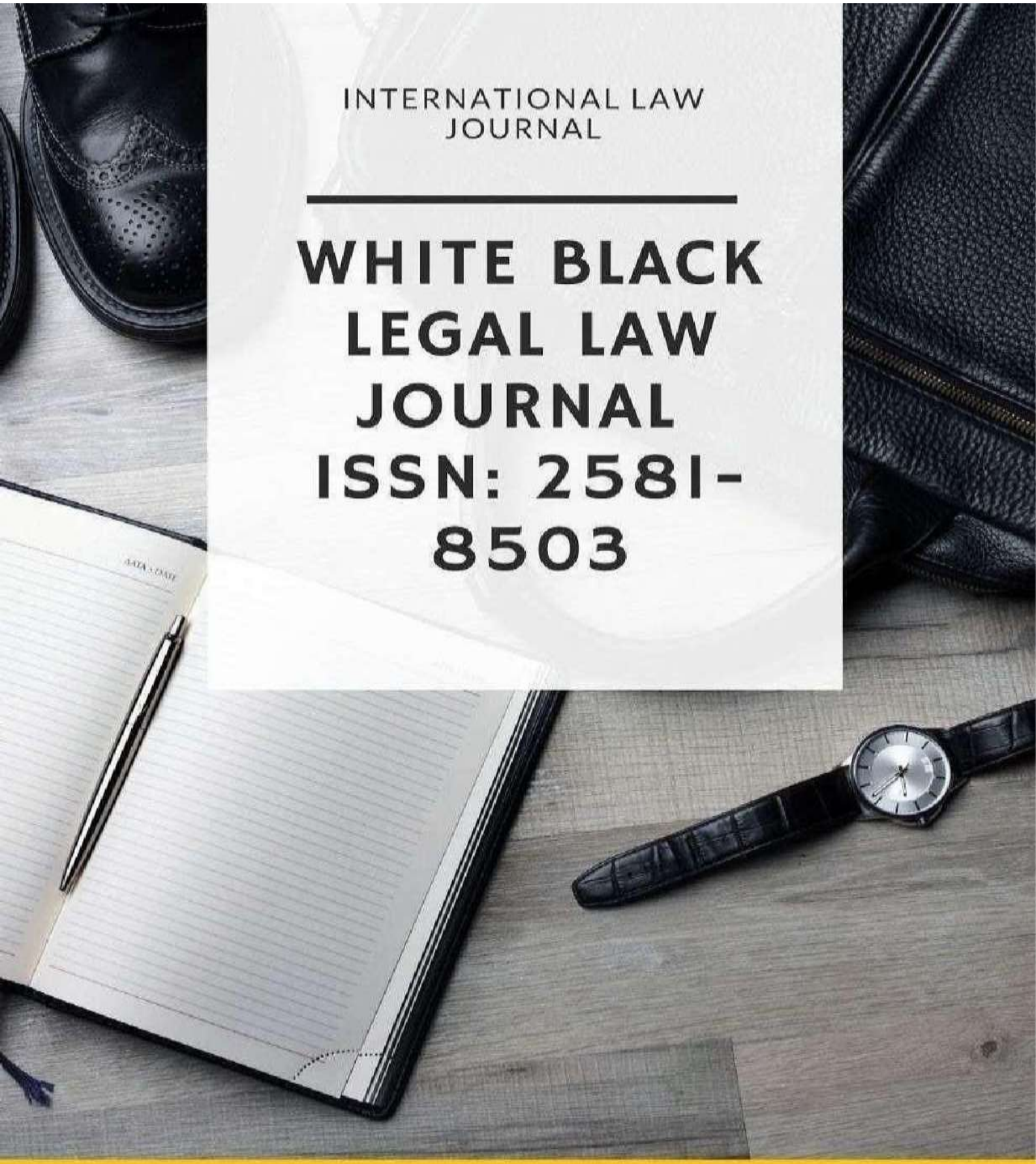

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

CYBER LAW: AN OVERVIEW OF CYBER LAWS IN THE INTERNATIONAL COMMUNITY AND WITHIN INDIA

AUTHORED BY: PRIYANSH RAJ SINGH SENGER
B.A.LL.B., 5th year
Ramaiah Institute of Legal Studies, Bangalore 560054

CO-AUTORED BY: SIDDHARTH MISRA
B.A.LL.B., 5th year
Ramaiah Institute of Legal Studies, Bangalore 560054

INTRODUCTION

Crime is as old as human civilization. Our age old books and stories are described with the crimes perpetrated by people and rebuffed likewise to the laws of the than culture. The Idea of these crimes changes as society developed and moved forward. In the present techno-shrewd climate, the world is turning out to be increasingly more carefully modern as are the violations. Internet was at first evolved as a researching and data sharing subject and was in an unregulated way. As the time passed by it became more transactional with e-business, e-commerce, e- governance etc., so did the transactions and the crimes as well like that of Online job fraud, Online sextortion, Child pornography or Child Sexually Abusive Material [1](CSAM), Cyberbullying, Cyberstalking, Cyber grooming, Phishing, Vishing, Smishing, Credit card fraud or debit card fraud, Impersonation, Identity theft and to name a few.

The well-defined field of law known as "Internet Law" offers guidelines to users regarding appropriate online behavior. Cyber laws are classified into two categories: criminal laws and civil laws. Cyber law is any legislation or regulation pertaining to the use of computers, smartphones, the internet, and other connected technology by individuals.

[1] Siegle, Del. "Cyberbullying and sexting: Technology abuses of the 21st century." *Gifted child today* 33.2 (2010): 14-65.

Sussman and Heuston [2]first proposed the term "Cyber Crime" in the year 1995 as "*Cybercrime cannot be described as a single definition, it is best considered as a collection of acts or directs."* The internet is the term for the virtual domain that exists on the web. Cyber Laws, which regulate this domain, apply to all residents of cyberspace since they have a sort of universal authority over it. Because it covers nearly every facet of transactions and activity using the internet, World Wide Web, and cyberspace, cyberlaw is important.

Cyberlaw encompasses laws relating to domains such as Cybercrimes, Electronic and digital signatures, Intellectual property, Data protection and privacy and a number of others which include crypto currency and Non-fungible Tokens (NFTs) which are in their developing stage in the terms of the legal procedures which are still unexplored in the legal domain.

BACKGROUND

The trailblazer in the space of Cybercrimes is, Donn B. Parker[3], a senior computer security consultant at the Stanford Research Institute in the United States. His journey with computer crime and cyber security started in the early 1970s; his first book on the subject was Computer Crime published in 1976. Parker was additionally the lead creator of Computer Crime: Criminal Justice Resource Manual (1979), the primary fundamental US government manual. In 1982, the Organization of Economic Co-operation and Development [4](OECD) appointed an expert committee, the Information and Computer Communication Policy[5] (ICCP) Committee, to discuss computer-related crimes and the need for changes in the legal systems. This committee presented its recommendations in 1986, stating that, given the nature of cyber crime, it was highly desirable to forge some form of international cooperation to reduce and control such activity. Likewise, it suggested that the nations under the banner of the United Nations change their corrective regulation to cover digital wrongdoings (OECD[6], 1986).

---

[2] Sabillon, Regner, et al. "Cybercriminals, cyberattacks and cybercrime." *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*. IEEE, 2016

[3] Parker, Donn B. "Computer Crime: Criminal Justice Resource Manual." (1989).

[4] Outlook, OECD Economic. "Organization for Economic Cooperation and Development." Paris, France (2001).

[5] Kimbel, Dieter. "Policy research for information activities: The OECD programme on information, computers and communications policy." Telecommunications Policy 1.5 (1977): 367-373

[6] Supra 4

At the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders held in Havana, a pivotal resolution was adopted, addressing the escalating challenge of computer-related crime. This resolution stands as a testament to the international community's recognition of the pressing need for concerted efforts in combating cyber threats. In light of the dynamic and ever-evolving nature of cyberspace, the United Nations, through this resolution, aimed to provide a framework for nations to formulate judicious legislation and policy directives.

The UNCITRAL Model Law on Electronic Commerce was developed in 1996 by the United Nations Commission on International Trade Law (UNCITRAL)[7]. Its goal is to make it easier for people to use contemporary communication and information storage methods. It is predicated on the creation of an electronic medium that serves as a functional equivalent for paper-based concepts like "writing," "signature," and "original."

The Council of Europe Convention on Cybercrime (Budapest Convention) [8]which came in 2001 is one and only multilateral agreement on the subject of cybercrime. The Convention is the first international treaty on crimes committed via the internet and other computer networks, particularly infringing copyright, computer-related fraud, child pornography, and network security violations along with a series of powers and procedures such as the search of computer networks and interception. Its principal level head, set out in the prelude, is to seek after a typical criminal strategy to safeguard society against cybercrime, particularly by taking on proper regulation and cultivating global collaboration. The Budapest Convention went into force on January 7, 2004.India has a very point by point and clear cut general set of laws set up. Notwithstanding the splendid keenness of our drafters of such laws, the prerequisites of the internet could scarcely at any point be expected. In that capacity, the approaching of the Web prompted the development of various sensitive legitimate issues and issues which required the authorization of Digital regulations. The Information Technology Act is a result of the goal dated 30th January 1997 of the United Nations, which took on the Model Regulation on Electronic Business, embraced the Model Regulation on Electronic Commerce on International Trade Law. This goal suggested, entomb alia, that all states give ideal thought to the

[7] Rules, UNCITRAL Arbitration. "United Nations Commission on International Trade Law (Uncitral)." General Assembly Resolution. Resolution 31 (1976): 98

[8] Wicki-Birchler, David. "The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?" International Cybersecurity Law Review 1 (2020): 63-72

said Model Regulation while updating sanctioning new regulation, so consistency might be seen in the regulations, of the different digital countries, material to choices to paper based techniques for correspondence and capacity of data.

However, the Indian Information Technology Act, 2000 has charged *Computer Emergency Response Team* (**CERT**)[9] to cooperate and collaborate with organizations within and outside the country. CERT being directly under the administrative control of the Ministry of Communications and Informational Technology does not have any operational independence or discretion to cooperate unless approved by the Government therefore it acts upon the direction of its master, which is the Government of the day. This vastly reduces the organizational utility of CERT when it comes to prosecuting international cybercrimes, in collaborating on information sharing and coercive interception of networks/computers, as an organization of national importance.

CHALLENGES SURFACED

In the year 2008, Sergei Nicolaevich Tsurikov[10] was sentenced to eleven years, three months in prison, with three years of supervised release, for his involvement in a complex scheme that defrauded a credit card processor of over $9.4 million. The indictment, issued nearly five years prior, detailed Tsurikov's role in conspiring to commit wire fraud and computer intrusion.

In November 2008, Tsurikov and his accomplices gained unauthorized access to RBS WorldPay's computer network, in the Royal Bank of Scotland Group PLC, payment processing division which came under the United States of America. Employing advanced hacking techniques, they breached the data encryption safeguarding customer data on payroll debit cards. Exploiting compromised accounts, the group used 44 counterfeit payroll debit cards to withdraw $9 million from ATMs across 280 cities globally within 12 hours.

To conceal their activities, the hackers attempted to destroy data on the card processing network. RBS World Pay promptly reported the breach, aiding the subsequent investigation. Tsurikov, extradited to

[9] Bada, Maria, et al. "Computer security incident response teams (CSIRTs): An overview." The Global Cyber Security Capacity Centre (2014)
[10] Kadlecová, Lucie. "Russian-speaking cybercrime: reasons behind its success." Eur Rev Organised Crime 2.2 (2015): 104-121.

the U.S. in August 2010, pleaded guilty in September 2012. He monitored fraudulent ATM withdrawals in real time during the cashout. The sentence includes restitution of $8,400,000. The FBI and U.S. Secret Service, with international law enforcement collaboration, investigated this cybercrime case.

Similarly, an 18-year-old hacker named Arion Kurtaj[11] from Oxford, who is autistic, was a key member of the notorious Lapsus cyber-crime gang. The firms like the Uber, Nvidia and Rockstar Games have lost nearly $10m under this gang's attacks. Kurtaj leaked clips of a forthcoming Grand Theft Auto (GTA) game and was sentenced to an indefinite hospital order.

Cybercrime acts show a broad distribution across the range of offences. According to the perceptions of law enforcement institutions, financial-driven acts, such as computer-related fraud or forgery, make up around one third of acts across almost all regions of the world. A number of countries mentioned that 'fraud in electronic commerce and payment', 'fraud on auction sites such as ebay,' 'advanced fee fraud', 'cybercrime targeting personal and financial information' and 'fraud scheme through email and social networking sites' were particularly prevalent.

CYBER LAWS AROUND THE GLOBE

Today in the age of computers, smartphones and the use of the internet and technology in all walks of life has inevitably led to an increase in cybersecurity concerns around the globe, all the countries are trying to have a safer cyber ecosystem and facilitate better international trade and e- commerce activities, here is an overview of cyber laws in western countries such as

a) **UNITED STATES OF AMERICA**: The United States of America is facing the highest number of cyber-attacks and cybercrimes in the world today the legislation which covers cybersecurity concerns are quite complex in America, each federal agency has its own cybersecurity regulations to be followed and there are many sector-specific cyber laws for critical infrastructure. Moreover, the legislation covers a large number of federal as well state

[11] Tidy, Joe. "Lapsus$: GTA 6 Hacker Handed Indefinite Hospital Order." BBC, BBC News, 21 Dec. 2023, https://www.bbc.com/news/technology-67663128.

laws. Some noteworthy provisions are in the following acts[12]:

- **The Counterfeit Access Device and Computer Fraud and Abuse Act of** 1984 regulates the frauds or any such cyber related attacks committed on the federal computer system or any such other banks, or in the interstate having access to sensitive information relating to foreign commerce and international trade
- **The Computer Security Act of 1987** [13]introduced an agency known as the **National Institute of Standards and Technology (NIST)** in order to develop not only healthy but also safer security systems and too maintain such security standards and take effective measures so as to considerably reduce cybercrime and also to take other initiate steps to create more cybersecurity awareness, however, military and defense-related concern are an exception under its domain.
- **The Paperwork Reduction Act of 1995** was an initiation to develop and advance the existing internet related policies.
- **The Homeland Security Act of 2002 (HSA)** was a landmark legislation which initiated to give responsibility to homeland security agency and aided them to give them a free hand to develop internet standards along with other tertiary security concerns
- **The Cyber Security Research and Development Act, of 2002** [14]**and The E- Government Act of 2002** are the most important legislation. They provides guidelines and regulations and other stringent rules for federal information technology in the country to be followed for cybersecurity In the view of these same legislations, the federal government has been introducing several new cybersecurity laws and has been pursuing to amend the older ones for a better security ecosystem.

b) **UNITED KINGDOM:** The executive agencies entrusted with the task of maintaining cyber security had a great degree of pliability in developing various approaches towards cyber security. The office of cyber security was set up in the year 2009 and came to be recognized as The **Office of Cyber Security and Information Assurance (OCSIA)**[15] in the year 2010.

[12] Chander, Harish, and GAGANDEEP KAUR. Cyber laws and IT protection. PHI Learning Pvt. Ltd., 2022.
[13] Barnsdale Jr, William J., and Frank G. Ford. "Computer security device." U.S. Patent No. 4,685,056. 4 Aug. 1987.
[14] President's Information Technology Advisory Committee. Cyber security: A crisis of prioritization. National Coordination Office for Information Technology Research and Development, 2005.
[15] Ring, Tim. "UK cyber-strategy suffers as spooks meet the suits." Computer Fraud & Security 2013.11 (2013): 9-13.

The OCSIA performs the dual responsibility of advancing and harmonizing the cyber security policies across the various wings of the UK government and also works for the private sector for information exchange. The authoritative body for implementing the cyber security policy is National Cyber Security Centre. It is the authority responsible for guiding the cyber security responses across the government bodies and industries. It was setup in the year 2016 incorporating the functions of the Communications electronic security group, which was also referred to as the intelligence wing of the UK. The responsibility of the Government Communications Headquarters (GCHQ) also extends towards taking the operations of the Centre of Cyber Assessment. The most recent development in the regulations of UK, applicable to the businesses were General Data Protection Regulations and Network Information security. Other relevant laws and regulations in relation to the cyber security includes Computer Misuse Act 1990, Communications act 2003, Privacy and Electronics Communications Regulations 2003. The Private businesses functioning in UK were required to adopt the strict measures for the preventing the breach of data by any of the entities, it also motivates the private businesses to maintain a cyber-hygienic system in order to prevent the cybercrimes.

c) **AUSTRALIA:** Cybercrime Act offers comprehensive regulation of computer and Internet-related offenses such as unlawful access and computer trespass, damaging data and impeding access to computers, theft of data, computer fraud, cyber stalking and harassment, and possession of child pornography. Other legislation such as **The Spam Act** 2003[16] established a scheme for the regulation of commercial email and other types of electronic messages. It limits unapproved, spontaneous, electronic messages for certain exemptions. This act is managed by the "Australian Interchanges and Media Authority. As far as data privacy of the public is concerned the Australian government has a comprehensive framework in the place known as the Protective Security Policy Framework and Information Security Manual. The Australian Government has most recently announced its Cyber Security Policy for 2020 [17]which aims at providing 247 cyber assistance, helping small and large businesses to set up

[16] Kigerl, Alex C. "Email spam origins: does the CAN SPAM act shift spam beyond United States jurisdiction?." Trends in Organized Crime 21 (2018): 62-78.
[17] Rajaretnam, Thilla. "A review of data governance regulation, practices and cyber security strategies for businesses: An Australian perspective." International Journal of Technology Management and Information System 2.1 (2020): 1-17.

better cyber security infrastructure, and to ensure reduction and awareness concerning cybercrimes. Australia has effective general regulatory cyber law but unlike the United States of America, it lacks regulatory laws in many sectors such as health, private business insurance, etc.

THE INDIAN SCENARIO

In the present techno-canny climate, the world is turning out to be increasingly more carefully refined as are the crimes. Cyber world was at first evolved as a researching and data sharing device and was in an unregulated way. As the time elapsed by it turned out to be more conditional with e-business, web based commerce, e-administration and e-acquisition and so forth. All legitimate issues connected with web wrongdoing are managed through digital regulations. According to the digital wrongdoing information kept up with by the National Crime Records Bureau (NCRB), a sum of 217, 288, 420 and 966 Digital crimes cases were enlisted under the Information Technology Act of 2000 during 2007-10 separately[18].

According to 2011 NCRB figures, there were 1,791 cases enlisted under the IT Act during the year 2011 when contrasted with 966 cases during the earlier year (2010) in this way reporting an increase of 85.4% in 2011 over 2010. The age-wise profile of persons arrested in cyber crime cases under the IT Act, 2000 showed that 58.6% of the offenders were in the age group 18–30 years (695 out of 1184) and 31.7% of the offenders were in the age group 30-45 years (376 out of 1184)[19].

According to Norton Cybercrime Report 2012, 66% of Indian online adults have been a victim of cyber fraud in their lifetime. In the past 12 months, 56% of online adults in India have experienced cyber fraud[20].

With regards to the interest of the times, the Cyber Crime Investigation Cell (CCIC) of the CBI[21], advised in September 1999, began working with impact from 3.3.2000. Cyber Crime Investigation

[18] Kumar, Sanjeev, and Anupam Manhas. "Cybercrimes in India: Trends and Prevention." Galaxy International Interdisciplinary Research Journal 9.05 (2021): 363-370.
[19] Supra 18
[20] Supra 18
[21] Rathod, Falgun. Handbook on Cyber Crime and Law in India Compiled by Falgun Rathod: Cyber Crime, Investigation and Cyber Law. Falgun Rathod, 2014.

Cell is a wing of Mumbai Police, India, to deal with Cyber crimes, and to enforce provisions of the Information Technology Act 2000, and different digital crime-related arrangements of criminal regulations, including the Indian Penal Code[22].

India has an intricately detailed and definitive legal system in place. However the arrival of Internet signaled the beginning of the rise of new and complex legal issues. Also that all the existing laws in place in India were enacted long ago while keeping in mind at that point of time the relevant political, social, economic, and cultural scenario. Nobody then could really visualize about the Internet. The approaching of the Web prompted the rise of various sensitive legitimate issues that required the establishment of Digital Regulations. None of the current regulations gave legitimate legitimacy or consent to the exercises on the Internet.

THE GENESIS OF I.T. LEGISLATION IN INDIA:

Mid 90's saw an impetus in globalization and computerization, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. With quite a bit of global exchange being finished through electronic correspondence and with email picking up speed, an earnest and inevitable need was felt for perceiving electronic records for example the information that is put away in a PC or an outer stockpiling connected thereto. The Assembled Countries Commission on Global Exchange Regulation (UNCITRAL[23]) took on the Model Regulation on web-based business in 1996. The Overall Gathering of Joined Countries passed a goal in January 1997 entomb alia, prescribing all States in the UN to give great contemplations to the said Model Regulation, which accommodates acknowledgment to electronic records and concurs it a similar treatment like a paper correspondence and record. The Data Innovation Act is a result of the goal dated 30th January 1997 of the overall together of the Assembled Countries, which took on the Model Regulation on Electronic Business and embraced the Model Regulation on Electronic Business on Global Exchange Regulation. This goal suggested, bury alia, that all states give good thought to the said Model Regulation while amending and establishing new regulations, so consistency might be seen in the regulations, of the different digital countries, pertinent to choices to paper-based strategies for correspondence and capacity of data.

[22] Supra 21

[23] Rattan, Jyoti. "Law Relating To E-Commerce: International and National Scenario with Special Reference to India." International Journal of Social Science and Economics Invention 1.2 (2015).

The Division of Gadgets (DoE) in July 1998 drafted the bill. Be that as it may, it must be presented in the House on December 16, 1999 (after a hole of very nearly one and a half years) when the upgraded IT Service was shaped. It went through significant adjustment, with the Business Service making ideas connected with internet business and matters relating to World Exchange Association (WTO) commitments. The Service of Regulation and Company Undertakings then verified this joint draft. After its presentation in the House, the bill was alluded to the 42-part Parliamentary Standing Advisory group following requests from the Individuals. The Standing Board of Trustees made a few ideas to be integrated into the bill. In any case, just those ideas that were supported by the Service of Data Innovation were consolidated. One of the ideas that were profoundly bantered upon was that a digital bistro proprietor should keep a register to record the names and addresses surprisingly visiting his bistro and a rundown of the sites that they surfed. This idea was made as an endeavor to check digital wrongdoing and to work with expedient situating of a digital crook. Be that as it may, simultaneously it was criticized, as it would attack a net surfer's security and wouldn't be financially practical. At last, this idea was dropped by the IT Service in its last draft. The Association Bureau endorsed the bill on May 13, 2000, and on May 17, 2000, the two places of the Indian Parliament passed the Data Innovation Bill. The Bill got the consent of the President on the ninth of June 2000 and came to be known as the Data Innovation Act, of 2000. The Demonstration came into force on the seventeenth of October 2000.

SHORTCOMINGS UNDER INDIAN LAW

The **Indian Information Technology Act, 2000** has charged CERT to cooperate and collaborate with organizations within and outside the country although it does not lay down any whatsoever criteria for CERT to exercise or to refuse to exercise its power. CERT being directly under the administrative control of the Ministry of Communications and Informational Technology does not have any operational independence or discretion to cooperate unless approved by the Government.

CERT is not an independent entity entitled to draw the limits of cyber-surveillance; it acts upon the direction of its master, which is the Government of the day. The limits of surveillance are undefined with the want of privacy law. This vastly reduces the organizational utility of CERT when it comes to prosecuting international cybercrimes, in collaborating on information sharing and coercive interception of networks/computers, as an organization of national importance.

The cyber-surveillance discretion of CERT is therefore restricted by administrative powers exercised by the incumbent Government. Therefore, instead of acting towards preventing cyber- attack incidents on the universality principle, it is reduced to serving the present-day Government and regulated by changing governments' policies. The present Indian framework of cyber law ignores that it is administratively impossible to seek government approval on day to day basis when cyber surveillance is an ongoing and continuous process to avert crime.

Indian law only provides for information security management systems (ISMS) and cyber crisis management plans (CCMP)[24] for safeguarded frameworks pronounced by the Public authority in public safety, economy, general well-being and security. India lacks a cyber-surveillance law and a framework that is instrumental in preventing cyber-attacks and an organization that monitors cyber violations continuously (not only incidence-based).

An autonomous position to forestall wrongdoing events and gather data for occurrences and exercises influencing any partner locally or globally is a need of great importance. In the absence of privacy law, the Indian Government has felt reluctant to part with the authorization process and grant operational freedom to agencies, without which real-time monitoring and collecting traffic data and information is impossible, leading to failure to discover crime before it happens. The Indian regulation is exceptionally crude in characterizing digital offenses and disregards a significant part of the contemporary improvements in the internet. For instance, the **Information Technology Act, of 2000** doesn't characterize licensed innovation cybercrime offenses, digital washing, virtual monetary standards, online clubs, and cyber warfare. Offenders can open e-gold accounts in different countries and combine them, complicating the use of financial instruments for money laundering and terrorist financing. Account-holders may likewise utilize wrong data during enlistment to cover their personality. In the absence of specific law, the prosecutions are initiated on deductive reasoning and broad, inclusive definition as including offences within the term by employing interpretative tools, which essentially negates access to justice for the absence of notice of the law and adequately defined safeguards to protect human rights violations.

[24] Bhoorani, Kamlesh, D. Murali Krishna, and Anand Shankar. "Cybersecurity for Indian Power Sector: A standards based approach." Water and Energy International 66.1 (2023): 39-44.

Cybercrimes are multisector, and India has not commanded a multisector CIRT by partners, consequently fundamentally diminishing its compass and power. India needs a complete digital regulation that incorporates all developing wrongdoings and a digital technique with a multisector approach with the foundation to screen and answer the rates consistently. The Indian regulation misses the mark on preventive ways to deal with wrongdoings that don't address the worldwide worry of other states and comes up short on a cooperative reconnaissance instrument that is multisector-driven and comprehensive.

CONCLUSION

In conclusion, the current state of the Indian Information Technology Act, of 2000, places CERT in a position where its effectiveness is hindered by administrative constraints. Operating under the direct control of the Ministry of Communications and Information Technology, CERT lacks the autonomy to set the boundaries of cyber surveillance independently. Instead, it acts under the directives of the government, limiting its utility in prosecuting international cybercrimes and collaborating on information sharing. The absence of a privacy law further compounds the challenges faced by CERT, as it operates within the administrative powers wielded by the incumbent government. This situation diminishes CERT's role in preventing cyber-attacks based on universal principles, relegating it to serving the interests of the present-day government and being subject to changing policies. The inadequacies in the current Indian cyber law framework are evident in the lack of a dedicated cyber-surveillance law and a comprehensive monitoring organization capable of addressing cyber violations continuously. While the law focuses on information security management systems and cyber crisis management plans for specific frameworks, it falls short in preventing cybercrimes on a broader scale. There is a pressing need for an autonomous entity that can proactively prevent cybercrimes, gather data on incidents, and respond to activities affecting stakeholders globally.

The absence of a privacy law has led to a reluctance on the part of the Indian government to grant operational freedom to agencies, hindering real-time monitoring and data collection essential for crime prevention. In light of the evolving nature of cybercrimes, the existing regulations in India lack specificity, especially in defining offenses related to intellectual property, cyber laundering, virtual currencies, online clubs, and cyber warfare. The prosecutions initiated under such vague legal

frameworks often rely on deductive reasoning and broad definitions, compromising access to justice and failing to provide clear safeguards against human rights violations. To address the multisector nature of cybercrimes, India requires a comprehensive digital regulation that encompasses emerging offenses. A multi-sector approach, supported by a well-defined digital strategy, is crucial for effective monitoring and response capabilities. The current regulatory framework falls short in offering preventive measures for crimes that concern the global community, highlighting the need for a collaborative surveillance mechanism that is multisector-driven and inclusive.