

Proceedings of
National Conference on

Data Privacy & Cyber Security Laws in India



Organized by
Faculty of Law



Date
15th February 2020



JUSTICE DR. RAVI RANJAN
CHIEF JUSTICE



High Court of Jharkhand
Ranchi - 834 033
Ph : 0651 - 2482095
Fax : 0651 - 2481115



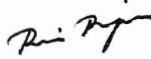
7th Feb. 2020

MESSAGE

It is a matter of great pleasure that the ICAI University, Jharkhand is organizing a National Conference on “Data Privacy & Cyber Security Laws in India” on 15th February 2020 at Ranchi and a souvenir is also being published to mark the occasion.

Cyber Security and Data Privacy are interrelated and interdependent on each other, being very sensitive aspect of the digital world. While every citizen is entitled to privacy of his particulars, cyber security is concerned with the Security of the data on the Internet. Security threats and Security breaches have become rampant in the cyberspace today. As such, there is a need to have a robust and resilient legal protection for the Data Privacy and Cyber Security in the country. The Government is also sensitive on the issue and has made a beginning in this direction by way of the proposed Personal Data Privacy Bill 2019. Digitalization of the trade and commerce, business, administration etc. is increasing day by day in the country and no aspect of life is without computer and the Internet. On the other hand cyberspace crimes are also increasing simultaneously with similar pace. Therefore, growing challenges of managing security of the data necessitates and demands a comprehensive approach to Information Security. Cyber Security and Data Protection are critical to safeguard the interests of the society and the nation. I am sure the Conference would be of immense help in this direction as new ideas and approaches would be articulated & debated during the course and outcome thereof will be used for the people and the nation as a whole.

I wish the Conference and its participants a grand success and hope it is able to achieve and deliver the desired aim, as also contribute to the common cause.


(Justice Dr. Ravi Ranjan)

Chief Justice's House, Kanke Road, Ranchi 834008
☎ : 0651 - 2202000, 2282000 Fax : 0651-2280868

PRASHANT KUMAR SINGH, Adv.
Member, BCI

Phone : 8292642626, 9431189644
E-mail : prashantkrs11@gmail.com



झारखण्ड राज्य विधिज्ञ परिषद्
JHARKHAND STATE BAR COUNCIL

(Statutory Body Constituted under The Advocates' Act, 1961)

Justice Colony, North Office Para, Doranda, Ranchi-2

Phone : 0651-2410008, 0651-2412722, 9431936083

E-mail : info@jharkhandstatebarcouncil.org | Website : www.jharkhandstatebarcouncil.org

Ref. No. M/12/JSBC/2020

Date : 12/02/2020

Message

I am extremely delighted to know that Faculty of Law, ICFAI University, Jharkhand is organizing one day National Conference on "**Data Privacy and Cyber Security Laws in India**" on 15th February 2019 at Ranchi and to mark occasion a souvenir is being published.

The organizers have rightly selected the contemporary and relevant theme "**Data Privacy and Cyber Security Laws in India**" for the conference, Growing challenges of managing security of the data in organizations, corporate and government, that are increasingly connected with their global suppliers, contractors and partners and the increasing exposure to threats and attacks demand a comprehensive approach to Information Security. In the current times of increased data flows, understanding Cyber Security and Data Protection becomes critical to harmonize the operations and build trust for Indian Industries and Government entities.

Cyber Security and Data Privacy are interrelated and interdependent aspect of today's digital world. While every citizen is entitled to privacy of his particulars, cyber security is concerned with the Security of the data on the internet. The way the Security threats and Security breaches are rampant in the cyberspace today, there is a need to have a robust and resilient legal protection for the Data Privacy and Cyber Security in the country. Initiative has been taken by the Indian Parliament for the framing of Data Privacy Law in the recent times. I believe that many new ideas and suggestions would be articulated & debated during the conference and outcome thereof will be used for the benefit of organizations, corporate, government and common people.

I extend my best regards to the Faculty of Law, ICFAI University Jharkhand for organizing this National Conference and Participants on this great occasion.

Prashant Kumar Singh

(Prashant Kumar Singh)
Member, BCI



Message from Vice-Chancellor

In the last few years , Innovations in Internet and Mobile Technologies have brought in enormous benefits to the individuals and the organisations in our day-to-day working, by way of better convenience, improved efficiency and cost savings. At the same time, criminals have been exploiting the weaknesses to cause harm, by way of thefts of personal information and trade secrets, Ransomware attacks, hacking of bank accounts and siphoning away money etc. Heinous crimes are being planned and committed each day under a cloak of anonymity. The roles of cybercriminals also are becoming more specialized and transnational.

This highlights the importance of the challenges in delivery of Justice in the case of Cyber Crimes. Ensuring the rule of law in such an environment has to ensure that critical evidence anywhere in the world does not lie beyond the reach of the law. Every serious threat that is investigated requires access to electronic evidence, like emails, instant messages, photos, server data, session logs, subscriber information etc. Many telecom and mobile devices and services today have default encryption controlled by the user or service provider. This encryption often bars access to evidence, even where law enforcement officers obtain a warrant from a neutral judge. Even as crimes are committed against millions of individuals with relative ease, investigators and prosecutors must carefully follow the law in tracing those crimes to their source.

There is also need to build more awareness among the users on the types of cyber crimes that are perpetrated and how to avoid them and also the need for speedy reporting to the concerned authorities.

In this situation, I am happy that our University is organising the National Seminar on Data Privacy and Cyber Security Laws in India. It is a good opportunity for academicians, researchers, practicing lawyers, investigation and law enforcing authorities like police and intelligence and enforcement agencies to discuss and evolve appropriate solutions to ensure Justice in the Cyber World. A Safe Cyber World is the key to the progress of the individuals and the society, at large. .

I wish the seminar all success

Prof O R S Rao
Vice-Chancellor

About the Conference

on

Data Privacy and Cyber Security Laws in India

Cyber security and privacy is an interrelated and interdependent concept. One cannot understand without analyzing the interface between these two. We know that Security is a process, not a destination. It is a process which never ends. The way the security threats and security breaches are rampant in the cyberspace, there is a need to have a robust and resilient cyber security policy in the country.

New emerging trends of cyberspace such as Artificial intelligence, Internet of things, Block Chain, Dark net& Cloud Computing posed new challenges to data security and privacy concerns in cyberspace. Growing challenges of managing security of the data in organizations, corporate and government, that are increasingly connected with their global suppliers, partners and contractors, and the increasing exposure to threats and attacks demand a comprehensive approach to information security. World has witnessed some alarming security breaches which also threaten to the national security. In the current times of increased global data flows, understanding cyber security and data protection becomes critical to harmonize the operations and build trust for Indian industries and government entities.

Objective: This seminar endeavors to comprehensively discuss the Cyber Security& Data Privacy in the light of proposed the Personal Data Protection Bill and other international standards on cyber security compliances. The seminar will provide a platform for academicians, cyber security professionals and students to connect with like-minded security enthusiastic and learn the latest in data security and privacy domain.

Broad Themes of the Conference

CYBER SECURITY

- Cyber Security: Emerging Threats, Security Breaches & Future Concerns
- Emerging Trends of Cyberspace (Artificial intelligence, Internet of things, Block Chain, Dark net& Cloud Computing) and Cyber security
- Social Networking and Concerns of Cyber security
- Legal Framework for Cyber security
- International Cyber security Standards and Cyber security Compliances

DATA PROTECTION & PRIVACY

- A Comparative Analysis of International Data Protection Rules/Regulations
- Emerging concerns of data security and privacy (Big data, Crypto Currency, Internet of Things, Cloud Computing etc.)
- Surveillance State and Right to Privacy
- Right to be forgotten
- Data Localization Data Localization and Cross-Border Data Transfers
- Judicial Interpretation of Data Protection and Privacy in India
- Intermediaries & Data Repositories and their Liability in the Case Data Breaches.

Conference Organizing Committee

Patron	Prof. ORS Rao, Vice Chancellor
Mentor	Prof. Arvind Kumar, Registrar
Conveners	Dr. Bhabat Barik & Dr. Rumna Bhattacharya
Organizing Secretary	Prof. Alok Kumar and Prof. Sumit Kumar Sinha
Advisory Committee	<ul style="list-style-type: none">• Prof. (Dr.) Y. R. Haragopal Reddy, Advisor ICFAI Society, Hyderabad• Prof. (Dr.) S. K. Bhatnagar, Hon'ble VC, RMLNLU, Lucknow• Prof. (Dr.) Kesava Rao Vurrakula, Hon'ble VC NUSRL Ranchi• Prof. (Dr.) Srikrishna Deva Rao, Hon'ble VC NLUO, Cuttack• Prof. Sukh Pal Singh, Former VC, HNLU, Raipur, Chhattisgarh• Prof. (Dr.)A. V. Narsimha Rao, Director, ICFAI Law School, Hyderabad• Dr. Rakesh Verma, Director, Institute of Legal Studies, Ranchi University• Dr. Pankaj Chaturvedi, Principal, Chotanagpur Law College, Ranchi• Dr. Jitendra Kumar, Principal, Jamshedpur Cooperative Law College, Jamshedpur• Prof. (Dr) Ajay Kumar, Professor of Law & Dean Academic Affairs and Law, CNLU, Patna• Dr. Syamala Kandadai, Associate Professor, NUSRL Ranchi• Dr. M. R Sreenivasa Murthy, Associate Professor, NUSRL Ranchi

	<ul style="list-style-type: none"> • Dr. Yogesh Pratap Singh, Associate Professor, NLU Cuttack • Dr. Rashweth Shrinkhal, Assistant Professor, Central University of Jharkhand • Mr. Kumar Gaurav, Assistant Professor of Law, CNLU, Patna
Organizing Committee	<ul style="list-style-type: none"> • Prof. Divya Utkarsh, Treasurer, National Conference • Dr. Manish Kumar & Dr. Vishal Kumar, Guests Affairs, National Conference • Prof. Ranjeet Kumar, Delegate Affairs, National Conference • Dr. Dilip Kumar & Dr. Sweta Singh, Accommodation Affairs, National Conference • Dr. Sudipta Majumdar, Dr. Mridanish Jha & Dr. M. Rajkumar, Publication Affairs, National Conference

Research Papers : Index

Sl.	Title Of Paper	Author/s	Affiliation	Page
1	Cyber Crime And Data Localization: A Study	Dr. M.R. Sreenivasa Murthy	Associate Professor, NUSRL, Ranchi	10
2	Data Privacy V. Data Sovereignty: A Constitutional View Point	Dr. Syamala Kandadai	Associate Professor-cum-Director (Research & Training), NUSRL, Ranchi	10
3	Changing Contours Of Panoptic Panoramas In Cyberspace Vis-À-Vis Privacy	Kumar Gaurav	Assistant Professor (Law), Chanakya National Law University, Patna, Bihar	11
4	Living In A Modern Surveillance State: Issues And Challenges	Hrishikesh Manu	Assistant Professor (Law), Chanakya National Law University, Patna, Bihar	11
5	Challenges In Cyber Security: An Analysis With Reference To Indian Law	Mukesh Kumar Ghosh & Pratigya Kumari	Assistant Professor (FOL), ICFAI University, Himachal Pradesh & Student FOL, ICFAI University Jharkhand	12
6	Legal Framework For Cyber Security	Ms.Tanya Pandey, Mr. Abhilash Arun Sapre	Asst. Professor of Law, Kalinga University, Raipur	12
7	Social Networkings In Unorganised Sectors & Concerns Of Cyber Security	Mardul Kumar Saxena	Director (Pers.), Heavy Engineering Corporation Limited	13
8	Cyber Threats For New Renewable Solar Energy Systems	Pramoda Kumar Behera	General Manager, Heavy Engineering Corporation Limited, Research Scholar, Jharkhand Rai University Ranchi.	14
9	Violation Of Fundamental Rights And Cyber Justice Mechanism In India	Rajesh Kumar & Rahila Imam	(Research Scholar, CNLU & LLM)	15
10	Scrutiny Of Data Protection Laws In India	Dr. Aseem Chandra Paliwal, Ms. Megha Middha	Associate Professor, Assistant Professor, Mody University of science and Technology, Lakshmangarh	16
11	Cyber Crimes In India: Legislative And Judicial Response	Dr.Akhilesh Kumar Pandey & Manisha Pandey	Associate Professor, Karnavati University, Gandhinagar Gujarat. & Student, FOL, ICFAI University Jharkhand	16

Sl.	Title Of Paper	Author/s	Affiliation	Page
12	Right To Be Forgotten: An Overview Of The Ongoing Legislative And Judicial Developments	Ms. Priyanka Chowdhary & Uzma Sohail	Assistant Professor, UPES, Dehradun & Student, FOL, ICFAI University Jharkhand	18
13	Judicial Interpretation Of Data Protection And Privacy In India	Nidhi Kumari & Siddhant Chandra	Student, Department of Criminology, Jharkhand Raksha Shakti Univesity	18
14	Fixing The Accountability Of Intermediaries And Data Repositories To Protect Personal And Sensitive Data-State Surveillance Vs Right To Privacy	Aditya Jain	Advocate, Supreme Court of India and Rajasthan High Court	19
15	Terms And Conditions Vis-À-Vis Data Privacy: A Study	Peter Ladis F	Assistant Professor of Law, CNLU Patna	20
16	Artificial Intelligence And Indian Legal System: An Analysis	Samrat Datta & Rakhi Kumari	Assistant Professor of Law at Faculty of Law, ICFAI University, Himachal Pradesh (Baddi) & Student, FOL, ICFAI University Jharkhand	20
17	An Analysis Of The Cyber Security Policy 2013 In Wake Of The New Cyber Security Strategy 2020	Ms. Disha Atri & Dr. Sagar Kumar Jaiswal	Assistant Professor, Guru Ghashidas Vishwavidyalay, Bilaspur (C.G.)	21
18	Intermediary Liability In India For Third Party Content	Mr. Sushil Jain & Dr. Ajaiy Singh	Assistant Professor, Guru GhashidasVishwavidyalaya, Bilaspur (C.G.)	21
19	Social Networking And Concerns Of Cyber Security	Tripti Bhushan & Rahul Kumar	Assistant Professor, Kalinga University, Raipur & Student, FOL, ICFAI University Jharkhand	22
20	Legal Framework Of Cyber Security: Indian Perspective	Simran Kumari & Shubhangi	Students, ICFAI University, Jharkhand	23
21	Issue Of Jurisdiction In Combating Cyber Crimes	Kamlesh Kumar	Asst. Prof. CNLC, Ranchi University Ranchi Jharkhand	23
22	Cyber Security, Legislation, Regulation And Enforcement	Prabhash Nath Jha & Arvind Kumar Jha	Asst. Prof. CNLC, Ranchi University,Ranchi	23
23	Right To Privacy Vs State Surveillance: Issues And Challenges	Mrs Sakshi Pathak & Mrs Lalsa Mohini	Assistant Professor, Chotanagpur Law College, Namkum	24
24	Data Privacy And Aadhaar	Mahima Agarwal & Komal Kumari	Faculty Associate, ICFAI Law School, The ICFAI University, Jaipur & Student, FOL, ICFAI University Jharkhand	24
25	Data Localization And Cross-Border Data Transfers	Abhinav Kumar Singh & Deep Raj	Advocate, Patna High Court, Patn	25
26	A Question On The Co-Existence Of Unique Identification Number (Uid) And Right To Privacy	Paridhi Shrivastava, Gaurav Purohit & Sourav Kumar Vardwaj	Students, Jagran Lakecity University & student, FOL, ICFAI University Jharkhand	25
27	Cyber Security Issues In India	Dr Anupam Manhas & Tudsii Kudadah	Assistant Prof, Career Point University Hamirpur H.P. & Student FOL, The ICFAI University Jharkhand	26
28	Cyber Literacy An Initiation To Cyber Security	Tulika Sinha	Assistant Professor Usha Martin University, Ranchi	26
29	Efficacy Of Cyber Security Laws: A Critical Study	Dr. Vijay Kumar Vimal & Vivek Kumar Saha	Assistant Professor of Law, Chanakya National Law University, Patna	27
30	State Surveillance In India: A Comparative Legal Study	Sunkara Vishnu Ameya	2nd year Law Student, DamodaramSanjivayya National Law University	27

Sl.	Title Of Paper	Author/s	Affiliation	Page
31	Legal Framework For Cyber Security Under It Act, 2000	Astha Bhatt & Reshav Kumar Mandal	Student (2nd Year), Faculty of Law, The ICFAI University Jharkhand	28
32	Pole Star On A Moonless Night Or Just Another Iota Of Sand In The Desert?An Intricate Analysis On The Personal Data Protection Bill, 2019	Swaraj Kariya & Ujjwal Sheth		28
33	Cyber Threats In Social Networking Websites And Legal Frameworks	Chandan Kumar Ojha & Anjali Sinha	LLB student, The ICFAI University Jharkhand	28
34	Surveillance State And Right To Privacy: Conundrum Of The Modern World	Chandra Mohan & Tushar Pal	Students, CNLU, Patna	29
35	The Emergence Of Blockchains: Another Sword Of Damocles For Law?	Raj Shekhar Student & Ujjwal Singh	(1st Year), NUSRL, Ranchi & Student (2nd Year), CNLU, Patna	29
36	Concerns And Issue Of Contemporary Data Regime	Abhijeet Kumar	Student, CNLU, Patna	30
37	Facesec: An Intelligent Model To Detect Face In Real Time	Paramita Bhattacharjee, Hrituraj Chakraborty, Dipjyoti Deka	Student, The ICFAI UNIVERSITY Tripura, Assistant Prof., The ICFAI UNIVERSITY Tripura	31
38	Data Protection - Conceptual And Theoretical Understanding	Syed Hozaifa Arsh & Fatma Jannat	Students, ICFAI University, Jharkhand	31
39	Cyber Security As A Backbone Of E-Commerce	Mr. Mukul Pandey & Mr. Rajeev Kumar Sinha	Research Scholar, Kolhan University, Chaibasa, Research Scholar, ARKA JAIN University, Jharkhand	31
40	Legal Framework For Cyber Security In India: A Qualitative Study	Prithvi Raj & Sourav Kumar Upadhyay	Students, Department of Criminology, Jharkhand Raksha Shakti Univesity	32
41	State Surveillance: A Threat To Right To Privacy?	Mani Shankar Mani & Adarsh Singh	LLM Students, CNLU, Patna	32
42	Data Protection Bill 2019 - Analytical Study	Nisha Kumari Mishra	BBALLB Student, FOL, ICFAI University, Jharkhand	33
43	Cyber Security And Cyber Laws Around The World And India: Major Thrust Highlighting Jharkhand For Concerns	Dolly Krishnan & Mohit Verma	Persuing LLB, ICFAI University, Ranchi, Jharkhand	33
44	Cyber Security International Legal Framework	Saumya Pratibha Tirkey & Shailvi Sinha	Students, ICFAI University, Jharkhand	34
45	Emerging Threats In Cyber Security Breaches And Future Concern	Nitish Chaubey	Student, Institute of Legal Studies, Ranchi	34
46	Legal Framework Of Cyber Security: Indian Perspective	Simran Kumari & Shubhangi	Student, The ICFAI University Jharkhand	34
47	Right To Be Forgotten	Pranjul Dalela (Author) & Samarth (Co Author)	National University Of Study And Research In Law, Ranchi	35
48	Privacy And Data Protection Laws In India	Ajay Kumar Singh Gautam	Student, The ICFAI University Jharkhand	36
49	Legal Framework For Cyber Security	Sonu Kumar	Department Of Law: - University Law College, Hazaribagh	36

Sl.	Title Of Paper	Author/s	Affiliation	Page
50	Data Privacy And Cyber Security	Jaya Jha & Samiksha Gupta	Student, University of Petroleum and Energy Studies, Dehradun	37
51	Artificial Intelligence: Challenges For Cyber Security	Dr. Dilip Kumar, Dr. Manish Kumar, Dr. Goutam Tanti & Dr. Vishal Kumar	Assistant Professors, Faculty of Management Studies, ICFAI University Jharkhand	37
52	Corporate Grid Over Human Need	P. K. Bhattacharyya, Advocate & Dr. Rumna Bhattacharyya	Vice President, Dhanbad Bar Association, District Court & Professor FMS, ICFAI University Jharkhand	38
53	State Surveillance And Right To Privacy	Mansi Goel & Akanksha Basundhra Raje	Students, FOL, ICFAI University, Jharkhand	38
54	Emerging Trends Of Cyber Space (Artificial Intelligence, Internet Of Things, Block Chain, Dark Net And Cloud Computing) And Cyber Security	Parambir Singh Bajaj	Student, ICFAI University, Ranchi	39
55	Challenges For Organization In Sharpening The Skills In Managing Data Privacy In An Increased Connected World	Dr. Pallavi Kumari & Mr. Randhir Ranjan	Assistant Professor, Faculty of Management Studies, ICFAI University Jharkhand & Advocate Jharkhand High Court	40
56	Right To Be Forgotten	Om Prakash Ravi	Student, CNLU, Patna	40

THEME: DATA PRIVACY AND CYBER SECURITY LAWS IN INDIA : ABSTRACTS :

CYBER CRIME AND DATA LOCALIZATION: A STUDY

Dr. M.R. Sreenivasa Murthy

Associate Professor, NUSRL, Ranchi

Abstract

The increasing instances of cyber crimes involving financial frauds, with the modus operandi of phishing, vishing, credit card frauds etc., is effecting the public faith in the cashless economy. The Government of India's Digital India Programme with the slogan, 'Faceless, Paperless, Cashless', which intended to provide facility of seamless digital payment to all citizens of India in a convenient, easy, affordable, quick and secured manner is creating a skepticism in the public towards online transactions, as cyber crime investigations are delayed or stalled due to the lack of data localization requirement for the digital wallet companies, who do not have any permanent establishment in India. The Srikrishna Commission recommended that data be stored in the country either directly or through mirror servers to serve law enforcement needs. The RBI on 6th April 2018 issued a circular mandating that all data related to payment systems should be locally stored in India. Supreme Court of India on 2nd August 2019 in response to a PIL (WP[C]921/2018) directed RBI to confirm WhatsApp's compliance with data localization of payments data as the company is planning to launch its UPI payment service in India this year. The Supreme Court also asked the Central Government to clarify its position on whether the company's grievance officer should be based out of India. The draft e-commerce policy and draft Personal Data Protection Bill, 2018 provides for specific requirements on cross border data storage. This article attempts to analyze the importance of data localization from the context of cyber crimes involving financial frauds and also the efforts of the Government of India to ensure data localization for providing a secured digital payments system. The article also analyzes the attempts of the Supreme Court of India in protecting the data privacy and data security in India.

Key words: *Data localization, Cyber crime, Digital Payments, RBI, E-commerce, Personal Data Protection Bill, 2018*

DATA PRIVACY V. DATA SOVEREIGNTY: A CONSTITUTIONAL VIEW POINT

Dr. Syamala Kandadai

Associate Professor-cum-Director (Research & Training), NUSRL, Ranchi

Abstract

In Justice (Retd.,) Puttuswamy v. UOI (2017) 10 SCC 1, the Supreme Court of India held that right to privacy is protected as a fundamental constitutional right under Articles 14, 19 and 21 of the Indian Constitution. As a consequence of the judgment, the 'Aadhar Card Scheme' which was alleged to be in breach of fundamental right to privacy, will now be tested by the same standards by which a law which invades personal liberty under Article 21 is liable to be tested. In the same way, the Personal Data Protection Bill, 2018 is also subject to right to privacy guaranteed under Articles 14, 19 and 21 of the Indian Constitution. Section 35 of the Bill, 2018 allows any government agency to bypass all the privacy safeguards provided in the Bill in the interest of sovereignty and integrity of India, security of the State,

friendly relations with foreign state or public order and for preventing any cognizable offence relative to the above. The safeguards provided are, a written order from the central government specifying the reasons for breaching privacy and in a manner as may be specified in future. This reflects that the future of Personal Data Protection Bill, 2018 after enactment is expected to face the test of constitutional validity due to the data sovereignty clauses conflicting with the data privacy requirements. This article analyzes the scope of fundamental right to data privacy guaranteed under Art.14, 19 and 21 against reasonable restrictions laid down in the Constitution and the constitutional validity of the Data Protection Bill, 2018.

Key words: *Data Privacy, Data Sovereignty, Fundamental Rights, Reasonable Restrictions, Personal Data Protection Bill, 2018.*

CHANGING CONTOURS OF PANOPTIC PANORAMAS IN CYBERSPACE VIS-À-VIS PRIVACY

Kumar Gaurav, Assistant Professor (Law), Chanakya National Law University, Patna, Bihar.

Abstract

Bentham's seeds of Panoptic Panoramascan be visualized in the contemporary grown up tree of Surveillance State. The advent of digital technology in general and internet in particular is instrumental behind this development. The development of technology together with social, economic and political factors have raised the antennas of those concerned with interference from governments, enterprises and other personal freedoms. Surveillance and privacy are two most debated phenomenon in this information technology ecosystem. Right to privacy is the right to be free from undue surveillance by government or anyone else. Surveillance by the State must be based on constitutional justifications. Privacy has numerous meaning, and its importance varies greatly among individual, communities, organisations and governments. It is one of the most significant basic rights acclaimed in all the international documents of human rights. The recent legal developments such as EU General Data Protection Regulations ("GDPR"), The Personal Data Protection Bill, 2018 and judicial viewpoint in the K. S. Puttaswamy or the other legal documents on data protection in various jurisdictions give due consideration to the data privacy. The principle of fair and lawful processing, is the very root of all data protection law and the reminder of the principles and the other legal provisions give detailed expression to that principle. Surveillance should be passed through the litmus test of fair and lawful processing of data. But is this so, the world has witnessed some massive data and privacy breaches in the last five years. There is a pressing need to go for the enactment of data protection law which should rational in terms of its constitutionality and at the same time stringent in terms the protection of constitutional rights.

This paper is an endeavour to address the concerns and issues of data privacy and surveillance in cyberspace.

Keywords: Panoptic Panoramas, Surveillance, Privacy, GDPR, Data Protection, the Personal Data Protection Bill, 2018.

LIVING IN A MODERN SURVEILLANCE STATE: ISSUES AND CHALLENGES

Hrishikesh Manu

Assistant Professor (Law), Chanakya National Law University, Patna, Bihar.

Abstract

Internet and smartphones have brought so many positive changes in our life. But at the same time, it has become a perfect tool for the surveillance state. The governments everywhere in the world are collecting data of its citizens through this tool. In an age of terror, our governments in the name of security

are acquiring this data and using it for unknown purposes. Our society also lacks an understanding of why government surveillance is dangerous. The Government of India has proposed a number of surveillance-based intelligence gathering projects over the last few years, especially after the 2008 Mumbai terrorist attacks.

The Constitution of India guarantees every citizen the right to life and personal liberty under Article 21. The Supreme Court, in *Justice K.S. Puttaswamy v. Union of India* (2017), ruled that privacy is a fundamental right. Even though this right is not an absolute right the government needs to increase accountability and responsibility, and infuse reasonable checks and balances in exercising these surveillance powers. There are two major laws that regulate digital and telephonic surveillance in India- The Information Technology Act, 2000 and the Indian Telegraph Act, 1885.

This paper will analyse the legal framework of surveillance and privacy in India with special focus on data protection.

CHALLENGES IN CYBER SECURITY: AN ANALYSIS WITH REFERENCE TO INDIAN LAW

Mukesh Kumar Ghosh & Pratigya Kumari

Assistant Professor (FOL), ICAFI University, Himachal Pradesh &

Student FOL, ICAFI University Jharkhand

Abstract

In the Cyber Security discussions that take place in the various policy forums around the world, there is often little appreciation that the security of the Internet is a distributed responsibility, where many stakeholders take action. By design, the Internet is a distributed system with no central core or point of control. Instead, cyber security is achieved by collaboration where multiple companies, organizations, governments, and individuals take action to improve the security and trustworthiness of the Internet – so that it is open, secure, and available to all. Cyber security that, broadly speaking, relates to the security of Internet infrastructure, the devices connected to it, and the technical building blocks from which applications and platforms are built. Since threat to cyber security is considerably growing therefore, it becomes necessary to provide a legal framework by which cyber activities can be done without any sense of fear. It is, often, observed that concept of cyber security transcend the boundary of nations that makes it complex. In such a situation to provide a legal protection to cyber related activities is a challenging task. Therefore, it is very difficult to claim as to the completeness of law by which task of cyber security is done. In order to maintain cyber security, law should be framed having regard to the nature of its threat and its complexity. In India cyber activities are regulated by Information Technology Act. Experience suggests that this law is not free from its defects. Therefore, the Government has introduced Personal Data Protection Bill, 2019. This paper makes an attempt to find out that whether or not the legal framework, relating to cyber security, in India is capable to provide effective mechanism to ensure cyber security.

Key words: Cyber, Security, Policy, Law, Framework.

LEGAL FRAMEWORK FOR CYBER SECURITY

Ms.Tanya Pandey, Mr. Abhilash Arun Sapre, Asst. Professor of Law, Kalinga University, Raipur.

Abstract

In the present era of growth and development, Information technology is incorporating varying position and texture throughout the world. These technological improvements have made the progress

from paper to paperless transaction plausible. We are presently making new norms of speed, proficiency, and accuracy in communication, which has become key achievements for boosting advancements, inventiveness and expanding by and large efficiency. Computers are extensively used to store confidential data of political, social, economic or personal nature bringing immense benefit to the society. The rapid development of Internet and Computer technology globally has led to the growth of new forms of transnational crime especially Internet related. These crimes have virtually no boundaries and may affect any country across the globe. Thus, there is a need for awareness and enactment of necessary legislation in all countries for the prevention of computer related crime. Globally Internet and Computer based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries. This new boundary, which is made up of the screens and passwords, separate the “Cyber world” from the “real world” of atoms. Territorially based law-making and law-enforcing authorities find this new environment deeply threatening. Systems across the globe have many different rules governing the behaviour of users. These users in most of the countries are completely free to join/ leave any system whose rules they find comfortable/ not comfortable to them. This extra flexibility may at times lead to improper user conduct. Also, in the absence of any suitable legal framework, it may be difficult for System Administrators to have a check on Frauds, Vandalism or Abuses, which may make the life of many online users miserable. Therefore, all of us whether we directly use Internet or not, will like to have some form of regulation or external control for monitoring online transactions and the cyber world for preventing any instability.

Keywords: Information Technology, e- commerce, Cyber world

SOCIAL NETWORKINGS IN UNORGANISED SECTORS & CONCERNS OF CYBER SECURITY

Mardul Kumar Saxena

Director (Pers.), Heavy Engineering Corporation Limited

Abstract

India is known as a developing as well as 2nd largest populous country in the world. Population is the important element of the country. Human Capital is should not be the problem of nation but the power of the nation. Currently, India’s population¹ is over 1.34 billion as of Monday, 18th December 2017, based on the latest United Nations estimates. This population shares 17.74 percent of the world total population. It takes rank number 2nd in the list of countries of dependencies by population. In India, 32.8 percent (439 million people in 2017) of the population has been leaving in urban. The median age of country has been measured as 27.0 years. This population can divided in dependent and working population. Working population is known as workforce or employed population of the country, which has considered as age group between 14 to 59.

The dependent population is considers below 14 year age. If they found in work it has classified as child labour, which law do not allow. The age above 59 year considered as old age persons in population. This dependent population of country is called unemployed and non-worker population. Population of Country has classified in (1) workforce means employed persons, the (2) labour force contains employed plus unemployed persons and (3) the non-workers are not doing any economic activity, where the unemployed and the non-workers are the dependent population of country. Here the research topic has selected “SOCIAL NETWORKINGS IN UNORGANISED SECTORS & CONCERNS OF CYBER SECURITY”

Social Networking describes the phenomena found in, participatory and self- expressive Web sites—such as YouTube, MySpace, Facebook— where members/participants expose, discuss, reveal, and expound

on their personal lives, activities, hopes, dreams, and even fantasies for others to see and marvel upon. Online communities represent a growing class of marketplace communities where participants can provide and exchange information on products, services, or common interests. Brands are, or have been, the commercial enterprises' approach to building social networks. They have created brand cohorts through logos, colours, and clever icons. All of these "brands," and the imagery and mystics behind them, have really been nothing more than attempts by the marketer to create a social network that was accepted and that engaged people to purchase or continued to purchase products or services. Companies are increasingly using online communities to create value for the firm and their customers. **Cyber risk** commonly refers to any **risk** of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems. ... Deliberate and unauthorized breaches of security to gain access to information systems. Unintentional or accidental breaches of security. **What is concerns of Cyber Security Important?** ... And while companies and institutions are constantly working to protect themselves with increasing **security** measures, you can play a role in this fight as well. When you are aware of the risks, it may be much easier to protect yourself from hackers, viruses and malware. Ensuring that brand activity is relevant to a social network's core audience is crucial for advertisers wanting to tap into niche communities. In this project we develop a framework that explores the process of how a firm's online community enhances consumers' brand commitment.

Key Words: Brand Commitment; Online Communities; Online Communities Commitment; Social Networking;

CYBER THREATS FOR NEW RENEWABLE SOLAR ENERGY SYSTEMS

Pramoda Kumar Behera

General Manager, Heavy Engineering Corporation Limited,
Research Scholar, Jharkhand Rai University Ranchi.

Abstract

The cyber security threat is real and even the biggest and secured solar installations aren't immune to it. The digitalization of smart power grids with increasing connectivity of solar power plants put the PV assets on high risk by illegitimate hackers who can break into the grid security, which can put the power supply at risk. What started as an industry built upon mechanical and structural engineering elements using solar power has now an equally robust software engineering component, making it susceptible to cyber security threats. Most people would not consider cyber attacks on solar plants to be capable of causing much damage. Researchers, however, have shown that such threats should not be taken lightly. There are multiple vulnerabilities found in products manufactured by the leading providers of PV assets. A serious cyber attack against solar panels could shut down an entire nation's power grid. Due to security vulnerabilities, hackers could disable grids and transformers remotely. Disabling the solar power system and grids at the same time could disrupt the power supply and would result in electrical grids getting knocked offline. Solar plants are part of a global, interconnected network that allows plants to draw power from those who have a surplus available.

The grids are operated based on the expected amount of power generated and power consumed. Any disruption to that balance could result in the shutdown of the entire grid. For a country like India, where solar energy is in the verge of elevation at a given time, such an attack could be devastating. It is understood that, it's too costly for developers to keep large supplies of powers on standby at all times, meaning most countries wouldn't have the type of energy reserves available to cover the lost production at a plant that falls victim to a cyber attack. The Concerns about the cyber security of the electric grid are widely recognized

and shared. The fundamental issue at stake is to determine next steps for improving grid security and how to prioritize these steps among all of the other issues that face the industry. The potential for malicious hackers to access and adversely affect physical electricity assets of India electricity generation, transmission, or distribution systems via cyber means is a primary concern for utilities. But in the last few months, several notable clean energy companies have taken steps to reduce the risk of a breach. The solar energy sector is sharpening its focus on solar cyber security amid growing concerns about cyber threats. Any software that has network access, security software and data infrastructure should be continuously monitored and kept up-to date to stay defensive against the latest cyber threats. In India to enable comprehensive cyber security policy compliance, the government mandated implementation of security policy within government agencies in accordance with the Information Security Management System (ISMS) Standard ISO 27001. Computer Security Guidelines have been issued for compliance within government and are being circulated to all departments and ministries. Cyber security drills are being conducted to assess preparedness for critical organizations. With cyber threat looming around the vulnerable energy assets, its time for the government to foster and promote enhanced cyber security within the renewable sector. It may require a further push from governments and/or regulators to mandate measures and practices to achieve awareness and preparedness on a broader scale.

Keywords: Cyber security, solar system, Cyber attack, Cyber threat.

VIOLATION OF FUNDAMENTAL RIGHTS AND CYBER JUSTICE MECHANISM IN INDIA.

Rajesh Kumar & Rahila Imam, (Research Scholar, CNLU & LLM)

Abstract

The latest advancements in the field of computer and technology have made the working patterns of society and state very different from the conventional ways. Now everyone is enjoying the benefits of the technology because of its accurate, expeditious, and easy way of doing things. The concept of e-commerce, e-education, e-governance has emerged due to this. The use of computers and the internet is inevitable today. But recent development and usage of computers by the government and private parties has increased the risk of security breaches of the sensitive and personal data of the citizens of the country and often it has been seen the mishandling of the personal information of the person's due to lackness in providing safeguards and a concrete data protection mechanism adopted by the government and also the private parties. In the case of M.C Mehta v UOI Hon'ble SC has held that whenever there is an infringement of the fundamental rights that are provided in part III of the Indian Constitution happens, the liability would lie on both the government and the private agencies.

In India, there is a concept of eminent domain and even it also is subject to fundamental rights of the citizens. But when we see today, there is always risk of the infringement of fundamental rights, when the sovereign power in the form of e-governance is performed and personal data and privacy are threatened by the state. In these circumstances, major role is to be played by the judiciary to protect this intervention and infringement and also the courts have to provide justice to the victims expeditiously. In this context, this paper will study which of the fundamental rights of the citizens are often affected and what the honourable courts has to say on these infringements, along with the different guidelines issued by it in different cases to tackle this menace of infringement and protection of the rights of affected persons. This paper also includes the working pattern highlighting the lacuna in imparting cyber justice when the violation of fundamental rights occurred.

Keywords: Eminent domain, Fundamental rights, E- governance, Privacy.

SCRUTINY OF DATA PROTECTION LAWS IN INDIA

Dr. Aseem Chandra Paliwal, Associate Professor & Ms. Megha Middha, Assistant Professor, Mody University of science and Technology, Lakshmgarh

Abstract

In India, we have so many laws for one or the other subject matter but when it comes to data protection, there is no law existing in the country and with the technology becoming so advanced, the information of one person is seen being transmitted from one person or organisation to the other without the consent of the person whose information is being transmitted and this is leading to the breach of privacy of personal information of the individuals. Technology has a great role to play in the present scenario in almost all the fields and this technology along with Internet has been able to do wonders which once we could have only imagined. For example it helps us to connect with people sitting miles away, have audio calls, video chats, sending of electronic mails, online shopping, electronic banking, online transactions, taking appointments, booking hotels, online plane, railway or bus tickets, etc. In short, the technology has made the things easier by saving a lot of time and other kind of costs attached. Today because of technology and internet related things, we are able to take advantage of the various websites like Flipkart, Amazon, Myntra, etc.; in addition to this, we now have Skype interviews as well, we have now Aadhar cards where biometric information of people is collected against which many questions were raised violating our fundamental right to privacy. Similarly, today we see our personal information is seen being collected by various online sites, banks, other financial institutions, health centres, educational institutions etc. Author in this article shall look:

- look into various laws existing in India with respect to data protection
- look into various laws existing in India with respect to data protection.
- look into the laws that are existing outside the country for the protection of data.
- look into Data Protection Bill which was introduced and the lacunas it had.
- look into the White Paper which was brought up by the Government and thereby analyzing the various aspects relating to the data protection law.

Key-words: Data Protection Bill, Privacy, personal Data

CYBER CRIMES IN INDIA: LEGISLATIVE AND JUDICIAL RESPONSE

Dr.Akhilesh Kumar Pandey & Manisha Pandey

Associate Professor, Karnavati University, Gandhinagar Gujarat. & Student, FOL, ICFAI University Jharkhand

Abstract

Indian Parliament has passed the first legislation in the Fifty-first year of the Republic of India called as the Information Technology Act, 2000 which is based on the resolution adopted by the General Assembly of United Nations regarding the Model Law on Electronic Commerce on January 30, 1997 which is earlier adopted by the United Nations Commission on International Trade Law (UNCITRAL). This resolution recommends that all States must give favorable consideration to this Model Law when the States are going to enact or revise their laws with the view of uniformity of law as alternative to paper based methods of communication and storage of information. India was also the signatory to this Model Law and had to revise its national laws as per the said Model Law. Therefore, India also enacted the Information Technology Act, 2000 for providing legal recognition to the transaction carried out by means of electronic data interchange and other means of electronic communication and to facilitate electronic filings of documents with the Government agencies. The Act further amends the Indian Penal Code, 1860,

the Indian Evidence Act, 1872, the Bankers Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934. The provision of this Act are not applicable to some instruments i.e. a negotiable instrument, a power of attorney, a trust, a will, including any other testamentary disposition, any contract for the sale or conveyance of immovable property or interest in such property and any such class of documents or transactions as may be notified by the Central Government in the Official Gazette. Though since 2000 the Information Technology Act is in place in India for curbing cyber crimes, but the problem is that still this statute is more on papers than on execution because lawyers, police officers, prosecutors and Judges feel handicapped in understanding its highly technical terminology. Primarily, the IT Act, 2000 is meant to be a legislation to promote e-commerce which is not very effective in dealing with several other emerging cyber crimes like cyber harassment, defamation, stalking etc. There was a need to amend the Information Technology Act, 2000 for the purpose of making it more relevant in today's context. For this purpose the Information Technology (Amendment) Bill, 2006 was proposed which was further amended by Information Technology (Amendment) Bill, 2008 and passed in Lok Sabha on Dec. 22 and in Rajya Sabha on Dec. 23, 2008. Then the Information Technology Act, 2000 is amended by Information Technology (Amendment) Act, 2008.

The current position of Indian cyber cases are increasing day by day. A total of 8, 045 cases were registered under Information Technology Act during the year 2019 as compared to 7, 201 cases during the previous year 2018 and 4,356 cases during 2017, showing an increase of 11.7% in 2019 over 2018 and an increase of 65.3% in 2018 over 2017. 81.6% of the total 8,045 cases in 2019 and 77.0% (5,548 cases) of the total 7,201 cases under IT Act were related to computer related offences (under section 66A, 66B, 66C, 66D and 66E of the IT Act) followed by 10.1% in 2019 and followed by 10.5% in under publication/ transmission of obscene/sexually explicit content (under section 67A, 67B and 67C of the Information Technology Act). A total of 14, 121 cases during 2019 and 2,246 cases during 2018 under Information Technology Act were pending for investigation from previous year. A total of 8,088 at the end of the year 2019 and 6,269 cases at the end of the year 2018 were remained pending for investigation. A total of 2,396 during 2019 and 1,451 cases during 2018 were charge sheeted. A total of 2,316 remained pending for the trial at the end of the year during 2018. Uttar Pradesh and Maharashtra has reported the maximum number of persons arrested under such crimes during 2019 as well as in 2018. As a result of the rapid adoption of the internet globally, computer crimes are multiplying like mushrooms. The law enforcement officials have been frustrated by the inability of the legislators to keep cyber crime legislation ahead of the fast moving technological curve. At the same time, the legislators face the need to balance the competing interests between individual rights such as privacy and free speech, and the need to protect the integrity of the world's public and private networks. Moreover while investigating cyber crimes, the investigating agencies and law enforcement officials follow the same techniques for collecting, examining and evaluating the evidence as they do in cases of traditional crimes. It is concluded that the due to this Indian legislative as well as judicial framework is found to be inadequate to face the threats posed by cyber crime, which have emerged as a challenge to human rights. Because there has been less judicial response to cybercrimes and insufficient legislations for dealing with these types of crimes which will be a great challenge for Indian judicial system on cybercrime in near future.

Right To Be Forgotten: An Overview of the Ongoing Legislative and Judicial Developments

Ms. Priyanka Chowdhary & Uzma Sohail

Assistant Professor, UPES, Dehradun & Student, FOL, ICAFI University Jharkhand

Abstract

The digital universe is huge and the 21st century has seen a tremendous rise in the manner we utilize the data or information. Much of the digital data or information we are talking about will consist of the personal details of an individual, which also includes the things they buy online, the place they visit and the data collected by the smart devices, which they use while connected to the internet. With digital technologies playing an integral part of the life for almost every individual today, we are losing control over such data and ends up in the violation of the right to privacy. Thus, keeping in mind the same, political voices have already started stressing upon the need to introduce a right to be forgotten, which is a subset of right to privacy, as new human right. Right to be forgotten is type of data protection rule whereby a person's imprint in any media record can be erased in order to give him relief from unwanted publicity. An individual subjected to the right to be forgotten will have the right to request the server the removal of any information regarding their personal life which for the time they consider have become inaccurate, inadequate or irrelevant. The European Union's (EU's) and many other countries including United States either have already implemented data protection requirements or are in the process of considering them. India, too, is taking steps to enact a data protection framework modelled along the lines of The European Union's (EU's) General Data Protection Regulation (GDPR). *Therefore, the author through this research aims to analyze the conception and development of the right to be forgotten and proceeds to explore the contextualization of the right to be forgotten in India and other territories along with the recent judicial trends.*

Keywords: Right to be Forgotten, GDPR, Human Rights, digital technologies.

JUDICIAL INTERPRETATION OF DATA PROTECTION AND PRIVACY IN INDIA

Nidhi Kumari & Siddhant Chandra

Student, Department of Criminology, Jharkhand Raksha Shakti Univesity

Abstract

The convergence of technologies has originated a different set of issues concerning privacy rights and data protection. India has not yet enacted specific legislation on data protection. However, the Indian legislature did amend the Information Technology Act (2000) to include section 43A and Section 72A, which gives a right compensation for improper disclosure of personal information. The Indian Central Government subsequently issued the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under section 43A of the IT Act. In a landmark judgment delivered in August 2017 (justice K.S.Puttaswami & another vs. union of India) the Supreme Court of India has recognized the Right to Privacy under Article 21 of the Constitution of India as a part of the Right to "life" and "personal liberty". Information Privacy has been considered as the right to privacy and the court held that information about a person and the right to access that information also needs to be given the protection of privacy.

This paper aims to initiate concern over the data protection and right to privacy issues in Indian perspective keeping in view the ongoing development in technologies. Case Study method and Data Analysis method is

used with qualitative approach and exploratory research technique for the study. However, IT Act does not clearly define the protection of data and its privacy issues, and a separate legislation is needed to maintain a balance between data protection and privacy.

FIXING THE ACCOUNTABILITY OF INTERMEDIARIES AND DATA REPOSITORIES TO PROTECT PERSONAL AND SENSITIVE DATA-STATE SURVEILLANCE VS RIGHT TO PRIVACY

Aditya Jain

Advocate, Supreme Court of India and Rajasthan High Court

Abstract

Data surrounds us and is generated in virtually everything we do. One type is data that we may voluntarily share, and the second type is the data which is generated literally every time we do something – whether it be travel, order a meal or use transportation. There is no doubt that this data is immensely valuable and several companies are willing to pay for access to this data. Indeed, in this age of universal and virtually free access of internet, data is the new currency. What is even more intriguing that the full potential of the data is not known. As technology progresses, newer applications emerge enhancing the value of the data.

Article 21 of the Indian Constitution is a fundamental right that guarantees protection of life and personal liberty. On August 24th, 2017, the Supreme Court in the decision of *Justice K.S. Puttaswamy (retd.) & Anr vs. Union of India and Ors* held that privacy is a constitutionally protected right which arises out of Article 21 of the Indian Constitution. The protection under Article 21 is not absolute and is subject to certain restrictions. For instance, the right could be restricted if there is a law created by the legislature to restrict the same (such law should promote a legitimate state interest, should not be arbitrary and should be proportionate to the object of the law). A draft Personal Data Protection Bill is presently under consideration. As on date, the current framework for data protection is set out in the Information Technology, 2008 («IT Act») and the rules issued thereunder, most importantly the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 («IT Rules»).

Under section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. There are other provisions of the IT Act as well, which can be put into play, but still the present IT Act coupled with rules remains insufficient. Instrumentally, a firm legal framework for data protection is the base on which data driven innovation and entrepreneurship can flourish in India. Fostering such innovation and entrepreneurship is essential if India is to lead its citizens and the world into a digital future committed to empowerment, experiment and equal access.

Section 3 of the proposed Data Protection Bill, 2018 provides definitions such as ‘Sensitive Data’ which is data relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity, or any combination of such features. ‘Personal Sensitive Data’ according to the section includes passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief.

By way of this paper, the authors will highlight the key aspects of intermediary liability and liability of data

repositories under the new IT Act and guidelines and newly proposed Personal Data Protection Bill. The author will also take into perspective GDPR Guidelines, California Privacy Act and other such international statutes and how they have played a critical role in determining the Indian jurisprudence on data protection and privacy. In the end, the authors will try to answer the key question as to how we can balance the aspect of State Surveillance Vs Right to Privacy of an Individual under the legal regime.

Keywords: Data Protection, Privacy, Sensitive, Personal Data, Article 21, Right, Duties, Intermediary, Repository

TERMS AND CONDITIONS VIS-À-VIS DATA PRIVACY: A STUDY

Peter Ladis F

Assistant Professor of Law, CNLU Patna

Abstract

Justice K. S. Puttaswamy (Retd.) and Anr. vs. Union of India and Ors is a landmark judgment wherein and whereby the Supreme Court of India has declared Right to Privacy as an intrinsic fundamental right under the golden triangle of the Constitution of India. Today there are ample number of instances whereby this fundamental right is being infringed by the service providers of internet uses and telecommunication agencies.

When one is desirous to purchase the services of a company, it gives a sets of terms and conditions which are difficult to read and the services shall be provided only when one agrees with the terms and conditions. The web engines also give a similar provision and one can utilise their services only when one agrees to the terms and conditions. There are mobile operating systems which can be downloaded freely but they can be used only when one agrees to the terms and conditions. All the above said agencies take the name and other private particulars of an individual before providing the services. Disclosure of these data with private agencies for commercial purpose does infringe one's fundamental right. Hence, this research paper studies the pros and cons of these terms and conditions and data privacy. The paper also analyses the constitutional validity of such conditions.

Key Words: Terms and conditions, Data Privacy, Fundamental Rights, Constitutional validity.

ARTIFICIAL INTELLIGENCE AND INDIAN LEGAL SYSTEM: AN ANALYSIS

Samrat Datta & Rakhi Kumari

Assistant Professor of Law at Faculty of Law, ICFAI University, Himachal Pradesh (Baddi) & Student, FOL, ICFAI University Jharkhand

Abstract

The domain of Indian legal system is dynamic in nature and is changing ever since its inception. The Indian legal system is always in its efforts to compete with the modern day technology to be at the same footing with the other developed nations. In its endeavour to do so, information technology, modern devices of law enforcement and various other mechanisms are being utilised on a day to day basis so that the dynamic nature of law is well established and rule of law is preserved. However, it is important to note that artificial intelligence or AI has become the need of the hour. The way modern society is changing, it is indeed a great challenge ahead for the legislature and the judiciary to make and implement the laws for the betterment of the society in the domain of artificial intelligence. Today, it might seem abstract, but sooner or later AI is definitely to be one of the sine quo non for the Indian society and the legal system needs to think about including AI under the domain of the Indian Legal System. The problem associated with AI is that presently there is no law with regard to AI. Now, no technology or for that matter nothing can operate

in vacuum. If there is any scope of AI or if the technology is prevailing in the coming decade, laws need to be made in advance to protect the hazards that can occur and also safeguard the rights of the users of AI. The paper highlights the need for AI today, its impact on the socio legal scenario of India and finally the implications of AI in the future. The paper also suggests the need for a proper structural framework so as to preserve the Indian Legal System and the difficulties associated in the domain of AI.

Keywords: Indian Legal system, AI, Cyber security, Structural Framework.

AN ANALYSIS OF THE CYBER SECURITY POLICY 2013 IN WAKE OF THE NEW CYBER SECURITY STRATEGY 2020

Ms. Disha Atri & Dr. Sagar Kumar Jaiswal,

Assistant Professor,

Guru GhashidasVishwavidyalay, Bilaspur (C.G.)

Abstract

The Government of India is all set to release its cyber security policy this year. This policy is supposed to be a rather ambitious project, given the amount of time, effort and resources which are being invested in it. The policy would encompass and apply to the entire realm of internet users in the country, whether Government or private, individual or organisation, providing an umbrella security to all its users. The NSCS, i.e., the National Security Council Secretariat appointed a task force to formulate a strategy for cyber security, which would be effective for five years. The project is being highly anticipated and already being seen as a revolutionary reform. The strategy is yet awaited, and cyber security is still regulated by the previous policy, i.e., Cyber Security Policy 2013. It would therefore be vital for us to take a look at the policy of 2013 and analyse its pros and cons, so as to make our expectations from the new strategy. The researchers in this paper would attempt to study the cyber security policy of 2013 and the effectuality of the policy, with respect to its contents, keeping in mind the objectives of the Government behind framing of the same.

Keywords: Cyber security Policy, NSCS, Privacy.

INTERMEDIARY LIABILITY IN INDIA FOR THIRD PARTY CONTENT

Mr. Sushil Jain & Dr. Ajai Singh,

Assistant Professor, Guru GhashidasVishwavidyalaya, Bilaspur (C.G.)

Abstract

With the increasing cases of cyber-crimes particularly relating to circulation of false information via social media, it has created challenge for policy makers to curb the menace. The road-block which authority faces generally is who all are liable for circulation? One question arises that whether only the person who circulates the false information is responsible or the platform (intermediary) is also responsible. However, Section 79 of Information Technology Act, 2008 gives protection or exemption to intermediary for any acts of third party while using the service given by service providers. The above-mentioned protection was given on the criteria that at that time information technology was in primitive stage. However, today after 20 years of enactment some of the intermediary like Google, Facebook, etc are big corporation and they can properly bear the liability as they have required resources as well as mechanism to detect and curb the circulation of false information.

The present paper is written for the same purpose to scrutinize the possibility of whether intermediary liability for third party contents which is circulated in their platform is possible in India or not. Research

paper will further discuss the connection of aforesaid liability with individual Fundamental right of speech and expression. Furthermore, it will delve deep into the relation of aforesaid liability with natural justice principle. Lastly, the paper will compare the existing European Union law relating to intermediary liability for third party content with Indian law i.e. Information Technology (Intermediaries) Rule, 2011 and to check whether European Union law can be applied in India with necessary modifications.

Keywords: IT

SOCIAL NETWORKING AND CONCERNS OF CYBER SECURITY

Tripti Bhushan & Rahul Kumar

Assistant Professor, Kalinga University, Raipur & Student, FOL, ICFAI University Jharkhand

Abstract

In the present scenario one of the quickest developing territories of specialized framework improvement is the Internet. The expanding digital assaults which are faced by the people over the previous decade are representing a genuine risk to the computerized world. The paper revolves around the issues of digital security for Social Networking Sites (SNS) and concern of cyber security since web based life appropriation among people and organizations is soaring. Long range informal communication Sites have numerous territories of uses like advanced advertising, social online business and marketing. The way that the most extreme number of clients don't know about dangers and their absence of information prompts further increment in digital wrongdoings is a significant test. Every one of these issues would shape a piece of the paper that would be presented before the audience. The security concerns and difficulties on SNS like personality abuse, malware, phishing assaults and outsider application dangers have additionally been talked about independently. While featuring the administration activities to check this major issue, the paper likewise recommends some proper arrangements which can be embraced by the individual clients just as the legislature in the coordinated effort with private area for a digital safe computerized world. This study features the issues applicable to current digital assaults on informal communities, challenges, and the potential approaches to defeat the digital crooks from getting to the interpersonal organizations and causing harm. At long last, it presents significant proposals for keeping the informal organization from digital assaults for better comprehension of the field and also covers the problems faced by the social networking sites. Digital security assumes a huge job in the present advancement of data innovation and administrations.

Keywords- Cyber Security, Social Networking Sites, Security issues, Cyber Crimes, Digital world, malware, security awareness.

LEGAL FRAMEWORK OF CYBER SECURITY: INDIAN PERSPECTIVE

Simran Kumari & Shubhangi

Students, ICFAI University, Jharkhand

Abstract

The policy formulation of cyber security in India has traditionally been associated with sovereign consideration particularly with the issue related to state sponsored terrorism and internal security. The 1st attempt to define Cyber Security is being attempted in Information Technology Act 2000. However such attempts are also not sufficient to cover all issues of cyber security but the same was appreciated that at least it started to address the issue. In 2004, The Indian Computer Emergency Response team was established that plays a dominant role in cyber security in India. By amending Information Technology Act in 2008, CERT-in has been designated to serve as National Agency to perform the functions in cyber security area.

The National Cyber Security Policy 2013 is enlightening as to the India policy objectives. The objective of 2013 policy highlights the social and economic significance of protection of personal data and protecting against cyber crime. Such policy is important as much as it recognizes the various assets of cyber security. In this paper, researcher tries to trace out the legislative history relating to cyber security in India and how far the existing legal framework is sufficient to deal such multi dimensional challenges of cyber space.

ISSUE OF JURISDICTION IN COMBATING CYBER CRIMES

Kamlesh Kumar

Asst. Prof. CNLC, Ranchi University Ranchi Jharkhand

Abstract

Computers with the aid of the Internet Have today become the most dominant medium of communication, activities, growth of Newer and varied kinds of crime are information, Commerce and entertainment. The Internet is at once several shopping malls, Libraries, universities, newspaper, television, movie theatre, post office, courier Service and an extension of government and business. It is like life in the real world being extended and carried on in another medium that cuts across boundaries, space, time, nationality, citizenship, jurisdiction, sex, sexual orientation, and age. The Internet, with all the benefits of anonymity, reliability, and convenience has become an appropriate breeding place for persons interested in making use of the Net for illegal gainful purposes, either monetary or otherwise Since anything related to the Internet was being prefixed with the word 'cyber' the However, the word 'cyber crime', by its very terminology, restricts itself to the offences committed on the Internet. The term is liable to be given a restricted meaning. It is for this reason that the authors have preferred the word 'computer-crimes' rather than 'cybercrimes' which, in its wider ambit, would encompass offences committed in relation to or with the help of computers. Defined broadly, the term 'computer crime' could reasonably include a wide variety of criminal offences and unlawful activities related to or having connection to computers. The potential scope is even larger when using the frequent companion or substitute term.

CYBER SECURITY, LEGISLATION, REGULATION AND ENFORCEMENT

Prabhash Nath Jha & Arvind Kumar Jha

Asst. Prof. CNLC, Ranchi University, Ranchi

Abstract

Due diligence for preventing cyber crimes- India is the third largest user of internet in the world today. We use mobile phones and computer for caring out banking transactions, shopping and other day to day activities. Internet, mobile phones and computer are used in abundance leading to increase in case of Cyber crime; however a digitally literate and well informed citizen can avoid a number of cyber crimes from taking place.

India has no specific cybercrime legislation. The IT Act and Penal Code cover cybercrimes punishable in India. There is no obligation under the IT Act or the rules made there under to keep records of any security incident. However, from a limitation perspective, companies should retain all such records for a minimum period of three years. Cyber crime can be categorized as

1. Crime against property
2. Crime against Government ,
3. Crime against person.

Crime against property: includes financial fraud, vishing fraud, job scam social media fraud, IPR crimes,

salami attack, data modifications etc. Crime against persons: It includes identity theft and impersonations, data theft, pornography, etc. Crime against Government: it also covers cyber espionage, cyber terrorism.

Preventive measures:

Advisories have been issued by the Ministry of Home Affairs (MHA) to states and Union Territories in the country on the steps to take to prevent cybercrimes, which are available on the Ministry's website. The Ministry of Home Affairs, is implementing the 'Cyber-Crime Prevention against Women & Children' Scheme with the intent to prevent and reduce cybercrimes against women and children. The Ministry of Home Affairs has constituted an Inter-Ministerial Committee on Phone Fraud and has issued advisories to states and Union Territories on the ways to check and handle phone frauds.

RIGHT TO PRIVACY vs STATE SURVEILLANCE: ISSUES AND CHALLENGES

Mrs Sakshi Pathak & Mrs Lalsa Mohini,
Assistant Professor, Chotanagpur Law College, Namkum

Abstract

Privacy today seems interrupted and infringed to every citizen. The legal codification and protection of data is significant but complex. This is because varying expectations of privacy exist in different social contexts demanding different forms and degrees of protection. Under the Constitutional privacy protection the Supreme Court of India ruled that the Indian constitution guarantees a right to privacy. But in India, an unambiguous and enforceable constitutional right to privacy does not exist. The Supreme Court of India has, intermittently and unconvincingly, recognized a limited right to privacy in certain situations when the Government exercise its rights. So it is important to understand the contours of the right to privacy and its restrictions in India with respect to state surveillance. State surveillance and citizens' right to privacy have been at the forefront of international debate since the explosive Snowden disclosure. The primary focus of debate today is on surveillance and data protection. The statutory regulation of surveillance in India is in an uneven and incomplete. Bearing this state of affair there is a war between right to privacy and state surveillance process.

This article presents an analytical and complete study of the Indian Supreme Court's engagement with the right to privacy. While discussions for a privacy statute have stagnated and are presently in limbo and facing complexities this article aims to achieve a comprehensive, doctrinal understanding of the constitutional right to privacy and state surveillance, as evolved, understood and implemented by the judiciary. Such an understanding, indeed, is an essential prerequisite to embarking upon a legal and constitutional critique of mass State surveillance in India. With this growing domestic intricacy that is alarming the state's collection of personal data without regulatory safeguards.

Key words- Right to Privacy, Mass State Surveillance, Democracy, Supreme Court, State

DATA PRIVACY AND AADHAAR

Mahima Agarwal & Komal Kumari

**Faculty Associate, ICAFI Law School, The ICAFI University, Jaipur & Student, FOL, ICAFI
University Jharkhand**

Abstract

The Aadhaar project of the Government of India is the most ambitious program in the world which aimed at issuing unique 12 digit numbers to every Indian as well as recording their biometrics for authentication services. A data leak would be potentially disastrous and would constitute a major breach

of privacy as well. Such a leak can take place at the application level, network level and the storage level. Data pertaining to the number of data breaches in the past decade have been analyzed to emphasize the importance of a secure ecosystem for such an ambitious project. A new methodology has also been studied which will help in heightening the security of the Aadhaar ecosystem and safeguarding the privacy of the people better.

The present article would focus on how Privacy is every Indian citizen's right and what measures should be adopted by the government to ensure that privacy is maintained in every situation. In case of Aadhaar, it contains all the personal information related to a person which can be misused by any person in the world. Therefore, cyber security is a major concern for everyone and it is the need of an hour that we should those suitable actions must be taken to ensure such cyber security in India.

Index Terms— Privacy, security, cryptography, authentication, identification, ecosystem

DATA LOCALIZATION AND CROSS-BORDER DATA TRANSFERS

Abhinav Kumar Singh & Deep Raj

Advocate, Patna High Court, Patna.

Abstract

Today, data is a real wealth and it is being said that whoever acquires and controls the data will have hegemony in the future. The global flow of data is creating big opportunities as well as challenges.” Data localisation is the process which involved in localising the data of the citizen to their home country for processing, storing and collecting the data before it reaches to the international market. This is done with the motive to protect data and its privacy laws. The basic of it is entirely based on data sovereignty.

Indian market is one the emerging market in the affairs related to the data breach and privacy threat. The legislature is now highly active to come up with a concrete solution for it in the form of The Personal Data Protection Bill, 2018(“The Bill”) and also the Data Protection Committee Report which was released on 27th of July 2018. Furthermore the draft legislation, the Digital Information Security in Healthcare Act got published by the Ministry of Health and Welfare, where a mandate to localise was issued by the RBI.

Data localization is an *opportunity for Indian technology companies to evolve an outlook from services to products*. International companies will also be looking at the Indian market, and this will benefit the growth of the local ecosystem.

Thus we can say that Indian Government has adopted very futuristic view in terms of Data Localization. In the era of Internet where privacy has become a myth, it is very essential for the Government to localise data for the sake of securing citizen's data, data privacy, data sovereignty, national security, and economic development of the country. Digital technologies like machine learning (ML), artificial intelligence (AI) and Internet of Things (IoT) can generate tremendous value out of various data.

Key Words: - The Bill, Data Sovereignty, ML, AI, IoT

A QUESTION ON THE CO-EXISTENCE OF UNIQUE IDENTIFICATION NUMBER (UID) AND RIGHT TO PRIVACY.

Paridhi Shrivastava, Gaurav Purohit & Sourav Kumar Vardwaj

Students, Jagran Lakecity University & student, FOL, ICAFI University Jharkhand

Abstract

This article lays emphasis on the system of UID's and breach of privacy of the citizens. With the emergence of big data, governments can now collect, process and scrutinize data from millions of people.

While governments have defended their actions on the basis of national security, citizens' concerns about their privacy rights still remain unaddressed. This article accentuates on the breach of the privacy caused by linking the Aadhar numbers with the benefits and services provided by the government. It also deals with the issue of dignity of the people of the country which is provided in article 21 of the Indian constitution and hence germane to the privacy issue.

Further, the article discusses in detail the recent landmark judgement on right to privacy by the supreme court of India. The judgement is supported by various case laws by the court supporting the right to privacy. This article answers several questions and arguments made on privacy and also evinces how the National Identification Authority of India Bill is not in tandem with privacy of individuals. Finally the article concludes with the strategies available to tackle and nullify the effects of privacy issues.

Key words: Privacy, Big Data, National Security, UID.

CYBER SECURITY ISSUES IN INDIA

Dr Anupam Manhas & Tudsii Kudadah

Assistant Prof, Career Point University Hamirpur H.P. &
Student FOL, The ICFAI University Jharkhand

Abstract

The development of e commerce has opened up a whole new world full of challenges related to cyber security. Cyber security poses bigger threat than any other spectrum of technology. The Digital India initiative is driving our country towards a digitized life where the existence will highly depend on elements like cloud computing, 5G in telecom, e-Commerce etc. it is imperative to keep a check on loose ends. The issues concerning cyber space are Digital Data Threat, Supply Chain Inter-connection, Hacking and Phishing. These challenges can be under surveillance and methodical steps can be taken to avoid such malpractices. These challenges may be tackled by making people aware of technologies and cyber issues, .having strong anti-cyber-terrorism-wings, employment of ethical hacker in govt. offices and educating the youth about cyber security and related issues as a part of their formal education.

CYBER LITERACY AN INITIATION TO CYBER SECURITY

Tulika Sinha

Assistant Professor Usha Martin University, Ranchi

Abstract

Cyber-crime and cyber security are two important aspects that one need to be acquainted with it in the current time. Presently where almost every activity is based and dependent on cyber technology zero knowledge can be really bearing and a partial knowledge can be lethal and operate against ones interest. So it becomes inevitable that one who is dealing with cyber world directly or indirectly must have some knowledge of the same. It is only about walking with time but also about securing ourselves.

In this paper I have mainly made an attempt to throw light on the kind of cyber world we live in and the urgent need to learn about it in order to avert the issues that arise due to the lack of cyber education. Hence the emergent need of cyber literacy and the rights and redressal of the grievances relating to cyber world is the central idea of the paper.

Keywords: Cyber crime, Cyber security, Internet literacy.

EFFICACY OF CYBER SECURITY LAWS: A CRITICAL STUDY

Dr. Vijay Kumar Vimal & Vivek Kumar Saha

Assistant Professor of Law, Chanakya National Law University, Patna

Abstract

The Internet has revolutionized modern life across the globe, enabling dramatic advancements in technology and communications. Furthermore, the Internet has triggered a dramatic improvement in the efficiency and capabilities of people, organizations, and governments around the world. Regretfully, the Internet also exposes its users to increasing collection of new risks and vulnerabilities. These risks affect organizations and individuals across the planet, but they also pose unique threats to nations.

From the rise of extensive cybercrime, fears of terrorists exploiting digital infrastructure, state and corporate cyber espionage, crippling disruption by cyber activists and even suggestions of cyberspace becoming the fifth element of warfare (along with land, sea, air and space) the issue of cyber security has become extraordinarily important global issue. The range of cyber adversaries varies from teen hackers to organized crime groups, industrial spies, terrorists, and even governments. Despite an attacker's identity or motivation, a successful intrusion could cost a company a lot of trouble - financial losses, data leaks, business disruptions, or infrastructure failures. The global market is becoming more and more interconnected, with new stakeholders joining every day, meaning that a cyber-attack on one company could easily trigger unexpected negative events in others. Keeping information and operations secure, this is of vital importance for any enterprise, which becomes the task of cybersecurity.

It is believed that a dedicated cyber security law of India is need of the hour. The same must be a techno legal framework keeping in mind contemporary cyber security threats. The cyber security awareness in India must be further improved so that various stakeholders can contribute significantly to the growth and implementation of cyber security initiatives of Indian government. This paper endeavors to addresses the all the possible concerns of cyber security and its legislation.

Key Words: Cyber security, Cybercrime, Cyberspace, Cyber warfare.

STATE SURVEILLANCE IN INDIA: A COMPARATIVE LEGAL STUDY

Sunkara Vishnu Ameya

2nd year Law Student,

DamodaramSanjivayya National Law University

Abstract

In the case of K.S. Puttaswamy v. Union of India, the Supreme Court of India held that Right to Privacy is a Fundamental Right inextricably linked to Article 21 of the Constitution of India. But there have been a lot of concerns regarding the State interference with ones data in this today's digital age. The present paper would delve into the dimensions of the Constitutional History of surveillance by the state and the Central Monitoring System which grants access to communication data to certain agencies. The study would do an analysis of the K.S. Puttaswamy judgement in this regard. The study would do a comparative study with the 4th Amendment of the US Constitution and the European Union Regulations 2016 in this regard.

Keywords: Privacy, Fundamental rights, Surveillance, Central Monitoring system.

LEGAL FRAMEWORK FOR CYBER SECURITY UNDER IT ACT, 2000.

Astha Bhatt & Reshav Kumar Mandal

Student (2nd Year), Faculty of Law, The ICFAI University Jharkhand.

Abstract

As a result of rapid proliferation of computer technology and the internet in India, the IT Act was enacted in the year 2000. Section 2(1) of the IT Act in India define the term cyber security as far as legislative intent behind defining cyber security serves very little about what the cyber security mainly consists. However the IT Act did not adequately address the issue of cyber security, it only introduced some penal provisions for cyber crimes. This paper is mainly based on the comprehensive study of penal provisions for cyber crime under IT Act 2000.

Keywords: cyber crime, cyber security, legal framework.

POLE STAR ON A MOONLESS NIGHT OR JUST ANOTHER IOTA OF SAND IN THE DESERT?AN INTRICATE ANALYSIS ON THE PERSONAL DATA PROTECTION BILL, 2019

Swaraj Kariya & Ujjwal Sheth

Abstract

In times when data analysing companies in the garb of “political consultancies” can manage to manipulate entire elections, in times when every input on the internet leaves behind a digital footprint, in times when Right to Privacy online is just a myth and the real meaning has gone to the gutters; it is up to the governments of the states to be nonchalant and pretend to live in a cave or take concrete measures against it. The Government of India introduced the Personal Data Protection Bill, 2019 amidst the backdrop of incidents like data manipulation and it’s selling in the general elections of the country by a British political consultancy ‘Cambridge Analytica’ came to light. The bill governs the processing of data by the government, companies and other organizations. It is revolutionary in the sense that it includes provisions for rights of data principals, consent and even grievance redressal. The bill is the first ever legislation introduced in India with regards to the data protection. The bill is also immaculate in the sense that it has apt classifications for different categories of data fiduciaries and also has categorized data in order of sensitivity.

The airtight provisions and new tribunals for Data Protection will serve as a deterring effect on data principals and will lead to a more careful way of handling and processing data. With penal provisions included in the form of offences and various punishments to them the bill will ensure that selling and manipulation of data is prevented and the faith of the general public is restored in privacy.

Keywords: Data Protection, Right to privacy, Election management.

CYBER THREATS IN SOCIAL NETWORKING WEBSITES AND LEGAL FRAMEWORKS

Chandan Kumar Ojha & Anjali Sinha, LLB student, The ICFAI University Jharkhand

Abstract

A social network is a social structure made up of individuals or organizations called nodes, which are connected by one or more specific types of interdependency, such as friendship, common interest, and exchange of finance, relationships of beliefs, knowledge or prestige. A cyber threat can be unintentional and

intentional, targeted or non-targeted, and it can come from a variety of sources, including foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, disgruntled employees and contractors working within an organization. Social networking websites are not only used to communicate or interact with other people globally, but also one effective way for business promotion. Cyber threats in cyber space include data privacy and traditional network threats. We are concerned with cyber threats in social networking websites and those threats may be in the form of fake social media profile, defamation, harassment and stalking. Here in this paper, we are trying to highlight common cyber threats in social networking websites such as privacy related threat, traditional network threats to name a few. In this research paper we have also tried to examine availability of legal framework in India, at last we conclude with some suggestions of anti-threats strategies and visualize the future trends of social networking websites.

Keywords: social networking sites, Information warfare, Defamation, cyber threat.

SURVEILLANCE STATE AND RIGHT TO PRIVACY: CONUNDRUM OF THE MODERN WORLD

Chandra Mohan & Tushar Pal, Students, CNLU, Patna

Abstract

The world in which we are living now is a technology- driven one, this goes without a saying, but the extent to which our lives are influenced by these technologies is unprecedented. The *modus operandi* associated with each and every sphere has witnessed a major overhaul, this rule is almost absolute and the current surveillance practices serves as a perfect example. Surveillance has been developed as a mechanism to ensure the security of a State and to prevent the disruption of peace in the society and in order to perform these functions properly, the individuality of a citizen was always met with a nasty glance. However, this stance exhibited gradual change, with jurisprudential developments, new judicial trends and increasingly complex societal structure. The stand-off between surveillance and privacy of individuals has achieved new heights, with the advent of intrusive technologies in the digital arena. This paper aims to critically analyse the surveillance practices which have been adopted by the governmental authorities and in what manner they tend to breach the personal sphere of an individual. The authors have also tried to analyse the provisions of various legislations which are related to scrutiny of data by the authorities and also highlighted the overreach of these authorities, which arise from these provisions. In explaining this position, the authors have also dealt with the implication of Section 69 of the IT Act, 2000, on Privacy and have indicated the manner in which the government is treading on the path of becoming a “Big-Brother State”. Other ancillary shortcomings of the Act, apart from the privacy, security and legality, necessary for understanding the impact of the surveillance practices on the citizens, has also been dealt by the authors. Further, judgement given in Puttaswamy case has been analysed in light of surveillance and privacy.

Keywords: surveillance, state, Privacy, Modus Operandi.

The Emergence of Blockchains: Another Sword of Damocles for Law?

Raj Shekhar Student (1st Year), NUSRL, Ranchi & Ujjwal Singh, Student (2nd Year), CNLU, Patna

Abstract

The main aim of this paper is to provide a deep insight and a comprehensive assessment of existing research and heated issues surrounding Blockchain technology and its developments in a few selected jurisdictions with a special emphasis on Indian subcontinent. In connection to the Indian context, the paper

tries to provide recommendations and policy considerations that could help in institution of a robust and dependable regulatory framework for Blockchain, both in respect of creating new and necessary rules and laws and also by modifying the pre-existing rules and regulations to encapsulate without any bias the new technological advancement without any hurdles.

This paper tries to highlight the benefits, advancements and modus operandi of Blockchain and its diverse applications, domestic and international, potential and that already in use, for academicians wanting to enhance their understanding of this subject matter. This paper evaluates academic works, articles, survey reports, research papers, policy drafts and frameworks, books and other sources, analyses as well as synthesizes the information mapped. The paper renders a readable landscape by logically and systematically organizing the content into the small sub parts namely – what blockchain is and how it works, the issues that it tries to address, types of blockchain implementation, and an analysis of existing legal and regulatory frameworks governing blockchain technology, with a special emphasis on the Indian Context. The research work contained in this research paper is indicative of the strengths and weaknesses of formally implementing this technology and if it is considered to the fullest, it could serve as foundation for several other detailed reports in future.

Keywords: Blockchain, Technology, Regulatory framework.

CONCERNS AND ISSUE OF CONTEMPORARY DATA REGIME

Abhijeet Kumar, Student, CNLU, Patna.

Abstract

With the advent of internet, connectivity has become an affair of seconds around the globe. Sharing personal data even related to one's identity often takes places in the cyberspace for business, educational or other such necessary purposes. But the fact that internet allows to share information around the globe. It makes personal information of such participants vulnerable. Access to other's data in the cyberspace is relatively easy and data are often illegally used for political or business purposes. Such developments makes it necessary for nations and international forum to make laws to ensure proper and fair use of such data so collected becomes necessary in national and international communities to ensure identity of individuals are protected. There are several domestic, international laws to ensure the protection of such data. For instance the "General Data Protection Regulation" act of EU ensures the protection personal data taking into account "the Treaty of functioning of the European Union". Similarly "The Data Protection Act 2018" of the UK restricts the usage of personalized data pertaining to individual's race, ethnicity, political beliefs, genetics, health, sexual orientation.

In India, Section 43A of the IT Act provides for compensation if a body corporate fails to protect personal data of individuals. Similarly the IT (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 defines sensitive personal data which is capable of identifying a person. In order to bring an enactment for protection of individual's personal data a committee was formed under the chairmanship of Justice B.N. Srikrishna to study the issue relating to data protection and submitted a draft bill (Personal Data Protection Bill, 2018). The Bill has been approved by cabinet on 4 December 2019, yet to be passed by the Parliament.

FACESEC: AN INTELLIGENT MODEL TO DETECT FACE IN REAL TIME

Paramita Bhattacharjee, Hrituraj Chakraborty, Dipjyoti Deka

Student, The ICFAI UNIVERSITY Tripura, Assistant Prof., The ICFAI UNIVERSITY Tripura

Abstract

As a country develops the requirement of security risk management in every sector also increases. So, a developing country must take all the security measures required to protect their data and privacy. In our research, we have developed a user-friendly application which will help to detect and recognize faces in real time that appear in a specified camera. The application is equipped with machine learning techniques using OpenCV library along with few other required libraries and python language for coding. While detecting a face there could arise few issues which might decline the performance of face recognition and we proposed a solution keeping the above-mentioned problem in mind. In order to make the application more accurate new parameters are added and the accuracy percentage as calculated was 91% while the accuracy rate which was acquired by the simple face recognition model was 80%. Thus, the proposed model could be considered to be a more efficient and better solution to our problem.

DATA PROTECTION - CONCEPTUAL AND THEORETICAL UNDERSTANDING

Syed Hozaifa Arsh & Fatma Jannat

Students, ICFAI University, Jharkhand

Abstract

Data Protection as a concept means designing a mechanism to protect your personal data. In Modern society it is imperative to protect the abuse of data as in day to day life everyone uses a service buy a product online, register email, go to your doctor, pay your taxes, or enter into contract and service interest etc which doing so everyone is suppose to handover the personal data.

In this context researcher tries to highlight theoretical and Conceptual understanding of protection. Moreover the researcher also explain different rational behind data protection and how such protection will serve best to the society.

Keywords- Data Protection, Privacy, Abuse of data.

CYBER SECURITY AS A BACKBONE OF E-COMMERCE

Mr. Mukul Pandey & Mr. Rajeev Kumar Sinha

Research Scholar, Kolhan University, Chaibasa, Research Scholar, ARKA JAIN University, Jharkhand

Abstract

According to approximation 40% people in India use ecommerce rest 60% still depends on traditional market. Even though the foreign people totally depends on e-commerce. Time saving is a big benefit of online shopping from end to end which our shopping becomes quicker. With the facilitate of online shopping we can shop anytime, anywhere, any product. There is no necessitating to go exterior for shopping. It enables us to decide a diversity of products of every range from well-matched to elite products. There is need to take some essential steps to defend our self at the time of shopping online. Anything linked to the internet, which can comprise mobile devices like smart phones and tablets need to be use securely. The hackers can also aim the grassroots those who shop online. Everyone should have an attentive for emails so that rapid reply can be complete. We should be conscious of our e-mails about evils with our credit cards or an explanation or the position of online sort. Efforts should be done to augment more cyber security. Whenever a user has to enter his/her credit/debit card details his thumb impression should be

established every time at whatever time she or he do purchases. Introducing Bio-metrics can protect our e-commerce market. Being a safe and secure shopper starts with STOP.THINK.CONNECT. Take Security safety measures think about the sentence of your proceedings online and enjoy the ease of technology with peace of mind while you shop online. memorize these instructions during all online acquire and have a protected and happy shopping.

Keywords: *stop, think, connect, time saving, cyber security*

LEGAL FRAMEWORK FOR CYBER SECURITY IN INDIA: A QUALITATIVE STUDY

Prithvi Raj & Sourav Kumar Upadhyay

Students, Department of Criminology, Jharkhand Raksha Shakti Univesity

Abstract

As a saying in Criminology goes, “a crime will happen where and only when the opportunity avails itself”. This is the era where most of the things are done usually over the internet starting from online dealing to the online transaction. The threat from professional criminals and state sponsored saboteurs in cyber space is growing and continues to become more sophisticated. This gives rise to the new criminal methodology, generally known as cybercrime. Cyber-attacks redirect threat to the economic interests and national security of countries. These developments call for an increased effort to strengthen the cyber-security infrastructure of country and thereby better protect their vital interests. In order to reduce and to punish the cyber criminals the term “Cyber Law” was introduced. We can define cyber law as the part of the legal systems that deals with the Internet, cyberspace, and with its legal issues. To stop cybercrime, spotlight is required on related laws and orders. There are many laws and measures which are framed and have been taken in order to prevent these evils such as IT ACT 2000, National Cyber Security Policy, IT (Amendment) Bill, 2008 – Data Protection & Computer crimes, Security Assurance Framework- IT/ITES/BPO Companies etc. The objective of the research is to study the India’s cyber edict framework and provisions and the issue in which the cyber law enforcement lacks. The method used for the study is data analysis. A qualitative approach with exploratory research technique was used in this study.

STATE SURVEILLANCE: A THREAT TO RIGHT TO PRIVACY?

Mani Shankar Mani & Adarsh Singh

LLM Students, CNLU, Patna.

Abstract

Surveillance is a part and parcel of the social life and it can even be traced dating back to the primitive society where different techniques were adopted for surveillance. With the technological advancement the modes adopted for surveillance by state has changed from Bentham’s and Foucault’s panopticon approach to modern day approach of creation of specific institutions for surveillance by the state. As state surveillance is an essential procedure in order to curb down crimes but the unauthorized use of these mechanisms have led to the violation of privacy of the individuals. Although the right to privacy has not been defined in the Constitution of India but the Supreme Court in plethora of judgments has settled this position that right to privacy is part of the fundamental rights enshrined in the Constitution. This research paper attempts to carry out in depth analysis of the state surveillance in the Pre and post internet era in India and what are the effects on right to privacy of an Individuals. Further the researchers tend to analyze the statutory provisions for surveillance in India and how the Supreme court in various judgments

has balanced the interest of the state and the privacy of the Individuals whenever there arose any dispute. The paper will be concluded by analyzing all the aspects and listing out the various methods adopted by the State for Surveillance and protecting the interest of the Individuals.

Keywords: Security, Data Protection, Fundamental Right, Right to Privacy, Surveillance

DATA PROTECTION BILL 2019 - Analytical Study

Nisha Kumari Mishra

BBALLB Student, FOL, ICAFI University, Jharkhand

Abstract

There is a global concern about the transfer and security of data. Keeping in view of these concerns many countries have started making law in this regard. A strong data protection framework can empower individuals, restrain harmful data practices and limit data exploitation. Supreme Court in a landmark judgement of Puttuswami case rightly held that right to privacy is a fundamental right and it is necessary to protect personal data as an essential substance of informational privacy. Whereas the growth of digital economy is also an important issue. In this context the personal data bill 2019 is India's first attempt to domestically legislate on issue of data protection in this paper the researcher tries to analyze the important provision of data protection bill 2019. Again researcher also tried to examine the provision of this bill is restrictive to achieve the object of law finally researcher conclude whether Data Protection Bill 2019 can establish a balance between growth of digital economy and the Fundamental Right of privacy.

CYBER SECURITY AND CYBER LAWS AROUND THE WORLD AND INDIA: MAJOR THRUST HIGHLIGHTING JHARKHAND FOR CONCERNS.

Dolly Krishnan & Mohit Verma

Pursuing LLB, ICAFI University, Ranchi, Jharkhand

Abstract

Cyberspace is the connected Internet Ecosystem and it refers to the virtual computer world, and more specifically, the notional environment in which communication over computer networks occurs. When this cyberspace is compromised, this leads to cybercrime and even Cyber **terror** which is *intended* to undermine the electronic systems to cause panic or fear and even monetary loss. The techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation is called cybersecurity. As a body of UN, International Telecommunication Union releases *Global Cyber security Index (GSI)* in which, by assessing certain parameters, it measures the commitment of countries to **Cyber security** at a global level and it has ranked Denmark, Australia, Republic of Korea, in top ten category. India drastically slipped down from 23rd Ranked in 2017 to 47th rank in the latest GCI, 2018 which is a matter of grave concern and it seeks immediate attention. **Cyber law** is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues.

In most nations globally, there are many legislations governing e-commerce and cyber crimes going into different facets of cyber crimes. In Indian context, the **IT Act' 2000** which was amended in 2008 and is known as Cyber Law. Though we have seen many new laws, initiatives and policies from the government of India, there are grave threats despite progress. Here, we want to give a brief overview of the cyber attacks, cyberspace encroachment and security concerns around the world and India with major thrust to Jharkhand which came into limelight when one of its cities, Jamtara, earned the title of Cyber Crime Capital of India. We have tried to explore existing legislative dimensions with regard to its effectiveness in handling

Cybercrime and possible future perspective for a more digitised and inclusive social order and economy for global growth.

Keywords: Cyberspace, Cyber Threat, Cyber security, Cyber law, Cybercrime in Jharkhand

CYBER SECURITY INTERNATIONAL LEGAL FRAMEWORK

Saumya Pratibha Tirkey & Shailvi Sinha

Students, ICFAI University, Jharkhand

Abstract

A number of indicators recommend that the international law of cyber security is in going through a crunch. The world wide challenge of cyber security has not been addressed by any single international actor. Much authoritative work relies that the international law fails to deliver on the concrete framework of management of cyber space. However the lack of cyber specific system of rules of international law does not indicate that there are no legal rule that would apply to cyber activities. Certain regional treaties taken together provide a patch work of regulation for cyber activities. In this work researcher tries to examine Budapest convention on cyber crime 2001, Sanghai corporation organization information security agreement 2009 and the African Unions cyber security convention 2014. However these international agreements in the form of regional convention cover some of the cyber security problem and have very limited membership. At last researcher tries to conclude cyber space in surely not a lawless territory beyond the reach of international law.

EMERGING THREATS IN CYBER SECURITY

BREACHES AND FUTURE CONCERN

Nitish Chaubey, Student, Institute of Legal Studies, Ranchi

Abstract

The exponential growth of Internet interconnections has led to a significant growth of cyber attack incident often with disastrous and grievous consequences Malware is the primary choice of weapon to carryout malicious internets in the cyberspace, either byexploitation into existing vulnerabilities of emerging technologies. The development of more innovative and effective malware defuse mechanisms has been regarded as an urgent requirement in the cyber security community.

The researcher in achieving this goal firstly present an over view of the most exploited vulnerabilities in existing hardware, software and network layers. This is followed by critiques of existing state of the art mitigation techniques as why they do or don't work. We then discuss new attack patterns in emerging technologies such as social media, cloud computing, smartphone technology and critical infrastructure. Finally we describe our speculative observation on future research directions.

LEGAL FRAMEWORK OF CYBER SECURITY: INDIAN PERSPECTIVE

Simran Kumari & Shubhangi

Student, The ICFAI University Jharkhand

Abstract

The policy formulation of cyber security in India has traditionally been associated with sovereign consideration particularly with the issue related to state sponsored terrorism and internal security. The 1st attempt to define Cyber Security is being attempted in Information Technology Act 2000 . However such attempts are also not sufficient to cover all issues of cyber security but the same was appreciated that atleast

it started to address the issue. In 2004 , The Indian Computer Emergency Response team was established that pays a dominant role in cyber security in India. By amending Information Technology Act in 2008 , CERT-in has been designated to serve as National Agency to perform the functions in cyber security area.

The National Cyber Security Policy 2013 is enlightening as to the India policy objectives. The objective of 2013 policy highlights the social and economic significance of protection of personal data and protecting against cyber crime. Such policy is important as much as it recognizes the various assets of cyber security.

In this paper, researcher tries to trace out the legislative history relating to cyber security in India and how far the existing legal framework is sufficient to deal such multi dimensional challenges of cyber space.

RIGHT TO BE FORGOTTEN

Pranjul Dalela (Author) & Samarth (Co Author)

National University Of Study And Research In Law, Ranchi

Abstract

The right to be forgotten refers to the power of people to erase, limit, delink, delete or correct personal information on the web that's misleading, embarrassing, irrelevant or anachronistic. In the information society, the role of personal sector entities in gathering information for and about users has long been a most crucial issue. Therefore, intermediaries became a main focus of privacy regulations, especially in jurisdictions with a robust tradition of privacy protection like Europe. In a landmark case, the ECJ ruled that an online program operator is liable for the processing that it carries out of private data which appear on web pages published by third parties. The recognition by the ecu Union of a so called "right to be forgotten" (RTBF) has ignited disgruntled reactions from civil society and legal scholars, especially within the us . This right was cast into the spotlight by the ecu Court of Justice decision within the Google Spain case, confirming it as a matter of EU law. This "right," however, has existed in many forms round the world, usually applying a balance-of-rights analysis between the proper to privacy and therefore the right to freedom of expression. The new European version, though, is predicated on a legal theory of intermediary liability where Internet search engines are now considered "data controllers," and intrinsically have liability for managing some content online. As it has evolved in Europe, this right has focused attention on key underlying policy considerations, also as practical difficulties, in implementation under the new European regime. In particular, shifting the burden of making compliance regimes and supervising important human rights from government to the private sector. Thus, in Europe, the function of balancing rights (privacy versus speech) within the digital context has been "outsourced" to the private sector. Recent experience in Europe under this regime shows that there's no uniform approach across countries. Moreover, different national approaches to the "right" make it almost impossible for multinational entities to comply across jurisdictions. Apart from the info controller threshold, civil-law jurisdictions seem to offer greater weight to privacy concerns in striking this balance. Common-law jurisdictions tend to offer greater weight to expression. The right to be forgotten is another example of an evolving transatlantic data struggle with potentially serious trade implications. This Article explores the historical and theoretical foundations of the proper to be forgotten and assesses practical legal issues including whether North American "free speech" rights are an efficient buffer to what's sometimes a really controversial and evolving issue.

PRIVACY AND DATA PROTECTION LAWS IN INDIA

Ajay Kumar Singh Gautam

Student, The ICFAI University Jharkhand

Abstract

The concept of privacy and data protection is taking the important place in today's world. The advancement of the technology and the dynamism of legal world provides outlook of privacy and data protection issues in this recent era. Privacy is something that is not to interfere to the interest of others. Privacy has become a concern of every individual due to technological advancement and it also emphasizes for protection of data. Data protection emphasis individual liberty and these individual's liberty is under threat by the interference of the stranger. The activity of the stranger to the individual's activity by any means is required to halt.

The basic legal requirement of any new phenomenon can be validate through the constitution. The constitution of India has given more emphasis on right rather than duty. For giving emphasis data protection, it consider as a right based approach. As India is developing state, it need some time for the effectiveness or implementation of the new area of law.

The data protection issue mainly attracted by these areas which are Right to Privacy, Right to Information, Information Technology, Indian penal Code, National Security, Intellectual property, Corporate Affairs, Consumer etc. The constitution of India has some provisions like, 'Freedom of Speech and Expression' and 'Right to Life and Personal Liberty'. These provisions have its effect to the right to privacy as a fundamental right. There are number of cases also which establishes the right to privacy as a fundamental right. The conceptuality of this proposition has also connected with the new dimension of the 'Data Protection'. The linkage between this privacy and data protection are interdependent to each other. The right of data protection is the closely related with the 'information' of an individual.

LEGAL FRAMEWORK FOR CYBER SECURITY

Sonu Kumar

Department Of Law: - University Law College, Hazaribagh

Abstract

Cyber security is a necessary consideration for information technology as well as internet services. It plays an important role in the field of information technology. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber-crime' which is increasing day by day. Various government sector and companies are taking many measures in order to prevent these cyber crimes.

Cyber crime is crime committed on the internet, using the internet and by means of internet. My paper gives detailed information regarding cyber security, cyber crime, nature and scope. This also involves classification of cyber crime which is against the person, property and government.

Finally, I will go for the research which type of cyber crime is most practice in the world. What are their impact on any country? Safeguard and punishment for the cyber-crime. Further, I will try to present some secondary data and analysis. Finally they give some conclusions and recommendation.

KEYWORDS: -Cyber Security, Cyber-crime, Classification of cyber-crime, Safeguard and punishment.

DATA PRIVACY AND CYBER SECURITY

Jaya Jha & Samiksha Gupta, Student, University of Petroleum and Energy Studies, Dehradun

Abstract

Privacy is one of the fundamentals of human life which gives it the stature of such a valuable asset making it one of the most cherished fundamental rights. Digging deeper into the concept we discover that the advanced era of internet and modern technologies have witnessed an acceleration of crimes related to privacy of data in terms of cyber security. The digitalization of economy opened the gateway of government's scheme called AADHAAR which infringed upon the personal data of the individuals. After the AADHAAR case the lawmakers were bound to give a thought on the data protection of the individuals suffering from it. One of the emerging case laws which helped to decide the same was the Justice K.S Puttaswamy V. Union of India making it an intrinsic part of Article 21 of the Indian Constitution. We humans are lured by the false notion of the customization (popping of similar products based on our search) of various applications on our electronic gadgets which in reality is nothing but an act of exploitation of our personal data. India being the largest democracy does not have specific cyber crime legislation. The IT Act, 2000 and IPC Act, 1860 are the only strings holding the cyber crimes punishable in India. However, the government has proposed the Draft Personal Data Protection Bill, 2018. Cyber crime is the infringement of the cyber space by the unauthorized access in the virtual world during the pleasurable event of internet surfing. Right To Information is seen to have disclosing the data and interfering with the privacy. The primary equipment to instrumentalise the security and safety is registered under section 43A of the IT Act, read with Reasonable Security Practices Guidelines. There are several countries party to several cyber domain bilateral treaties and agreements of which India is not a favouring party to and hence it needs strict and stringent laws to enforce and to curb with the emerging cyber threat awaiting the netizens of the country before it's too late. This paper aims at recommending laws relating to strong data protection regime of the country.

Key words: Cyber security, Privacy, Netizens, Crime.

ARTIFICIAL INTELLIGENCE: CHALLENGES FOR CYBER SECURITY

Dr. Dilip Kumar, Dr. Manish Kumar, Dr. Goutam Tanti & Dr. Vishal Kumar

Assistant Professors, Faculty of Management Studies, ICFAI University Jharkhand

Abstract

As we know that the artificial intelligence is the science of creating intelligent machines and intelligent computer program that can think and act like human beings. The term 'artificial intelligence' was coined by an American scientist named John McCarthy in 1956 which was based on the human philosophy that whether a machine can be as intelligence as the human being. Most of the researchers continuous working on it, to explore the different aspects of the artificial intelligence and some of the popular examples are Siri, Alexa, Tesla, Cogito, Boxever, John Paul, Amazon.com, Netflix, Pandora and Nest. These application has been using by the people for their personal and professional growth.

The existing challenges for the user like building trust among the people due to lack of awareness, heavy investment required, software malfunction issues, data scarcity problems, algorithm bias, data security for the people, high expectations among the pool of technologist, scientist, interests and AI human interface etc. which provided a obstacles in front of cyber security. The prime objectives of the research paper is to focus on a comprehensive consequence and challenges facing by the coming generation in the cyber security. Then, we outline current states of the research and future perspectives.

Key words: Cyber security, Artificial Intelligence, Challenges, People etc.

CORPORATE GRID OVER HUMAN NEED

P. K. Bhattacharyya, Advocate, Vice President, Dhanbad Bar Association, District Court & **Dr. Rumna Bhattacharyya**, Professor FMS, ICFAI University Jharkhand

Abstract

“Data Privacy and Cyber Security” apprehends the Cyber crimes as Reflection of that Hollywood super hit movie released in the year 2002 “Resident Evil” which foresees the perdition of Human Civilization due to Biochemical warfare and Genetical Mutation, Alike owing to Revelations of Cyberspace, its “Evil” Cybercrime now becoming “Omnicide” from the hilleck of homicide to gene-cide to Ecocide all over the world (Omnicide perdition) as the Australian Oydou University Sociologist opined recently.

The resident Evil of Cyberworld is cyber terrorism now in superhighway (e.g. hacking, theft spamming fraud, phishing, defamation, pornography stalking and piracy etc., the legal framework on cyber crime brought about various amendments in the Evidence Act, 1872 by amended insertion of (vide Sec. 92 of I. T. Act) Sec. 5, 17, 34, 35, 39, 59 and 131 of the said Act along with amendments have been made in section 167, 172, 173, 175, 192, 204, 463 and 464, 466, 468, 469, 470, 476 and 477-A of the Indian Penal Code, 1860. The Bankers Book Evidence Act, 1891 has also been amended in the manner vide 3rd Schedule to the I. T. Act, 2000 for permitting e-commerce the emphasis to I. T. Act highly felt as a tool for socio-economic Development. Undoubtedly cyberspace is the most useful place for e-commerce, Social networking, information and many more. The crown of civilization started emitting illumination by the philosophy of “Corporate grid over human Need” But **Key words:** E-commerce, Cyber Terrorism, Micro-Volution, Gene-Frequency, DNA, Global Perdition, Cyber Crimes.

STATE SURVEILLANCE AND RIGHT TO PRIVACY

Mansi Goel & Akanksha Basundhra Raje, Students, FOL, ICFAI University, Jharkhand

Abstract

Surveillance and privacy has become a major issue in a world dominated by information technology. In this paper, authors have dealt with the conceptual and legal frame work related with the surveillance and citizen’s right to privacy. We also discuss the historical evolution of the state surveillance in the context of right to privacy. After the Supreme Court’s landmark judgment in the case of Puttaswamy, the issue of surveillance through different mechanism by the Indian state leading towards the violation of right to privacy has become a bone of contention between the right conscious citizenry and the sovereign state. Authors have tried to analyse the problem of competing interest of both parties in the Indian legal jurisdiction and the other legal jurisdictions across the world through comparative study of the issue.

Keywords: Privacy, Surveillance, comparative analysis. Legal Framework.

EMERGING TRENDS OF CYBER SPACE (ARTIFICIAL INTELLIGENCE, INTERNET OF THINGS, BLOCK CHAIN, DARK NET AND CLOUD COMPUTING) AND CYBER SECURITY

Parambir Singh Bajaj
Student, ICFAI University, Ranchi

Abstract

The Cyberspace Internet can be defined as a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities. It

exists in the form of bits and bytes – zeroes and ones (0's and 1's) which are simply, electronic impulses. Over the past decade, there has been a dramatic shift in the demographic of the users of Cyberspace- from the Developed to the Developing nations. Along with this, emerging trends within the ambit of Cyberspace have emerged such as Artificial intelligence, Internet of things, Block Chain, Dark net and Cloud Computing. Artificial Intelligence is a wide-ranging branch of computer science concerned with building smart machines capable of performing tasks that typically require human intelligence. The IoT (Internet of Things) is a giant network of connected things and people – all of which collect and share data about the way they are used and about the environment around them. Its practical applications will have far reaching impact on improving our everyday lives. Block Chain is a decentralized Public ledger that stores crypto currency and allows for data miners around the world to oversee every single transaction. It has single- handedly disrupted the entire banking and accounting world. Dark net is the part of the Internet below the private deep web that uses custom software and hidden networks superimposed on the architecture of the Internet. Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

This paper will focus on how these emerging trends within the world of Cyberspace were initiated, where they stand currently and what the future holds for these trends. Along with their fundamentals, the paper intends to elaborate on the threats they face and pose to Cyber security and their implications on our socio-economic life.

Key words: Cyberspace, Artificial intelligence, Internet of things, Block Chain, Dark net and Cloud Computing, Cyber security

CHALLENGES FOR ORGANIZATION IN SHARPENING THE SKILLS IN MANAGING DATA PRIVACY IN AN INCREASED CONNECTED WORLD

Dr. Pallavi Kumari & Mr. Randhir Ranjan

Assistant Professor, Faculty of Management Studies,
ICFAI University Jharkhand & Advocate Jharkhand High Court

Abstract

In the competitive edge, the world of business is data-focused. Organizations need a more holistic approach to cyber-security. With global innovation, the business process has become complex, and there comes the role of the internet to transform into a simpler form. The success of a business depends on its speed and the hinges of innovation. But unfortunately, data-driven innovation also uncovers new vulnerabilities. It is evident that with the growing globalization the economy coming closer to perform and the role of information technology has become inevitable. There is a need for an hour that the organizations should be able to monitor and respond to changing business conditions, and emerging customer needs much faster than the challenges posed by the competitors.

With the help of the internet, the organizations can quickly capture the information of the customer from different sources for creating a pool of prospects for their own business. Business organization extensively uses the internet to perform their business activity. With the use of the internet, the works are done more effectively and efficiently. The managers perform the activities of production, sales, marketing, and distribution by making use of information technology. Hence, it is critical for every business to develop a strong data privacy strategy. The organization should offer seminars and workshops on data analytics and business intelligence for creating awareness.

Security and safety ethics encourages companies to carry out innovations at a faster rate. There is no

denying the fact that the internet provides speed, accuracy, and efficiency, but simultaneously data privacy and protection are also an emerging concern for the IT professionals. This paper will discuss how human error significantly affects data privacy. The role of IT managers plays an important role in imparting training to employees to avoid all possible mistakes which can lead to loss of privacy of data. It is rather important to empower the employees by creating awareness through data loss prevention tools. IT professionals need to be ahead of cybercriminals which requires continuously adapting and updating on latest security controls and practices. This paper will throw light on a few practices for enhancing security aspects of data and ways to reduce the ever-evolving cyber attacks. Cyber-security preparedness can reduce the threat of hacking. This paper will help the managers to understand the importance of cyber-security and take preventive steps while making use of robust technology. The paper highlights that the organization's biggest security challenge faced in large organizations is their delays in adopting technologies and keeping a bird's eye view on risk from the business environment.

This paper concludes that of course the evolution of the Internet is empowering the business innovations throughout the world but it is also creating ever-greater vulnerabilities for a cyber attack. In order to prevent the data, organizations must overcome the challenges with the help of innovative technologies and methods to identify cyber threats. Hackers can be defeated only when we follow constant examination, evaluation, and modification in the data security process.

Keywords: *Competitive Edge, Innovation, Managers, Employees, Internet, Organizations.*

RIGHT TO BE FORGOTTEN

Om Prakash Ravi
Student, CNLU, Patna

Abstract

The *Right to be Forgotten* is recognised in multiple jurisdictions, it allows people to demand erasure of their personal information from the internet. This right has its origin in right to reputation and right to privacy. It's also based on the idea that because the internet remembers forever, it doesn't leave space for redemption or self-correction. In India, the right to be forgotten has not been formally recognised, *but it's a part of the Draft Personal Data Protection Bill, 2018*. The bill provides for the right to restrict or prevent information disclosure, but not the right to erasure. Under the bill, an adjudicating officer will decide whether RTBF should be granted on the basis of sensitivity of the personal data involved, role of data owner in public life, the scale of information sought to be restricted, etc.

The etymological background of such right can be traced back in French Jurisprudence where this right used to be known as right to Oblivion, and this right was utilized by the offenders, who had served their sentence, to object the publication of their conviction or about the wrong committed by them in order to protect reputation among the society members.

According to this right, any person can ask to remove his or her personal information permanently in order to protect his or her right to privacy from search engines like Google, Yahoo or Bing. The commencement of such right took place in European Union and Argentina and it has been in practice since 2006 and this right consists of lawful removal of personal information from online platforms if such request is made by someone and the reason behind evolution of such right was that a person should not be further victimized in future.