning and conditioning as a result would help the world grow. This could be done with the help of the right and up-to-date cyber laws and guidelines. This article presents a status-quo overview of the present cyber law situation from the global as well as Indian perspective and aims at going through all the possible trends that might follow up with all these new dynamic technological advancements. The main highlighting part presents a comparative analysis of Indian cyber laws with that of other foreign countries and also presents how after COVID-19 in the year 2021 our world has entered a new phase of Cyber sovereignty wherein every country should move towards more effective cyber jurisprudence and internet freedom. It suggests how India requires a collective effort from the government, service providers as well as users to adopt a synergetic approach towards and use tech-savvy human resources to combat cyber crimes and sustain itself through the evolving cyberland.

Keywords: *internet databases, cyber laws, collective effort, ever-changing and evolving, cyberland.*

INTRODUCTION: BASIC INTRODUCTION TO CYBER LAW

The Law of the Internet is also known as cyber law or IT law. According to the definition of cyber law, it is a legal framework created to address legal issues relating to cyberspace,

computing, and the Internet. Cyber Law is best described as "paper laws" in a "paperless society," which is a fitting beginning.[1]

Intellectual property, contracts, jurisdiction, data protection legislation, privacy, and freedom of expression are all included in the field of cyber law. It controls how information, software, internet security, and e-commerce are distributed digitally. E-documents are given legal legitimacy by the field of cyber law. Additionally, it establishes a framework for electronic commerce and online forms. Therefore, Cyber Law can be easily understood as a legal framework to address cybercrimes. Suitable regulatory practices must be put in place to ensure that there are no malpractices because of the rise in the use of e-commerce. Over 4.66 billion individuals are internet users as of the beginning of 2021. with that figure increasing by 7% per year.[2] Additionally, this indicates that every day there might be about 8,75,000 new users. A safe and secure environment for users is created by the creation and use of strong cyber laws, given the rapid growth in the use of cyberspace.

Cybercrime can be at a personal level, as against an individual, entailing offences such as identity theft for personal gain, online harassment, the sale and distribution of child porn, the tampering with personal data, and the usage of obscene material; or against property, which include the use and dissemination of harmful programs theft of data and information from financial institutions, intruding into cyberspace, computer vandalism, and unlawful possession of digital information; or against the government including Cyberterrorism, deception, intimidation, and the abuse of power against the government and the populace are crimes that fall under this category. This kind of cyberterrorism happens when teams or individuals terrorise official websites. The importance of cyber laws in contemporary circumstances include[3]

- The goal of cyber regulation is to bring individuals who engage in illegal cyber activity to justice.

[1] 'Cyber Law: A Comprehensive Guide for 2021' (*Jigsaw Academy,* 22 June 2022) <https://www.jigsawacademy.com/blogs/cyber-security/what-is-cyber-law/> accessed 11 January 2023
[2] Statista Research Department, 'Internet and Social Media Users in the World 2022' (*Statista*, 20 September 2022) <https://www.statista.com/statistics/617136/digital-population-worldwide/> accessed 10 January 2023
[3] 'Cyber Law: What Is Involved in Cyber Law and Its Importance?' (*EDUCBA*, 31 May 2021) <https://www.educba.com/cyber-law/> accessed 12 January 2023

- These issues, including cyberbullying, attacks on other websites or people, record-stealing, disruption of every company's online operation, and other criminal behaviours, must be dealt with in court.
- When someone breaks a cyber law, action is taken against them based on the type of cyber law they broke, where they live, and where the law was broken.
- Since most cyber crimes are more serious than felonies and are not typically crimes, prosecuting or expelling hackers is of utmost importance.

APPLICABLE CYBER LAWS IN INDIA

Cybersecurity is a concern for every government in the globe, including that of our nation. India must accept responsibility for the growing number of cyber security concerns it is particularly confronting. An investigation of worldwide cybercrime by the Economic Times found that cyberattacks cost the government roughly Rs. 1.25 lakh crore annually.[4] According to their nature and the amount of harm they do to the victim, cybercrimes may typically be divided into numerous sorts, however, the primary ones that are now prevalent and at their height in India include hacking, matrimonial Frauds, Salami attacks, Cyber Stalking, Cyber defamation, Banking Fraud as well as Cyber Terrorism. Cyber laws in India are especially important in nations like India, where the internet is widely utilised. Strict cyber laws serve the objective of regulating the electronic exchange of data, software, security, and financial activities; When it comes to cybersecurity, there are four main cyber laws to cover:

Information and Technology Act, 2000 - The Information Technology Act, written in 2000, overseas Indian cyber law. This Act's main motivation is to provide trustworthy legal inclusion for eCommerce by making it easier to register real-time information with the government. some of the important sections under the ITA act are section 43 which applies to those who harm computers without the owner's authorization, section 66 whenever a person is seen dishonestly committing things under section 43, section 66B includes the penalties for receiving computers

[4] 'Cyber Crimes in India Caused Rs 1.25 Lakh CR Loss Last Year: Official' (*The Economic Times*) <https://economictimes.indiatimes.com/tech/tech-bytes/cyber-crimes-in-india-caused-rs-1-25-lakh-cr-loss-last-year-official/articleshow/78773214.cms> accessed 11 January 2023

or communication equipment that have been taken fraudulently, section 66C examines the identity frauds associated with fake digital signatures, compromised passwords, or other distinguishing identification characteristics and section 66D was added as needed and focuses on penalising cheaters who use computer resources to impersonate others. All of these sections ascribe respective penalties and punishments for defaulters.

Indian Penal Code, 1860 - Invoked in conjunction with the Information Technology Act of 2000, the Indian Penal Code (IPC), 1860, defines identity theft and related cyber offences. The IPC's most pertinent sections address cyber frauds: Forgery (Section 464) (Section 464) Planned forgery used to cheat (Section 468) falsified records (Section 465) presenting a fake paper as a real one (Section 471) reputational harm (Section 469).

The largest misunderstanding ever over the simultaneous application of the Indian Penal Code, 1860 and the Information and Technology Act, 2000 regarding cybercrimes is now present before the Honourable Judiciary regarding which among the available laws would be applied as some of the IT Act provisions are far more forgiving than the severe provisions of the Indian Penal Code. This ambiguity was removed by the Hon'ble high court of Bombay by relying on the decision of The hon'ble Supreme court in the case *Sharat Babu Digumar v NCT of Delhi* [5], wherein it was held that Given that *we have a special law in the form of the IT Act for specifically containing and preventing cyber crimes, prosecuting the petitioners under the IPC and IT Act at the same time would be a flagrant violation of protection against double jeopardy. As a result, prosecution under both laws for the same offence is unconstitutional.*

Companies Act of 2013 - The Companies Act of 2013 is cited by business stakeholders as the legal need required for streamlining everyday operations. The requirements of this Act's directives solidify the necessary techno-legal compliances, putting less compliant businesses in a problematic legal situation.

[5] 'Framework Documents' (*NIST*, 9 November 2022) <https://www.nist.gov/cyberframework/framework-documents> accessed 11 January 2023

NIST Compliance[6] - As the most trustworthy worldwide certifying organisation, the National Institute of Standards and Technology (NIST) has authorised the Cybersecurity Framework (NCFS), which offers a unified approach to cybersecurity.

SCOPE AND COMPARISON WITH OTHER COUNTRIES

Fraud, identity theft, and other forms of cybercrime have increased dramatically in recent years. However, the laws that are already in place do not adequately or completely address it. Additionally, we anticipate seeing a deeper penetration of cybercrime in India. This underlines the significance of creating stronger legal mechanisms for cybercrime that are both effective and deterrent. Undoubtedly one of the most anxiously awaited developments in Indian cyber legislation is the National Cyber Security Strategy. This strategy aims to be both a continuation of the National Cyber Security Policy of 2013 and a comprehensive set of guidelines for people, decision-makers, and other stakeholders.

The plan will probably provide more insight into the best response techniques for enhancing government cyber security. India will need to start working on a separate national cyber security law very soon. The need for such a law is critical since it will be a critical weapon for safeguarding India's cyber security and cyber sovereign interests. India is slightly behind the curve at a time when many other countries have already begun enacting specialised cybersecurity legislation. Appropriate action is required in this regard. Hopefully, the government will focus on more effective measures to tackle cybercrime in the future. It is also hoped that more relevant reforms in Indian cyber law will be made to include enabling legal measures to address the difficulties posed by rapidly emerging technologies.

India has to start crafting its own national cyber security law right away. Such a law is urgently required since it would be an essential instrument for protecting India's online sovereignty and cyber security. India is a little behind the curve at a time when many other countries have already begun enacting specialised cybersecurity legislation. In this regard, suitable action is required. Hopefully, the government will focus on tactics that combat cybercrime more

[6] *Ibid*

effectively in the future. It is also hoped that other relevant modifications would be made to Indian cyber law, such as allowing for legislative measures to address the problems brought on by rapidly advancing technology.

Cyber Laws of Australia

The following are examples of cybercrime offences covered by Commonwealth law under sections 10.7 and 10.8 of the Criminal Code Act of 1995[7]:

- Internet incursions;
- Data alteration without authorization, including data erasure;
- Unauthorised interference with digital communications, such as denial-of-service attacks;
- The development and dissemination of harmful software (for example, malware, viruses, ransomware);
- Collecting or trafficking personal financial information dishonestly.

Australian cyber laws include the Australian Privacy Principles (APP) which regulate personal information, the Cybercrime Act which regulates computer and internet-related offences, the Spam Act which regulates commercial email and others and the Telecommunications (Interception and Access) Act to protect the privacy of individuals. It also has many guidelines by various industry verticals[8]

Cyber laws of the USA

The amount of cyberattacks and cybercrimes in the United States is now the greatest in the world.[9] American cybersecurity laws are highly complicated; each federal agency must adhere

[7] 'Cyber Crime' (*Australian Federal Police,* 16 November 2022) <https://www.afp.gov.au/what-we-do/crime-types/cyber-crime#:~:text=Cybercrime%20offences%20are%20found%20in%20Commonwealth%20legislation%20within,Dishonestly%20obtaining%20or%20dealing%20in%20personal%20financial%20information> accessed 13 January 2023
[8] Agarwal H, 'A Glance at Australia's Cyber Security Laws' (*Mobile Application Security Testing Company,* 28 April 2021) <https://www.appknox.com/blog/glance-australias-cyber-security-laws> accessed 13 January 2023
[9] 'Federal Laws Relating to Cybersecurity: Overview of Major Issues ...' (*SGP*) <https://sgp.fas.org/crs/natsec/R42114.pdf > accessed 12 January 2023

to its own set of rules, and there are several industry-specific cyber laws for vital infrastructure. Some of the laws governing cyber laws of the USA are The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 Regulating fraud, The Computer Security Act of 1987 for developing healthy and safer systems, The paperwork Reduction Act of 1995 for better policies, The Homeland Security Act of 2002 making home security responsible for developing cyber security standards, The Cyber Security Research and Development Act of 2002 provides guidelines for regulation and the government is also introducing some new guidelines and amending the old ones to keep up with the pacing world.[10]

Cyber Laws of the United Kingdom

In the UK, there is no overarching law that regulates cybersecurity or information technology, and each agency is governed by a specific law, such as the Security Services Act of 1989 or the Civil Contingencies Act of 2004[11]. Therefore, executive agencies charged with ensuring cybersecurity have a lot of latitude in creating various cybersecurity strategies. After being established in 2009, the Office of Cyber Security evolved into the Office of Cyber Security and Information Assurance (OCSIA) in 2010. The General Data Protection Regulation ("GDPR") and the Network and Information Security Regulations of 2018 are the most current legal provisions that are relevant to enterprises in the United Kingdom (the "NIS Regulations").[12]

The Computer Misuse Act of 1990, the Communications Act of 2003, the Privacy and Electronic Communications (EC Directive) Regulations of 2003, the FCA Handbook, the PRA Rulebook, and the common law tort of misusing private information are additional laws and regulations that may be pertinent. The GDPR and the 2018 Act compel private businesses in the UK to take strict security measures to avoid data security breaches by third parties[13]. They also urge the private sector to enable and maintain more cyber-hygienic systems to prevent cybercrimes.

[10] Agarwal H (n 8)
[11] *Ibid*
[12] 'India UK Legal Regulatory Approaches' (*CIS-India*) <https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf> accessed 14 January 2023
[13] John Timmons & Paul Pittman, 'Cybersecurity and the UK Legal Landscape' (*White & Case LLP*, 1 May 2019) <https://www.whitecase.com/insight-alert/cybersecurity-and-uk-legal-landscape> accessed 15 January 2023

Additionally, it puts cybersecurity rules on all businesses that offer basic services including health, internet commerce, transportation, etc.

To conclude, the expansion and development of electronic networks are closely tied to the long-term progress and expansion of our society, and we must promote raising attention to this phenomenon. The next war will be fought virtually rather than on battlefields. All governments must take the appropriate steps to create an intergovernmental accord on cyber deterrents. We must now see the entire internet network as a massive family and work further towards everyone's betterment and peaceful cohabitation.[14]

INDIA'S STANCE ON THE CYBER SITUATION 2021 AND THE GOLDEN ERA OF CYBERCRIME

Ransomware is malware that uses encryption to hold a victim's data hostage for a fee. The critical data of a user or organisation is encrypted, making it impossible for them to access files, databases, or applications. A ransom is then demanded to gain access. Ransomware is frequently designed to spread across a network and target repository and file servers, paralysing an entire organisation in a matter of minutes. It is a growing threat, generating billions of dollars in fees to cybercriminals while causing significant damage and expense for businesses and governments.[15]_ENISA (European Union Agency for Cybersecurity) released its ENISA Threat Landscape (ETL) report, which covered cybercriminal activity between April 2020 and July 2021. The results of the study were rather worrisome, as they foreshadow an increase in cybercrime, particularly those motivated by the revenues of ransomware attacks.[16]

Even though the paper warned that many various cybersecurity threats were on the rise, ransomware happens to be the "prime threat" that organisations would face, with a 150% increase in ransomware attacks during the reporting period. And there were concerns that,

---

[14] JusCorpus, 'Comparison of Cyber Laws of India with US & UK' (*Jus Corpus,* 29 July 2022) <https://www.juscorpus.com/comparison-of-cyber-laws-of-india-with-us-uk/#_ftn7> accessed 15 January 2023

[15] 'What Is Ransomware?' (*Trellix*) <https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html> accessed 9 January 2023

[16] Panduru D, 'The Ransomware Threat in 2021: We're Facing the 'Golden Era' of Cybercrime, New Report Reveals' (*ATTACK Simulator,* 23 February 2022) <https://attacksimulator.com/blog/enisa-warns-of-ransomware-threat/> accessed 16 January 2023

despite the attention of world powers, the ransomware problem would worsen before it improves.[17]

"*We are observing the golden era of ransomware -- it has become a national security priority -- and some argue that it has not yet reached the peak of its impact*," the paper warned.[18]

The reason why it is difficult to find the perpetrator of ransomware is that it is a type of malware that is cryptographically secure to hold a victim's data hostage in exchange for a fee. A user's or organisation's critical data is encrypted, thereby rendering it impossible for them to access files, databases, or applications. To gain access, a ransom is demanded. Ransomware is quite often constructed to spread across a network and target databases and file servers, effectively paralysing an entire organisation in minutes. It is a growing threat that earns cybercriminals billions of dollars in fees while causing significant harm and expense to businesses and governments.[19]

RECENT LAWS AND HAPPENINGS IN THE FIELD OF CYBER LAW

2021 had been quite a busy year in terms of cyber legal development in India. Like the rest of the world, India has also survived the pandemic. In 2021, a second wave of deadly infections will wreak havoc, and towards the end of the year, we saw the dramatic spread of the Omicron variant of Covid-19, raising many concerns and issues related to its further spread.[20]

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: 2021 kicked off with some dramatic developments for one of the largest social media service providers. WhatsApp has decided to unilaterally change its privacy policy and urged all Indians to abide by the aforementioned privacy policy if they wish to continue to enjoy the

[17] 'Ransomware: It's a 'Golden Era' for Cyber Criminals - and It Could Get Worse before It Gets Better' (*ZDNET*) <https://www.zdnet.com/article/ransomware-its-a-golden-era-for-cyber-criminals-and-it-could-get-worse-before-it-gets-better/> accessed 10 January 2023
[18] *Ibid*
[19] 'What Is Ransomware?' (*Trellix*) <https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html> accessed 9 January 2023
[20] 'Indian Cyber Law Developments in 2021' (*Cyberlaw University*, 6 January 2022) <https://cyberlawuniversity.com/indian-cyberlaw-developments-in-2021/> accessed 10 January 2023

benefits of the WhatsApp platform. It caused a stir, and as a result, WhatsApp decided to suspend enforcement of its amended privacy policy. However, this unilateral action by the service provider had different consequences. is made under Section 87 of the Information Technology Act, 2000, and constitutes a secondary law under the Indian Cyber Law. However, these rules are fundamentally different from the others. The main reason is that for the first time, these rules had a deterrent effect and came into effect when an intermediary failed to comply with the parameters of his 2021 IT Regulation.

Intermediary Liability under Rule 7 of the IT Rules, 2021: Rule 7 of the IT Regulations 2021 provides two specific examples of legal hazards. Rule 7 states that if an intermediary fails to comply with the provisions of his IT Regulation 2021, he loses the statutory exemption from liability granted under section 79 of the IT Act 2000. The 2021 IT Regulations stipulate that waivers of statutory indemnification for intermediaries are by operation of law. A second serious legal ramification of not complying with IT regulations was that the management of intermediaries could be held liable for various violations under the Information Technology Act, 2000, and the Penal Code of India. Hence, for the first time in the history of Indian cyber law, a chilling message that by the statutory deadline, he must be prepared to face criminal penalties as an intermediary if he fails to comply with IT Regulation 2021. was issued to intermediaries from India. Nevertheless, the IT Regulation 2021 has taken an important step in India's definitive approach to this whole issue of intermediary liability.

Golden Age of Cybercrime: With the advent of Covid-19, the golden age of cybercrime has already begun. India has recognized a trinity of cybercrime as the top three cybercrimes during the Covid-19 era were phishing, identity theft, and online financial fraud. Jamtara's cybercrime model also boomed in 2021, with small neighbourhoods, small villages, or small communities banding together to engage in cybercrime and make quick money. However, India's decisive approach to combating and regulating the growing cybercrime phenomenon has been hampered by the lack of an effective legal framework to combat cybercrime. We also found that the existing provisions of the Information Technology Act 2000 and the Indian Penal Code were grossly inadequate to deal with these emerging cyber crimes in India during the 2021 pandemic.

It is clear that the time has come for India to establish a dedicated legal framework to regulate cybercrime.

Need for Data Privacy Laws: India also needs to address the peculiar vacuum that currently exists in India in terms of the lack of digital privacy laws. We need digital privacy laws to be protected.

Growing Menace of Fake News: Overall, 2021 has been a great year. It was the year of the pandemic that fake news surged in India. No wonder the pandemic has become known as the "infodemic". Also, India did not have laws on fake news, making it even more difficult to control the growing threat of fake news. Some elements of fake news should be addressed under the 2021 IT Regulations, but clearly, that wasn't enough. Meanwhile, the whole fake news phenomenon continues to change the way Indians generate and distribute disinformation and disinformation.

CONCERNS AND NEED FOR INITIATIVES

2021, the year of the pandemic, has taught us that the future of cyberspace is a very bright yet still uncertain one. All digital players need to hone their digital skills to be well prepared for the special challenges of the cyberspace of the future. [21] Overall, 2021 has been a very exciting year in terms of the development of cyberspace and cyber law in India. The development of Indian cyber law in 2021 will be the foundation for the further development of Indian cyber law in the future. Cyberlaw is an ever-evolving paradigm globally and especially in India, and it will be interesting to see how new developments in this evolving paradigm of cyberlaw play out in the future.[22]

[21] *Ibid*
[22] *Ibid*

CYBERLAW TRENDS: GLOBAL TRENDS ON CYBER LAWS

This is because cyberspace is increasingly dynamic, and technological advances are being introduced with new and distinct challenges.[23] Some of the major and important trends in global cyber laws are:

Cybersecurity: According to studies, cybersecurity will be focused on a lot in the year 2022. Cybersecurity has de facto become the first matter of concern for all relevant parties in the digital ecosystem, and this position will be further centralized and bolstered in 2022. There is no single international law that governs cybersecurity. There isn't even a single international cyber law.

Ransomware Attacks: Ransomware attacks have and will continue to grow in frequency. According to studies, every 11 seconds, one company from around the world becomes a victim of a Ransomware attack, and from reports by 2022, this situation is likely to worsen. As a result, it is expected that nation-state actors will develop cyber legal frameworks to address the unique challenges of Ransomware.

Cybersecurity Reporting: National cybersecurity reporting mechanisms must be strengthened further. Several countries have already enacted legislation requiring stakeholders to report any vulnerabilities and data and cybersecurity breaches. This particular trend is expected to consolidate further in 2022.

Cybercrime: In addition, the year 2022 is likely to see the unification of the Golden Age of Cybercrime. In the year 2022, cybercrime will continue to grow and evolve into new manifestations and avatars. As a result, countries around the world are likely to be pushed to reconsider not only their national cybercrime laws but also to make them more effective and efficient in these ever-changing cybercrime paradigms. The economic loss that the world is currently facing as a result of cybercrime and cybersecurity breaches is phenomenal, and these loss figures will continue to rise. As a result, more nation-states are likely to develop new

[23] 'Cyberlaw Global Trends in 2022' (*Cyber law- The New Legal Discipline*) <https://cyberlaws.net/cyberlaw-global-trends-2022/> accessed 15 January 2023

mechanisms in 2022 to reduce the potential losses caused by cybercrime to the cyber data economy as a whole.

Artificial Intelligence: The year 2022 was also expected to see a significant push in the evolution of legal jurisprudence concerning Artificial Intelligence. Already in 2021, the European Union introduced the Draft Artificial Intelligence Law, which was then being debated. This potential draft could serve as the foundation for further development of cyber legal jurisprudence concerning artificial intelligence in 2022. Furthermore, different countries are likely to work on artificial intelligence legal principles in 2022.

Metaverse: In the year 2021, we also saw the significant emergence of the Metaverse. In the year 2022, we were to see further proliferation, growth, and consolidation of the Metaverse as a notion. As the Metaverse becomes more real, stakeholders around the world will be increasingly asked to address legal policy and regulatory matters about the Metaverse at large in the year 2022. We are likely to see some legal advancements in Metaverse law judicial review in the year 2022.

Blockchain Technology: Blockchain as a technology has continued to evolve at a very fast pace in 2022. More modern nation-states could be pushed towards creating legal frameworks and regulations for blockchain and crypto ecosystems. May create a legal framework. While there is much debate around the world over whether cryptocurrencies should be legally sanctioned, various countries have already taken their approaches to this. The jurisprudence should be further developed.

Darknet: In 2022, the darknet could grow even more as a paradigm. Therefore, legal. policy and regulatory issues related to the dark web must be properly addressed. As more and more stakeholders migrate to the dark web, sovereign governments can no longer turn a blind eye to the growing importance of the dark web. Appropriate new legal frameworks should therefore be put in place to regulate some aspects of the activities that take place on the dark web

Data Protection Laws: In 2022, we saw increased activity in the area of data protection. Other countries are expected to enact laws that promote data protection.

TRENDS IMPACTING INDIA'S PLANS REGARDING CYBER LAWS

Cyber-attacks in India have increased during the pandemic and this trend is likely to continue as the newly distributed workforce provides opportunities for criminals to exploit. It is expected to grow to $3.05 billion by 2022, with investments by organisations[24]. Here we take a look at some trends that will impact the Indian cybersecurity sector in the coming year.

Cybercriminals will take advantage of weaknesses brought forth by the pandemic: During the pandemic, organisations around the world have increasingly relied on increasingly powerful technological approaches to build business resilience. Threat actors continue to exploit vulnerabilities that organisations find difficult to remediate due to their increasing complexity to their advantage. In other words, 2022 is expected to look similar to 2021 in terms of notable and sensational exploits.

Cyber threats, such as ransomware, will continue to increase: The IT world was in turmoil. People started working from home at night and had to work out on a large scale and there was a boom in performance without any prior warning. We all know attackers like chaos. More network disruption means more and more successful cyberattacks.

Automation helps to improve endpoint security: New remote workers have become an easy target for attackers, completely replacing traditional antivirus solutions and adopting the concepts of Extended Detection and Response (XDR) and Endpoint Detection and Response (EDR) to create advanced and sophisticated antivirus solutions. Protect your endpoints from threats. Traditional security analytics solutions such as Security Information and Event Management (SIEM) evolve into tools that leverage AI and ML concepts for security automation and orchestration.

Interest in a Zero-trust security model: As one of the most important security frameworks, the acceptance of Zero-Trust architecture by Indian businesses is increasing. By implementing

[24] Sawhney R, 'Trends Impacting India's Cyber Security Sector in 2022' (*BW Businessworld*) <https://www.businessworld.in/article/Trends-Impacting-India-s-Cybersecurity-Sector-in-2022/03-01-2022-416458/> accessed 12 January 2023

strategies such as Zero Trust Network Access (ZTNA), micro-segmentation, and IoT security, organisations can leverage a variety of processes and technologies to implement a user-to-user, machine-to-machine, and application-to-application Zero Trust approach. support. - Applications, or user-to-user applications, secure communications.

Cybercrime is a top concern in every country as it not only undermines trust in governments but also undermines people's trust in their daily transactions. With the increased use of digital technology, cyber law is experiencing several new trends. These various trends include spam laws, cloud computing and rights, social media and major issues, mobile law challenges, cybersecurity legal issues, and more. to an increase in cybercrime. Even law enforcement officers may not be well-trained to fight cybercrime. Most cyber threats have complex behaviour that slows understanding, making them difficult to contain in the early stages of a cyberattack. Such attacks have had a profound impact on Indian society. India can tackle the problem of cybercrime by taking a synergistic approach with a well-trained workforce in a tech-savvy society.[25]

CYBER SOVEREIGNTY, A TREND OF 2022

"Cyber-sovereignty, otherwise called internet freedom, is a phrase describing the government to exercise control over the internet within their boundaries including economic, political, cultural and technological activities."[26] 2022 happened to be a pivotal year in terms of the growth of cyber sovereignty as a concept.[27] Countries were and are increasingly concerned that their sovereignty extends not only to their borders but also to cyberspace. Other countries had enacted various domestic laws to further expand the scope of cyber sovereignty and address the sovereignty, security, and integrity of their respective nation-states in both the physical world and cyberspace. In 2022, states and nations adopted different laws of their own, which had a

[25] 'Emerging Trends of Cyber Law in India – Legge Rhythms' (*Leggerhythms*) <https://leggerhythms.org/emerging-trends-of-cyber-law-in-india/> accessed 14 January 2023
[26] Moharana KK, 'Manupatra' (*Articles,* 29 May 2018) <https://articles.manupatra.com/article-details/Cyber-Sovereignty-in-Indian-Context> accessed 10 January 2023
[27] 'Cyberlaw Global Trends in 2022' (*Cyberlaw- The New Legal Discipline*) <https://cyberlaws.net/cyberlaw-global-trends-2022/> accessed 15 January 2023

few implications for further strengthening and expanding the concept of cyber sovereignty for each state going forward.

The list mentioned above is some of the more significant cyber rights trends we saw globally in 2022. Of course, the list is not exhaustive. This is just an example list. But one thing is very clear, 2022 was built on the massive developments in cyber case law that happened around the world in 2021. 2022 was expected to be extremely busy with emerging cyber jurisprudence. The emergence of new technologies further complicated the whole scenario. 2022 also ushered in an era in which digital stakeholders and policymakers were increasingly called upon to address a range of complex legal issues related to current and emerging technologies that have distinct implications for activity in cyberspace. Overall, 2022 promises to be an exciting year in terms of continued growth and development of global cyber law.[28]

CONCLUSION

Although it is believed that India's cyber legal framework meets the needs of the moment, it has several shortcomings. The cybersecurity frameworks of some industry authorities, in particular, need to be updated to keep up with the rapid changes in technology. The Indian government is developing new policy frameworks in response to this necessity to maintain the aforementioned developments. The provisions of this new policy framework are deemed sufficient to withstand the challenges presented by these developing trends. After all, India is one of the most likely targets for cybercriminals, as can be seen from precedent, thus the effectiveness of these rules depends on their careful and corruption-free execution by the relevant authorities. The United States of America, although having several policies and statutory frameworks to assure cybersecurity, struggles with the proper application when these present and prospective cyber laws are compared to those of some other nations[29]. All of these nations also exhibit a pattern of inadequate policy frameworks for certain industries, such as the health sector, the insurance industry, and private companies. Additionally, severe enforcement of carefully crafted

[28] Emerging Trends (n 25)
[29] 'Centre for Academic Legal Research | Journal of Applicable Law ...' (*CALR*) <https://calr.in/wp-content/uploads/2021/04/Cyber-Laws-_-Comparative-Study-of-Indian-and-Foreign-laws.-1.edited.pdf> accessed 10 January 2023

regulations must be used in all cases, including those involving India, or else the policies will be ineffective.

Cybersecurity regulations need to be updated and improved continually in India and throughout the world as human dependence on technology grows. In addition, the pandemic has increased the demand for app security by forcing a large portion of the workforce into a remote working mode. To stop the impostors at their onset, legislators must go above and beyond to keep one step ahead of them. Cybercrime can be reduced, but it requires coordinated actions from the government, Internet service providers, intermediaries like banks and online retailers, and, most crucially, end users[30]. Online safety and resilience can only be achieved by these stakeholders making cautious efforts and adhering to the rules of Cyberland.

[30] Agarwal H, 'Cyber Laws in India: Cybersecurity Crime Laws & Regulations' (*Cyber Laws in India | Cyber Security Crime Laws & Regulations,* 12 January 2023) <https://www.appknox.com/blog/cybersecurity-laws-in-india> accessed 12 January 2023