INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

DIGITIZATION AND VIOLATION OF THE RIGHT TO PRIVACY

AUTHORED BY - SHIVANGI.

We currently live in the 21st century where the online forum rules the world. In every sphere of work, from Software, Law, Design, Marketing and Sales, Manufacturing, and Media, digitization reigns over all. Some countries, like Japan, are flourishing due to digitization, with their whole society reliant on digitalized machines and sources. The majority of restaurants and office buildings in China are operated by manual robots that are programmed with the help of AI to do duties according to the instructions coded into them. These are a few examples of large-scale digitization in developed nations. Even in emerging or undeveloped countries, digital media is an indispensable part of our everyday existence. Digital platforms underpin everything from, paying online, connecting with people on sites like LinkedIn, Tinder, and Instagram, and even buying stuff from Amazon. Whether it's advanced countries or those still growing, digital technology greatly impacts how we live and work.

This profound impact of digitization on the contemporary world is undeniable and cannot be ignored. It has reached a level were envisioning any task without incorporating digitization is nearly inconceivable. The influence of digitization extends its transformative reach, providing an indispensable framework for myriad activities. Moreover, it is undeniably acknowledged that this technological revolution has not only facilitated but also propelled businesses, ideas, and creative endeavours to unprecedented heights, resulting in remarkable and awe-inspiring outcomes. The current pace at which the world operates, with immense ease and speed, owes much of its credit to digitization. This force has become an integral part of the fabric of our daily lives, influencing and shaping various facets of society. The acknowledgment of this reality is widely shared among the present youth, who recognize the imperative need to acquire a nuanced understanding of digitization and artificial intelligence (AI). The prevailing consensus underscores the notion that these technological realms are poised to dominate the majority of platforms in the foreseeable future. Within this evolving landscape, individuals who are not well-versed in digitization and AI find themselves at a disadvantage, facing potential challenges in securing a foothold in various domains. The awareness among the youth underscores the urgency for cultivating proficiency in

ISSN: 2582-6433

these areas. Those who excel in this area will end up being assets to companies and organizations. Progress continues to be intertwined with digitization, and the imperative for individuals to stay abreast of these transformative technologies becomes increasingly evident.

Everything remains acceptable as long as digitization serves as a supportive tool in tackling a wide range of challenges and streamlining expansive and viable work processes. However, concerns emerge when this instrumental role evolves into an authoritative and pervasive presence across major domains and platforms. While the idea of digitization assuming control over various issues may seem appealing, questions regarding its credibility and trust come into the picture. As we increasingly rely on digitization to address multiple challenges, there is a growing need for an understanding of the reliability and authenticity of the digital world. This necessitates a careful examination of the mechanisms in place to ensure the integrity of digital processes, the security of data, and the transparency of digital interactions. As we navigate the expanding influence of digitization, it becomes imperative to establish robust frameworks that not only harness its potential benefits but also ensure confidence in its credibility, fostering a digital landscape that is both dependable and trustworthy.

The digital world is vast, it is huger than one can even imagine. It consists of millions of networks, each interconnected with one another to form a linkage to work most efficiently and try to have answers to everything one could ever imagine. But it is this network one should also fear. We common people hardly have around 5% knowledge about what the digital world works like. We search for news on Google, and we blindly agree to give sites access to our media, and our history, basically ending them having control of our phones. But what we don’t realize is that all the data we give gets stored in this huge network, and it is very easy for this information to spread widely and very quickly across this entire network. People, and organizations who we have no clue about can get access to such information. There is no control of the information once it is out there. We have hackers, we have fraud sites, and we have online thieves having access to such networks and can misuse this information once it reaches their hands.

And this is what one should be fearful about. Here is where the question arises, is our privacy in the digital world truly safe? The right to privacy is a human right for every individual and that applies even in the digital platform. In 2018, a resolution titled "The right to privacy in the digital age" was approved by the UN General Assembly. The resolution's main argument was that

ISSN: 2582-6433

anybody might feel less free to speak or do anything they want when they know that their actions or words could be intercepted. For this reason, the resolution called for international attention to human rights.[1] In the Indian Constitution, the right to privacy falls under the fundamental rights of every individual as per Article 21. The Supreme Court in a landmark judgment has recognized the right to privacy as a guaranteed fundamental right. In its judgment, it also mentioned that "Technological change has given rise to concerns which were not present seven decades ago and the rapid growth of technology may render obsolescent many notions of the present. Hence the interpretation of the Constitution must be resilient and flexible to allow future generations to adapt its content bearing in mind its basic or essential features[2]." The Indian Parliament has also put forward, The Digital Personal Data Protection Bill, 2023 whose aim is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their data and the need to process such personal data for lawful purposes and matters connected therewith or incidental thereto.[3]

The digital world has remarkably succeeded in building a pervasive trust within us. Often, we find ourselves unhesitatingly entering our personal information without a thorough consideration of the potential repercussions. Engaging in digital interactions becomes a routine of thoughtlessly ticking boxes to accept terms and conditions, thereby offering a trove of details to the seemingly insentient digital world, oblivious to the potential negative effects it could have on our lives. The compulsion to divulge personal information has become inherent in various aspects of our online activities – be it the creation of a Google account or signing up on platforms like Instagram. Each interaction necessitates a divulgence of a fragment of our identity. As we navigate through this digital landscape, the challenge arises in maintaining a comprehensive record of our actions. Despite exercising immense precautions and willingly providing information, there remains an inherent uncertainty regarding the safeguarding of our right to privacy. The ubiquity of this digital exchange raises concerns about the perpetual vulnerability of our data and the inevitability of its potential misuse in the absence of a foolproof guarantee for our safety in the realm of privacy.

In the contemporary landscape, the prevalence of cybersecurity breaches on digital platforms has increased in number. There have been instances where we find our details exposed in the

[1] Right to privacy and data protection in digital age: Possibility of Myth? India, *available at:* https://www.lawyersclubindia.com/ (Last Modified January 23rd 2024)
[2] Prachi Bhardwaj, Right to Privacy: Landmark Supreme Court rulings & why a 9-judge bench decision is crucial, *available at:* https://www.scconline.com/ (Last Modified January 23rd, 2024)
[3] Digital Personal Data Protection Act 2023

ISSN: 2582-6433

expansive digital world, susceptible to unauthorized access. Advanced technologies have further enabled systematic scrutiny of online conversations. There is digital surveillance that acts as spy cameras, meticulously observing every digital footprint we leave behind. It keeps track of our search histories, keystrokes, and website visits, constructing a comprehensive profile that shows our preferences. This online platform is an intricate network, which is a silent observer secretly documenting every online move. The consequence of this surveillance is particularly evident in fraudulent activities, often involving illegal financial transactions from unsuspecting bank accounts. Individuals, in these instances, may unknowingly share their details with entities whose credibility remains dubious. Once it is out there, such information becomes part of a network that is prone to exploitation, leading to the emergence of fraudulent events.

Cybercrime attacks arose a long time ago, almost 2 decades in the year 1994 cybercrime attacks occurred in Russia where several corporate banks discovered that around $400,000 went missing. FBI became involved in the case and it was discovered that the hackers had attacked the institution's cash management computer system, which allowed corporate clients to move funds from their accounts into other banks around the world[4]. In January of 2021, approximately 8.4 billion passwords were leaked. It was famously called the RockYou2021 attack. It was the largest breach the site had suffered since 2009 where around 32 million accounts got leaked. In 2016, Yahoo Inc., a prominent internet company, disclosed that information related to a minimum of 500 million accounts had been compromised in the year 2014. The day following the cyberattack, Yahoo witnessed a 3% decline in its stock price, resulting in a loss of $1.3 billion in market capitalization. In India, it has been calculated that a whopping Rs 10,319 crore was lost to online fraud from January 2021 to December 2023. The National Crime Records Bureau (NCRB) reported that cybercrime cases have doubled in 2022 since 2021 in the national capital, Delhi. It was reported that in 2023, the Indian Government had to disconnect 5.5 million phone numbers that were obtained by using fake documents and were fraudulent and involved in committing such crimes.

Everything in the digital world is connected highlights the need for us to be more aware and take steps to protect ourselves. This is crucial in reducing the risks that come with the increasing range of online dangers. Statistical data shows that 3 billion Yahoo accounts had been breached as of

[4] A Byte Out of History- $10 Million Hack, 1994-Style, *available at:* https://www.fbi.gov/ (Last modified 24th January 2024)

ISSN: 2582-6433

2017, 1.1 billion have had Aadhar details violated as of March 2018, 533 million Facebook users as of 2019, and many more. The largest reported data leakage as of November 2023 was the Cam4 data breach in March 2020, which exposed more than 10 billion data records[5]. According to The Cisco Consumer Privacy Survey 2019, 45% of respondents indicated that the federal government is responsible for protecting data privacy. 24% of respondents find the individual user responsible for protecting data privacy. 21% of respondents find that companies should be responsible for protecting data privacy.[6]

While encouraging entrepreneurship and innovation in the digital space is important, we also need to take action to safeguard the privacy of our citizens. The most recent and well-known example that can best explain such personal violation is the deep-fake video that became viral all over the internet of a famous Indian actress. It affected her immensely to the point she had to take to the internet to address the situation and the harm it had caused her. Recently, Google, WhatsApp, Facebook, and iPhone have been receiving numerous complaints regarding their policy of digital privacy. All these platforms which offered social networking and searching tabs for people ended up gathering personal information about them through cookies and advertisement pop-ups on their sites. Google has recently updated upon disabling a tracking technology in its Chrome web page. Facebook has announced that hundreds of its engineers were developing a new technique for displaying advertisements that wouldn't require users' personal information. Apple and Google have begun updating the policies governing the gathering of personal data online. Apple has released technologies that prevent advertisers from monitoring users, claiming privacy as its guiding principle. Google is attempting to have it both ways by reimagining the system to continue targeting individuals with advertisements without abusing access to their personal information[7].

Governments frequently fall short of adequately informing the public about their surveillance initiatives. Even when surveillance tools are initially introduced for legitimate purposes, they can easily be repurposed for unintended objectives. States must restrict public surveillance measures to those deemed "strictly necessary and proportionate," targeting specific locations and times.

[5] Most significant cases of data breach worldwide as of August 2023, *available at:* https://www.statista.com/ (Last Modified January 23rd, 2024)
[6] 100 Data Privacy and Data Security statistics, *available at:* https://dataprivacymanager.net/ (Last Modified January 24th, 2024)
[7] Brian X. Chen, The Battle for Digital Privacy Is Reshaping the Internet, *available at:* https://www.nytimes.com/ (Last Modified January 24th 2024)

ISSN: 2582-6433

Additionally, the duration of data storage should be limited. It's crucial for countries worldwide to quickly set up strong rules controlling the export of surveillance technologies that could seriously threaten human rights. Additionally, these nations need to carefully make sure that they enforce thorough assessments of the impact on human rights. This means looking closely at what these technologies can do and understanding the situation in the country receiving them. This comprehensive approach is not just about strengthening oversight on potentially harmful surveillance technologies but also emphasizes the importance of understanding the specific factors that affect how these technologies impact human rights in different parts of the world. By creating a solid system that combines strict export controls with thorough impact assessments, countries can actively prevent the potential misuse of such technologies, promoting a more responsible and ethical global technological environment.[8]

The Cambridge Analytica and Facebook scandal explains that social media companies should be subject to stricter laws regarding their data handling and sharing practices. These companies maintain a repository of millions of users' data, and the unethical use of this data can give certain stakeholders undue influence over public opinion. In May 2018, the European Union decided to enforce stronger safeguards for the personal information of its residents. This was accomplished through the General Data Protection Regulation, which unifies data protection rules throughout the EU while allowing each member state to implement its modifications. All businesses, regardless of location, that conduct business in the European Union are subject to the GDPR. Additionally, Article 17 of the GDPR grants its beneficiaries the "Right to be forgotten" by extending the scope of its regulation beyond the gathering and processing of such data to the deletion of such data.

As time unfolds, the challenge of cybercrimes intensifies, propelled by the rapid evolution of new technologies in the contemporary world. The attention and accelerating research towards the field of artificial intelligence (AI) further exerts its substantial influence and control over various businesses and activities. This intersection of AI and cybersecurity not only amplifies the potential for safeguarding digital landscapes but, paradoxically, provides a massive area for cybercriminals to conduct their illicit activities. This escalating trend not only widens the scope but also encourages the perpetration of illegal acts on an unprecedented scale. As individuals, we

[8] Spyware and surveillance: Threats to privacy and human rights growing, UN report warns, *available at:* https://www.ohchr.org/ (Last Modified January 23rd, 2024)

ISSN: 2582-6433

must maintain a vigilant stance in discerning and promptly reporting any instances of the potential misuse of digitization. The advent of the COVID-19 pandemic has ushered in a predominant shift towards hybrid work models for the majority of us, thereby increasing the risks within the professional domain. Despite the existence of legal frameworks and proactive measures undertaken by prominent organizations and governmental entities, the collective responsibility falls upon all of us to actively participate in the safeguarding and protection of personal information in the digital platform. In the aftermath of the changes which has occurred from the pandemic, we find ourselves facing an immense responsibility to exercise caution and accountability in managing our online presence, ensuring a secure and resilient digital landscape for ourselves and others.