BRAWIJAYA LAW JOURNAL Journal of Legal Studies
e ISSN 2503-0841
p ISSN 2356-4512
Volume 10 No 2, October 2023
Nationally Accredited No. 164/E/KPT/2021 Dated 27th December 2021

Cyber Surveillance and Privacy Issues vis-à-vis International Law

Ivneet Kaur Walia

Rajiv Gandhi National University of Law, India
Email: ikwalia@gmail.com

DOI: http://doi.org/10.21776/ub.blj.2023.010.02.05

Submitted: 2023-06-26 | Revised: 2023-10-28 | Accepted: 2023-10-30 | Published: 2023-10-31

How to Cite : Walia, Ivneet Kaur. 2023. "Cyber Surveillance and Privacy Issues vis-à-vis International Law". *Brawijaya Law Journal* 10 (2): 219-241. http://doi.org/10.21776/ub.blj.2023.010.02.05

Abstract: *The 'Big Brother is Watching', is now a trend that is prevalent in the society where the unregulated and unfiltered monitoring of data and interception has led to interference with the privacy rights of the individuals. The background to the concept may not be expressly seen in text but the context of privacy be protected can be seen in legal instruments such as United Nations Declaration on Human Rights, International Covenant on Civil and Political Rights. Though, the legal jurisprudence has also taken sides for placing community interest over individual interest but has often been deficient in providing objective reasonings and justifications. When the privacy and the human rights are interfered with, no one but the State should own the responsibility. The contours of this responsibility have been circumscribed by the existing international legal instruments, but their effectiveness is compromised because of their non-binding characteristics. The paper outlines the importance of regulating mass surveillance, secret surveillance, cyber espionage, cyber attacks etc. and has facilitated a discussion of establishing a pattern of standardized norms in line with human rights obligations catalyzed by cyber diplomacy, which can easily be adopted by States. The paper is Analytical and descriptive in nature. The question will always be debatable when it comes to States exercising their right of surveillance for maintaining law and order and upholding the security of the nation being violative of individual rights. So, whether the States are able to strike a balance between State authority and Fundamental rights of the individuals? Whether the proportionality that is exhibited is justifiable? The uncontrollable parasitic attack on digital communications, without reasonable suspicion is excessive, arbitrary and abusive. There is a need not only for a structured legal framework but also procedural safeguards, oversight mechanisms and redressal forums.*

Keywords: *Human Rights; International Law; Privacy; Surveillance*

I. INTRODUCTION

International Law is the grand norm which regulates the conduct of the States in terms of cyber activities in virtual space ensuring State Sovereignty, equality and non-intervention. Surveillance State and the overindulgence of Media and Technology contribute towards manipulation of public opinion towards the government and the non-government actors. The domination of digital world by infusion of cyber technologies has led to an uncontained

revolution which impacts the human existence and living in every possible way. Most of the countries across the globe have enacted laws pertaining to information technology. Most of the laws so enacted do provide for direct or indirect mention about criminalizing data theft or identity theft or even prohibits the deletion, manipulation or modification of any stored data or information thereby securing the privacy. Privacy even when read into provisions generally express about the privacy of an individual's body against obscenity, explicit contents etc. But looking at the judgements in the background and reading the term privacy through the lens of the fundamental rights and freedoms. Thus, privacy has different aspects and multiple variations to its definitions, but whether privacy under certain circumstances can be interfered with? If yes, there is no document that makes an express mention, and even if provisions exists on pretext of maintaining law and order, the circumstances under which this can be done is not specifically mentioned.

The stretched horizons of technology, allow for data sharing or information sharing matrix, allowing conducive and swifter functions. Such a free flow of information has facilitated interaction and communications enhancing intelligence collection activities. The intelligence gathering process evolved with advent of signal transmission using telegraphs. The communications became easy for sharing information, but once the information became available, it was unregulated and accessible by any. Though, the spies and defense authorities started to incorporate use of such advancement for espionage or transmission of confidential information but overhearing or accessibility to information was always a concern. Over a period of time with advancement in technology, the intelligence units have started inducting more sophisticated systems for communication and data transmission. The transfer of information is now more computerized, artificial intelligence driven and algorithmically structured. The growing technology has not only triggered an encrypted interaction but also enhanced the storable abilities. These features of transmitting, storing and managing information has benefitted agencies to combat again serious offences and heinous acts like terrorism. [1] But sometimes collecting voluminous data for surveillance purposes intrudes or rather infringes the privacy rights of the individuals. It interrupts with their freedom of free expression and communication. Although, privacy and fundamental

[1] William L. Tafoya, "Cyber Terror," *FBI Law Enforcement Bulletin* 80, no. 11 (November 2011): 5-7

freedoms come to the forefront of the debate but restrictions of these freedoms for maintaining sovereignty of nation and law and order in society provides a defensive shield. This creates a rift between those making policies for stringent securities and surveillance provisions and those who are proponents of protecting individual rights.[2]

Privacy and surveillance have different connotations in different situations. Different perspectives can lead to different outcomes, for instance a military based approach would lead to a mindset where cyberspace will be seen as a militarized area and liberal approach on the other side would mean focusing on the national security issues rather than worrying about the individual rights. Though various measures are taken to police the cyber space but places like dark web are nearly out of the reach of surveillance. What was developed by United States as a measure to facilitate anonymous routing has now been termed as 'onion routing' is the most used tool to develop cloud computing. This is one of the examples to show that how systems developed for establishing a secure space is corrupted for malicious purposes. The famously known Edward Snowden's revelations in 2013 of Mass Surveillance/Espionage by Intelligence agencies brought to table the excessive use of modern technologies. This triggered the basic question to understand the context of privacy before diving into challenges and responses related to it. Nissenbaum has claimed to call privacy as 'contextual integrity', which means and assumes that every piece of personal information has a correlation with a societal context and there must always be certain specific norms available when there is a requirement of disclosure of such personal data. Solove has also attempted to provide a clearer understanding of 'Privacy' and showcases a 'pluralistic understanding of privacy' as he says that there are sufficient elements that constitute privacy and it should be understood as a consolidation of 'family resemblances. Snowden's revelations question the regulatory issues pertaining to security measures and sovereign control. This control contention can be substantiated by an argument that in present times the intelligence agencies have power enforcement power than the State itself. Such an excessive and unplanned delegation is the major factor contributing towards a weak regulatory framework. Snowden revelations thus pinpoint towards the power struggle of controlling the internet or the cyber space. The State's do make attempts to make the public aware of the technologies but how much are they

[2] Anish Roy, "Privacy Issues in Cyber World," *International Journal of Law Management & Humanities* 3, no 3 (2020): 1388-1390.

apprised and does the public respond differently to different technologies at place. It is important to understand the cyber victimization, to make a study of impact of such technologies on the individuals who are subjected to or are susceptible to interception. The intrusions by the State are known been looked upon as causing privacy victimization.[3]

The difficulty in international law standing on matters of surveillance or espionage is because of random forces that move outward for instance:[4]

- The cost of surveillance is already at peak and is still rising
- Incidents like Snowden revelations have created trust issues between individuals and policies of the governments
- Intelligence gathering repeatedly interferes with the liberties of the individuals which may be excessive and unnecessary for the required purposes of the government.
- The exponential rise in the terrorist activities is a shout out to accelerate the process of surveillance.
- Surveillance beyond borders may not always interfere with the State's Sovereignty.

II. LEGAL MATERIALS AND METHODS

The beginning of the century witnessed corrosion of privacy norms both at the legal front and the societal front. The prevalence of mass surveillance was an indiscriminate arbitrary use of power, with the ability to compromise on data as well as individual rights. On study into the core of the subject, the author could understand that traditionally the interception is referred to the signal intelligence and state sponsored espionage activities for which the reading of telegraph communication legislations became essential to understand the base and the background. It is because of such material available, that one could understand the need for differentiating the categories of surveillance. The paper aims at exploring the impact of surveillance on international human rights and right to privacy against digital or cyber surveillance. The researcher has also explored online portals and platforms that provide for ebooks and e journals for references and additional readings. Online news clippings were also referred to understand the intrusiveness of nation states and if justifiable, on what grounds.

[3] Ales Zavrsnik and Pia Levicnik, "The Public Perception of Cyber-Surveillance before and after Edward Snowden's Surveillance Revelations," *Masaryk University Journal of Law and Technology* 9, no. 2 (2015): 35-37, https://doi.org/10.5817/MUJLT2015-2-3.

[4] William C. Banks, "Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage," *Emory Law Journal* 66, no. 3 (2017): 517.

The research work presented here is analytical piece of work. The author has resorted to qualitative analysis. Informal interviews were the major data collection technique that was put to use. The qualitative analysis also involved observations involving proper structuring, reliability and validity. The author has also conducted informal interviews with the international law experts and privacy experts for gaining a better understanding of customary international law norms, human rights law and data protection issues and concerns. The author was not in specific able to gather any surveillance related data as matters of such nature are highly confidential and not open easily for discussions and debate. The author has interacted with data protection officers of various corporate officers to evaluate the involvement of corporations in extracting data from the internet service providers to cater to the needs of the individuals in terms of providing goods and services as per the behavioral patterns of an individual. Informal interactions and interviews with defense personnel has also indicated towards emerging use of such technologies for gathering information about hostile nations.

The author had referred to prevailing laws, models and recommendations of the other jurisdictions for comparative study and understanding of best practices and regulatory compliances across the globe. The author while analyzing the grey areas of the subject matter referred to various primary sources like Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, American Convention on Human Rights, Vienna Convention on law of treaties etc. Along with the study of various international instruments, certain reports of the important committees were also referred to, such as, The Report of the Investigatory Powers Review, Report of the United Nations High Commissioner for Human Rights etc.

III. RESULT AND DISCUSSION

Need for Balancing Security and Surveillance

Most of the crimes committed today possess transnational characteristics and thus transcend boundaries confusing jurisdictions and their agencies. The most prevalent crimes include terrorism, money laundering, trafficking etc. Though, the paper is more focused on safeguarding privacy rights in times of State dominance, but the role of the corporations cannot be ignored, the corporations are the major data banks of personal information and whereabouts of an individual. The individuals nowadays are spending more time on the digital platforms thereby leaving behind a digital trial and a digital twin. This trail is trodden upon by the corporations to understand their behavioral

patterns, beliefs and opinions. The data so collected is not only used to customize services but is also used to be sold to the government and the most relevant reference in this regard is of the famous Cambridge Analytica case.

The problem with the States is that they focus more on identifying crime and less on strengthening strategies and decision making. Surveillance can be justified for maintain law and security but withholding excessive information will always be the reason for anxiety amongst the countrymen. The high security threats are directly connected with outgrowth of crimes like terrorism, cyberattacks on important establishments, major accidents and military crises, etc.[5] The impactful damage caused by terrorist activities and misfortunes of military crises between the States are so massive and impactful that they cannot be ignored and always gets a placement above arguments of civil liberties activist. The States for protecting their boundaries resort to various tactics like cooperative and collaborative measures between governments of different jurisdictions, information sharing for crime prevention or law enforcement, upgradation of tools and techniques for interception and analysis of voluminous intercepted information.[6]

The Mass surveillance and monitoring of a greater number of people in a demography indiscriminately is the most common design of information gathering by the intelligence authorities. The critical part about such mass data gathering is that it has no basis, neither of suspicion nor of evidence, because of which it is always in conflict with interest of the citizens. If we place national interest over the individual interest, such intelligence inputs gathered from the interceptions can protect us from eminently dangerous activities of the miscreants and the hostile nations. As it is difficult to differentiate between the common public and the militant. Surveillance with these objectives can always be justified for interception and investigation unless and until the information pertaining to an individual is targeted for other purposes causing damage and injury.[7]

There are various ways and means of deploying varied technology for purpose of interception, monitoring and retention of information because of which the legislators are uncertain about incorporating legal provisions. Data Collection or information gathering for

5 Radu Dan Cristian, "Cyber-Terrorism," *Drepturile Omului / Human Rights* 2009, no. 2 (2009): 34-36.

6 Prabhjot Singh, "Data Encryption and Surveillance," *Supremo Amicus* 18 (2020): 639-640.

7 Jann K. Kleffner, and Heather A. Harrison Dinniss, "Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations," *International Law Studies Series. US Naval War College* 89 (2013): 512.

surveillance can be done by process of intercepting, collecting and retention of data travel like any other data packets through the internet trajectories, second place to gather information for surveillance can be from the social media handles like facebook, twitter etc. The telecommunication devices like mobile phones, pagers, and global positioning systems, remote sensing satellites can bombard the agencies with immersive information, facial recognition, biometrics, voice identification systems and Internet of Things provide unfiltered information, that caters not just to the intelligence agencies but also by commercial entities for earning immeasurable profits. The Artificial Intelligence driven algorithms and software dive deep into the cognitive understanding s of an individual and cater to their wishes by providing results as desired in the consumer world. The incidents like Cambridge Analytica are an example of algorithms doing the mind reading. Across the globe different interception technologies have always caught the eyes of the activist, media and citizens for unfair infringements and data collection, for instance, Pegasus in India and PRISM and Tempora in United Kingdom.[8] There are two ways that agencies adopt firstly they can get the upfront information or use the front door, acquire the companies and access the unlimited information second method is back door technique where the information is taken away without prior intimation or permission using sophisticated systems.[9]

Once the set up for information sharing is done, the States take a step forward to establish methods of collaboration and cooperation to fight terrorist like activities. The cooperation can help in identification of the criminals and enforcement and execution of the law transnationally. The States can assist in interception of messages, use history records of the people who can be suspected or may otherwise help in building institutional infrastructure for enabling training and capacity building collaborations. The international community with the help of already set up United Nations specialized bodies and committees must build a viable operational and strategic course of action. To support the idea, we already have in place the Global Counter Terrorism Strategy of the United Nations, which provides for action plan concerning measures to be taken by the State for combatting terrorist activities and also calls for safeguarding the basic Human Rights and the rules for governance.[10] The

8 "America's Global Surveillance Record," Human Rights 13, no. 5 (September 2014): 30-35

9 Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy* 30, no. 1 (January 2019): 53-66.

10 Gary D. Solis, "Cyber Warfare," *Military Law Review* 219 (2014): 1-52

other regulatory framework that can provide guidance is the UKUSA Signals Intelligence Agreement. This agreement provides interception rights to its signatories in demarcated spaces across the world. These kinds of arrangements are crucial for constraining the excessive discretions in matter of interception or rather surveillance. Intelligence sharing in this way has become the most common and thus calls for supervisory oversight.[11]

Another issue crawls in when States delegate the interception right to private players or other agencies. These sub delegation authorities don't share the same accountability levels as the State's Government and can often circumvent the local regulations and expectations in terms of privacy or human rights protection[12].

Accepting Right to Privacy as an International Law Norm

It is very difficult to contain peripheries of the term privacy. It is difficult to provide a definition which must be exhaustive and precise at the same time. In General Assembly's, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism', Ben Emmerson has remarked that, "the presumption that individuals should have an area of autonomous development, interaction and liberty free from State intervention and excessive unsolicited intrusion by other uninvited individuals.[13]

Article 12 of the *Universal Declaration of the Human Rights*, 1948, Article 17 of the *International Covenant on Civil and Political Rights*, 1966, Article 8 of the *European Convention on Human Rights*, 1950, Article 11 of the *American Convention on Human Rights*, 1969 and International Human Rights Law in general provides for Right to Privacy as a fundamental right. Human Rights Council issued two reports, one relates to discussion on policy issues arising out of State's interception activities and second pertaining to protection and promotion of freedom of expression. After the advent of technology and rising incorporation of surveillance tools, the international organization assign privacy as a concern of utmost importance. The safeguards that

11 Kubo Macak, "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers," *Leiden Journal of International Law* 30, no. 4 (December 2017): 877-890, http://dx.doi.org/10.1017/S0922156517000358.

12 Abhilash Pattnaik and Soumya Kumar Palo, "Cyber Sovereignty: A Dichotomy," *GNLU Law Review* 5 (2018): 70-80.

13 Anna W. Chan, "The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware," *Brooklyn Journal of International Law* 44, no. 2 (2019): 795-820.

individuals are assured in the physical space must also be provided in the virtual space. The States are getting habitual in using surveillance methods for general policing as well. This raise concerns over vulnerabilities to human rights violations.[14]

The initiatives for protection of privacy are not limited to Specialized agencies or international agreements but rather intergovernmental initiatives, private industries agreements and civil society activism have contributed towards protection of right to privacy. Certain corporations are protecting by way of design and intrusion into the communication tools. The social media chat groups have incorporated features like end-to-end encryption for ensuring safety against interceptions. Another example of intergovernmental co-operation are the guidelines provided by Economic Co-operation and Development for protection of privacy and transborder flow of data. The Tallin Manual 2.0 is the latest volume that provides for International Law Applicable to Cyber Operations.[15]

Right to privacy as such cannot be compartmentalized as a right under customary international law because of the broad issues that in encompasses, state practices concerning protection of right to privacy are not consistent and uniform, right to privacy cannot be called as an absolute right and restrictions placed on it will always be eloquently discussed. There is also a lack of coherence of beliefs and ideas pertaining to privacy by the courts across the globe.[16]

Interpreting the term 'Interference' vis-à-vis Privacy Rights

When reading the text of the international instruments, the common perception about privacy is relatable to maintaining the sanctity of communications ensuring integrity and confidentiality which means that any transmission of information either in the form of email, messages or other online communication methods, must be delivered to the recipient uninterrupted, without any interference, manipulation or monitoring by a sovereign authority.[17] If we analyze the provisions of the surveillance laws prevailing in UK or USA we will

14 Brian Simpson and Maria Murphy, "Cyber-Privacy or Cyber-Surveillance: Legal Responses to Fear in Cyberspace," *Information & Communications Technology Law* 23, no. 3 (2014): 189-191, http://dx.doi.org/10.1080/13600834.2014.978551.

15 Ales Zavrsnik and Pia Levicnik, "The Public Perception of Cyber-Surveillance before and after Edward Snowden's Surveillance Revelations," *Masaryk University Journal of Law and Technology* 9, no. 2 (2015): 33-59, https://doi.org/10.5817/MUJLT2015-2-3.

16 Machiko Kanetake, "The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches," *Business and Human Rights Journal* 4, no. 1 (January 2019): 155-158, http://dx.doi.org/10.1017/bhj.2018.18.

17 Abhilash Pattnaik and Soumya Kumar Palo, "Cyber Sovereignty: A Dichotomy," *GNLU Law Review* 5 (2018): 70-85.

conclude that such interference is exempted under the clauses of these laws, or in other sense it can be said that the laws allow for such sovereign interferences. Human Rights Council has made several observations after referring to laws from different jurisdiction. Certain general observations about surveillance laws or provisions are cited herewith:[18]

- The council observed that certain legislations give excessive and intrusive powers to the intelligence agencies on the basis of undefined objectives without requiring authorizations either from the court or the sovereign heads.
- The Council also takes a note of intelligence agencies collecting bulk data by means of surveillance and catering to the needs of other State agencies. The massive data collected must be used for a specific and legitimate objective and must not be put to misuse for any other purposes.
- The Council questions the transparency norms followed with respect to the scope of such legislations and its implementations.
- The Council is perplexed at the undefined justification of national interest and national security which has nowhere been objectively deliberated.
- The Council has also raised concerns over excessive and unrestrained use of satellite communications and bulk data retention about activities conducted within or beyond the territorial limits of the State.
- The Council has emphasized the adherence to norms set in Article 17 of the ICCPR and endorses that States must take initiatives to safeguard against any interference in an individual's personal rights and if such interferences are made on some legal basis, it must be done in consonance with principles of legality, necessity and proportionality.
- The Council emphasizes that the laws authorizing interferences must clearly state the exact situations and circumstances and the class of people which will be placed under such monitoring.
- The Council urges the State to check the integrity and ensure effectiveness and independence of

[18] Shubhankar Das and Sarthak Patnaik, "Cyber Space Mass Surveillance Programs and Violation of Human Rights: The Way Ahead," *Indian Journal of Law & Public Policy* 2, no. 2 (2016): 43-52.

tools and techniques deployed for monitoring and surveillance.[19]

A landmark judgement was delivered by the European Union's Court of Justice in the case of *Digital Rights Ireland,* the crucial observations made in this case by the Court are as follows:[20]

- The Court is an important benchmark in understanding interference with privacy rights. The court reported that the cumulative aggregate of the information attained by way of surveillance reflect information about private preferences, relationships, individual behavior of person which can be more explanatory than deciphering a direct private communication.
- The court also stated that retaining the data may facilitate drawing inferences about the individual's private life. Hence, holding the Data even for the purpose of investigation or detection of crime can intrude upon the privacy and freedom of an individual violating Article 7 of the European Union Charter and the transgressing the personal data protection.[21]
- The Court also objected to the access of data gathered by the competent authorities using the blanket justification of public security, calling it an infringement of privacy.
- The court condemned the usage of secret surveillance and remarked that such surveillance practices infuse distrust and keep them in constant fear of being monitored, thus curtailing their freedom of speech and communication.

It is also important to mention about the levels of interception where the 'interference' occurs. In general sense it is stated that interference occurs when the authorities begin to intercept the signals and start with the procedure of data gathering. The interference with the privacy is set in motion, the moment the agencies or the authority's access and analyze the information or communication. In other jurisdictions, the term interference is interpreted to mean the time when

---

19 Nicolas Jupillat, "From the Cuckoo's Egg to Global Surveillance: Cyber Espionage That Becomes Prohibited Intervention," *North Carolina Journal of International Law* 42, no. 4 (2017): 933-968.

20 Caroline B. Ncube, "Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-Surveillance in South Africa," *SCRIPTed: A Journal of Law, Technology and Society* 3, no. 4 (December 2006): 344-350, http://dx.doi.org/10.2966/scrip.030406.344.

21 Motohiro Tsuchiya, "Japan's Response to Cyber Threats in the Surveillance Age," *Seton Hall Journal of Diplomacy and International Relations* 17 (2015-2016): 7-20.

intelligence uses the data rather than collecting it.[22]

Adding to the above explanation, the interference in relation to privacy rights can be set out in following circumstances: (a) where the law permits for secret surveillance (b) where the data collection goes on, irrespective of the fact whether it will be examined or analyzed (c) Where the data collected is analyzed as well (d) data retention for unreasonable period or without explanation (e) where the technology is compromised to maintain anonymity.[23]

Justifications by States for Privacy Intrusions during Surveillance

The States often bring certain doctrines to establish justifications and assign reasoning for curtailing human rights of the general population. This is indicating towards lawful practices of the States to curtail freedoms on the ground of public interest. Various provisions provide for such exemption but only on the condition that such exercise of power must not be excessive, abusive and arbitrary. The generalized deduction is that privacy can be curtailed in accordance with the law and only when it is necessary to maintain the sovereignty, law and order. Such interpretations involve, (a) in the interest of national security and safety, (b) for preventing serious crime and disorderly situation, (c) for safeguarding health[24] and morals, (d) for protecting rights of the others. The reasons given as justifications can be evaluated on the basis of established law, legitimate aim and proportionality as referred earlier[25].

Interpretation of term, 'in accordance with the law' means the legality of curtailing privacy must have a legal basis. The legislations that provide for strong basis must be accessible to the public, must be precise and foreseeable. The legal basis or the domestic law should be straightforward in this regard as international law can only be invoked after consuming the availability of relief at domestic level. The presence of a law on surveillance is not the only criteria, the objective and the standard of the law is the core area that defines 'in accordance with the law'. For a law that maintains a standard and a quality, must be accessible to public. The public will be aware about the circumference of the discretion only when

22 Oves Anwar, Ayesha Malik, Abraze Aqil and Noor Fatima Iftikhar, "Cyber Surveillance and Big Data - Pakistan's Legal Framework and the Need for Safeguards," *RSIL Law Review* 2020 (2020): 35-56.

23 Jamal Aziz, Ayesha Malik, and Noor Fatima Iftikhar, "Public Health vs. Individual Privacy in the Age of Cyber Surveillance," *RSIL Law Review* 2020 (2020): 10-30.

24 See Also: Nandu Sam Jose, "*Information and Communication Technologies and the Right to Informational Privacy in Health Care: A Comprehensive* Analys," Brawijaya Law Journal 10, no. 1, 2023

25 Scott A. Gilmore, "Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act," *Columbia Human Rights Law Review* 46, no. 3 (2015): 227-267.

it is aware about its existence and practice. Checks and balances on discretionary or arbitrary powers cannot be studies in Isolation. The interpretation of the phrase is also explained in the case of *Privacy International* v. *Secretary of State for Foreign and Commonwealth Affairs*, (2016), this case was presented before the Investigatory Powers Tribunal in UK that explained the phrase as 'in accordance with law'. The Investigatory Powers Tribunal remarked that there must not be excessive discretionary freedom with executive and secondly, the law must guarantee proper protection against abuse. Also, the law that curb such discretionary powers must lay down safeguards clearly and make accessible to public.[26]

Another important aspect is the foreseeability, where the State must ensure a that citizens be made aware of situations and circumstances under which authorities are empowered to conduct surveillance, or rather to put it more elaboratively, the States must provide details of permissions and authorizations for surveillance, the procedure adopted for attaining authorizations, the time period of surveillance, target population for surveillance, the procedure for the use, retention and collection of data. These norms are inherent in the international law standards and any State which indulges in surveillance must adhere to these norms, to conduct the process lawfully. The standards laid down act as a whistle to over arbitrary use of discretionary powers. It is also stated that to maintain the International Law Standards and check the compliances, the responsible specialized agencies must assess, whether the surveillance mechanisms are adequate and proper to conduct mass surveillance with a provision of segregating communications that are reasonably suspicious. Also, to check that there is no irregular, improper secret surveillances. It is also important that while granting authorization, there are certain requirements that must be considered for example, clear authorization must be given when furnished with complete details of person or persons who will be under surveillance and premises demarcated for it. The concerns have also arisen in matters where because of the development in technology automated collection or storage of information has become prevalent. The specialized agencies have condemned usage of such technology and called it a clear intrusion on privacy rights. Foreseeability aspect requires to be connected with aspect of effective oversight or effective supervision, the effective

[26] Laura Huey and Richard S. Rosenberg, "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention," *Canadian Journal of Criminology and Criminal Justice* 46, no. 5 (October 2004): 597-600.

oversight ensures both following of the rule of law in matters of authorized surveillance and redressal against arbitrary interferences.[27]

Need for Regulating Espionage in Cyber Space

The emerging trends have led to the coinage of the term 'cyber espionage'. The telecommunication sector had witnessed the tapping of phones or manipulation of lines for extracting information. The attacks nowadays are not launched via shells and rockets alone but rather hacking into the critical infrastructure. The telecommunication sector also engages in the cyberwarfare when calls and communications are made for sharing of information. The so-called encrypted calls can also be decoded by using the quantum computing. It is interesting to note that we have referred to regulation of cyberspace activities for protecting sovereignty of State[28] and Privacy of individuals against the miscreants but how will the international law check the role played by States in matters of espionage at different times. Cyber espionage or spying is swifter, easier and cost effective. Data theft and hacking are the most common terms through which easy access to other's information is possible. There is no definition that can define or explain what all can be termed as cyber espionage[29]. Mere extraction of confidential data, without being analyzed, transmitted across virtual space can also fall within the preview of espionage. Espionage will always lack the consent of the party whose information is being spied upon. It is used for intelligence gathering for both attacking the Sovereign and for protecting the Sovereign, depending on the objective. Under the International Law, an obligation of one State to respect another Sovereign is sufficient to establish State Responsibility. It is implied that no wrongful act be perpetrated against the other State. Referring to the international law Commission words on State Responsibility, ensures that no State shall breach international legal obligations under the international law to trigger responsibility under law.[30] In 2013, it was clarified that when we talk about State Responsibility, it encompasses activities involving Information and Communication Technology (ICT). Dealing with cyber espionage is a difficult assignment because of its characteristics in the form of

---

27 David J. Harvey, "Here's the Thing: The Cyber Search Provisions of the Search and Surveillance Act 2012," *Digital Evidence and Electronic Signature Law Review* 10 (2013): 39-50.

28 See Also: Nicholas Tsaugourias, Law, *"Borders and the Territorialisation of Cyberspace,"* Indonesia Journal of International Law, Vol. 15, no. 4, 2018, p.545-550

29 Jason Krause, "Cyber-Libertarians," *ABA Journal* 89, no. 11 (November 2003): 50-55.

30 Kartikeye Joshi, "Cyber Security and Cyber War," *International Journal of Law Management & Humanities* 4 (2021): 496-500.

anonymity, multifunctionality and swifter operation ability.[31]

The international law needs to strengthen its framework to understand and devise terms that can help us understand the characteristics of cyber espionage in the absence of the definition. Peacetime espionage and wartime espionage needs to be differentiated in this framework. Presently, the espionage during wartime is a subject of International Humanitarian Law which is regulated by Geneva Convention and Hague Regulations. The International level cyber espionage is not only to be understood as a parasitic attack on confidential information but the scope should rather be extended to disinformation, foreign interference etc.[32]

There is a complex issue related to protecting privacy rights of a nationals and protecting privacy rights of people residing beyond national territory. States majorly within the country may engage in surveillance activities, interception of communications, monitoring of information, but they do so within the restraints of their legal framework that exists. The engagement of Nations in extraterritorial surveillance will raise contentious issues like whether discriminatory approach on surveillance between nationals and foreigners be violative of international human rights law.[33] Above all, the major issue will be the legality of human rights treaties applicability to State's over the border applications. There are two models that suggest how the international human rights law may be made applicable extraterritorially, the spatial model and the personal model. According to the Spatial Model, the State is obliged to protect against human rights violations, taking place within the jurisdiction of the State territory beyond geographical limits, especially in the cases of occupied territories. The other model is the personal model, where the States are obligated to account for human rights violations, towards individuals on which they exercise authority, while such person is placed in police custody. There is global consensus on extending treaty obligations to surveillance using cyber activities extraterritorially on the basis of 'effective control' doctrine relating to spatial and personal model. Though, the doctrines facilitate in an understanding of

---

31 George O'Malley, "Hacktivism: Cyber Activism or Cyber Crime," *Trinity College Law Review* 16 (2013): 137-141.

32 Andrea M. Matwyshyn, "CYBER," *Brigham Young University Law Review* 2017, no. 5 (2017): 1109-1196

33 Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, "Limitless Worker Surveillance," *California Law Review* 105, no. 3 (June 2017): 735-750; See also: Sihabudin, "Expanding the Limitations of the Protection and Processing of Children's Personal Data: An Overview of Current Regulations, Challenges, and Recommendations," *Brawijaya Law Journal* 10, no. 1 (2023): 59

applicability of human rights but there are certain limitations and hiccups to tackle with, for instance, cyber surveillance is not dependent on presence of surveilling State on jurisdiction of monitoring, a foreign State cannot exercise effective control over individual located in foreign State when it comes to collecting individual data by way of interception and monitoring etc. The demand of physical presence to make both models workable make space for other States to continue the exploration and exploitation of data. To ensure that there is no discrimination and equal treatment by the States we depend on test of legitimate aim and proportionality. In the above scenario the treatment with the foreign nationals in terms of protecting against privacy violations is not proportional. It is suggested that there shouldn't be a demarcation of higher standard of protection for nationals and lower standard of protection for the foreign nationals in terms protecting privacy against mass surveillance. The law is oscillating between the effective control and the control over individual rights.[34]

There is an inherent bent of obligation and respect by Nations which agree to follow the human Rights instruments. One can see the inclination of being committed to the cause of protecting human rights when they ratify documents which are optional and legally non-binding. The importance of these instruments lies both in endorsement and enforcement when victims suffer because of breach of privacy. In the absence of Data Protection Laws, only the Constitution and the Courts can become the guardian.[35]

International law stipulations for Surveillance Governance

The appetite of States is increasing in terms of gathering information and data about its own citizens and activities of hostile or other foreign nations. There are several provisions in the international legal instruments but not much attention is paid to them because of their non-binding nature. As the consensus is difficult amongst nations on building a stringent legal framework on surveillance, it has become even harder to bring the international norms in balance with the human rights protection clauses. To work towards a better legal framework and legible international norms certain measures may assist in regulation of unwarranted surveillance such as, Enhancing Cybersecurity where the nations are generally indulgent in acquiring knowledge about other nations and being hostile towards destroying their

[34] Viola Rodrigues, "Cyber Stalking Issues of Enforcement in Cyber Space," *International Journal of Law Management & Humanities* 3 (2020): 568-570.

[35] Nathan Alexander Sales, "Regulating Cyber-Security," *Northwestern University Law Review* 107, no. 4 (2013): 1503-1556.

communication network or major establishment. In situations like these the State are left with no option but to upgrade their cyber security measures to combat against the cyber threats. To fight offensive cyber behavior, they devise strategies to increase their strength in terms of critical infrastructure and services.[36] The nations across the globe acknowledge that cyberspace is transnational and to maintain peace and unity it would also require cooperation and strength from the neighboring States. These measures lead to fruitful regulatory discussions and meaningful outcomes. The major shortcoming in this area is refusal and rejection by States of the idea of codifying norms protecting cyber threats. The approach accepted in the Eastern and the Western world are centrifugal on the grounds for instance internet freedom and internet sovereignty, self-governing approaches, multistakeholder and multi-governance issues etc.[37]

It's been a long trail that has been followed by the States to establish norms for responsible State behavior in cyber space.[38] The general cyber norms and other measures are not legally binding and are rather more flexible when compared with the international law. Resultantly, the States have become more casual in adopting such rules or code for their conduct. Such voluntary, non-binding, flexible rules can accelerate the vulnerabilities to peace and security. The concerns gave birth to a United Nations establishment of Group of Government Experts (GGE) to focus on determining the threats in the field of information security and undertake discussions and measures on, existing threats and prevalent norms. Sovereignty and non-intervention concerns, capacity building, peaceful settlement of disputes etc.[39]

For the first time in 2015 the Group of Government Experts made an effort to strike a balance between human rights and information and communication technologies. The Group recommended consideration of certain stipulations by the States which are mentioned below:[40]

- The group recommended to ensure respect for privacy, by creating conditions to prevent such infringements and take measures if

[36] Jan Neutze and J. Paul Nicholas, "Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms," *Georgetown Journal of International Affairs* 14, no. 3 (2013): 3-09.

[37] Ifeoma Ajunwa, "Confronting Surveillance," *Jotwell: The Journal of Things We Like (Lots)* 2022, no. 5 (May 2022): 1-2.

[38] Shruti, Ashutosh Kumar, and Priya Ranjan, "Prevailing Cyber Security Law," Supremo Amicus 29 (2022): 25-30.

[39] Mary Anne Franks, "Democratic Surveillance," *Harvard Journal of Law & Technology (Harvard JOLT)* 30, no. 2 (2017): 425-465.

[40] Kate Weisburd, "Punitive Surveillance," *Virginia Law Review* 108, no. 1 (March 2022): 147-167.

there are violations in reference to digital communications.

- To revamp and reform the procedures and practices along with review of existent legislations concerning surveillance in terms of monitoring, interception and collection of information (especially, personal data), while considering the protection against privacy violation.
- To develop independent redressal and oversight mechanisms capable of ensuring transparency and accountability.
- Ensuring remedy to individuals, who suffered privacy infringements as a result of arbitrary and excessive surveillance.[41]

These recommendations are guidelines for the State Surveillance, wherein the States must structure and execute these measures in line with human rights obligations.[42] The States must under obligation must ensure that the State should have a legal ground before practicing surveillance and must possess the characteristics like access to public, identification of possible offence, procedural safeguards, effective remedy, intelligence sharing arrangements etc. The States must also refrain from (a) surveillance when the public authorities are otherwise also allowed to have access to communications (b) third party involvement in storing communication data on pretext of being required by investigating agencies and (c) lastly, limitless intelligence sharing between agencies and other parties.[43]

Resorting to bilateral arrangements between smaller groups can prove beneficial for effective governance and adherence to the international law norms. The smaller the group, the better are the opportunities to share ideas and opinions and it is easier to engage in commitments on matters that require greater considerations. Thus, the idea of mass surveillance is now trending. The question no more remains about its legality or constitutionality but it has transgressed to question the State's obligations on protecting Human Rights in general and privacy in specific. The reason behind the not so prepared treaties is because these treaties were not drafted keeping in mind the times of cyber surveillance.[44] The privacy considerations are continuously being dictated by the moves of the corporates in acquiring data and information for their profit. The internet

41 Alan Z. Rozenshtein, "Surveillance Intermediaries," *Stanford Law Review* 70, no. 1 (January 2018): 99-101.

42 Gilad Yadin, "Virtual Reality Surveillance," *Cardozo Arts & Entertainment Law Journal* 35, no. 3 (2017): 707-742.

43 Rebecca Green, "Election Surveillance," *Wake Forest Law Review* 57, no. 2 (2022): 289-299.

44 Erin C. Carroll, "News as Surveillance," *Washburn Law Journal* 59, no. 3 (2020): 431-441.

service providers are holding information and meta data justifying their acts in the garb of assistance to criminal justice functionaries and then selling it off to the private players for predicting behavior of their customers. The democracies will have to keep their foot down and take charge of the free flow of information to answer the trickiest of question: how much information would be beneficial for the surveillance purposes and at what cost?[45]

IV. CONCLUSION

To conclude, the idea behind the research work was to check the applicability of state sponsored surveillance in conjunction with cyber space and also to evaluate the efficacy of present-day treaty regime to tackle challenges posed by advanced technologies. The collection of mass data or meta data, its communication, transmission, retention and examination has always been chaotic unresolved debate. The free flow of information, extraction and mining of data from systems have led to International Organizations like United Nations to closely watch over these categories of State Surveillance and study its accountability under international law. Looking at the vulnerabilities mentioned above, it is highly recommended to establish specialized agencies or organizations and develop standard set of binding rules to address the mindless collection and retention of intercepted information. It is pertinent to establish consensus globally and define basis upon which mass surveillance is conducted. It is important to interpret the term 'interference' in terms of privacy infringements, as the trend is prevalence is in regard to data being analyzed and inspected and ignores the juncture of it being collected and stored. It is also recommended, that international law be strengthened in terms of cyber espionage and establishing legal framework that may ensure the compliance of international law on one hand and protection of human rights on the other. At one point it also seems important to distinguish between cyber espionage and other ways of gathering intelligence. The stringent authorization requirement along with principles defining legitimate aim, proportionality, in accordance with law etc., helps in maintaining a high standard. As there are many challenges that need to be battled with, its essential to categories the initiatives into three parallels of developing namely focusing on International and regional legally binding agreements, development and establishment of cyber norms and bilateral agreements. Confidence building measures and standardized norms trigger

[45] Sonia K. Katyal, "The New Surveillance," *Case Western Reserve Law Review* 54, no. 2 (2003): 297-302.

international dialogues and acceptance of conflict issues. These initiatives go a long way in not only protecting the privacy of an individual but also acts as a shield against cyber industrial espionage where the matters may concern infringement of intellectual property rights. Thus, open sharing or excessive sharing of information with lesser limitations can cause a chain effect of violations that will keep sweeping from one domain to the other. Thus, it is important to curtail surveillance activities with the help of cyber diplomacy to incur minimum violations.[46]

REFERENCES

"America's Global Surveillance Record," Human Rights 13, no. 5 (September 2014): 30-35

Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." California Law Review 105, no. 3 (June 2017): 735-750.

Ajunwa, Ifeoma. "Confronting Surveillance." Jotwell: The Journal of Things We Like (Lots) 2022, no. 5 (May 2022).

Anwar, Oves, Ayesha Malik, Abraze Aqil and Noor Fatima Iftikhar. "Cyber Surveillance and Big Data - Pakistan's Legal Framework and the Need for Safeguards." RSIL Law Review 2020 (2020): 35-56.

Aziz, Jamal, Ayesha Malik, and Noor Fatima Iftikhar. "Public Health vs. Individual Privacy in the Age of Cyber Surveillance." RSIL Law Review 2020 (2020): 10-30.

Banks, William C. "Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage." Emory Law Journal 66, no. 3 (2017): 513-525.

Carroll, Erin C. "News as Surveillance." Washburn Law Journal 59, no. 3 (2020): 431-441.

Chan, Anna W. "The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware." Brooklyn Journal of International Law 44, no. 2 (2019): 795-820.

Cristian, Radu Dan. "Cyber-Terrorism." Drepturile Omului / Human Rights 2009, no. 2 (2009).

Das, Shubhankar, and Sarthak Patnaik. "Cyber Space Mass Surveillance Programs and Violation of Human Rights: The Way Ahead." Indian Journal of Law & Public Policy 2, no. 2 (2016).

Dragomir, Andreea. "Cyber Diplomacy." International Journal of Information Security and Cybercrime 10, no. 2 (2021).

[46] Andreea Dragomir, "Cyber Diplomacy," *International Journal of Information Security and Cybercrime* 10, no. 2 (2021): 37-40

Franks, Mary Anne. "Democratic Surveillance." Harvard Journal of Law & Technology (Harvard JOLT) 30, no. 2 (2017): 425-465.

Gilmore, Scott A. "Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act." Columbia Human Rights Law Review 46, no. 3 (2015).

Green, Rebecca. "Election Surveillance." Wake Forest Law Review 57, no. 2 (2022).

Harvey, David J. "Here's the Thing: The Cyber Search Provisions of the Search and Surveillance Act 2012." Digital Evidence and Electronic Signature Law Review 10 (2013): 39-50.

Huey, Laura, and Richard S. Rosenberg. "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention." Canadian Journal of Criminology and Criminal Justice 46, no. 5 (October 2004).

Jose, nandu sam. "Information and Communication Technologies and the Right to Informational Privacy in Health Care: A Comprehensive Analys". Brawijaya Law Journal 10, no. 1 (2023).

Joshi, Kartikeye. "Cyber Security and Cyber War." International Journal of Law Management & Humanities 4 (2021).

Jupillat, Nicolas. "From the Cuckoo's Egg to Global Surveillance: Cyber Espionage That Becomes Prohibited Intervention." North Carolina Journal of International Law 42, no. 4 (2017): 933-968.

Kanetake, Machiko. "The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches." Business and Human Rights Journal 4, no. 1 (January 2019): 155-158, http://dx.doi.org/10.1017/bhj.2018.18.

Katyal, Sonia K. "The New Surveillance." Case Western Reserve Law Review 54, no. 2 (2003).

Kleffner, Jann K., and Heather A. Harrison Dinniss. "Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations." International Law Studies Series. US Naval War College 89 (2013): 512-535.

Krause, Jason. "Cyber-Libertarians." ABA Journal 89, no. 11 (November 2003).

Macak, Kubo. "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers." Leiden Journal of International Law 30, no. 4 (December 2017): 877-890. http://dx.doi.org/10.1017/S0922156517000358.

Matwyshyn, Andrea M. "CYBER." Brigham Young University Law Review 2017, no. 5 (2017).

Ncube, Caroline B. "Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-Surveillance in South Africa." SCRIPTed: A Journal

of Law, Technology and Society 3, no. 4 (December 2006): 344-350. http://dx.doi.org/10.2966/scrip.030406.344.

Neutze, Jan, and J. Paul Nicholas. "Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms." Georgetown Journal of International Affairs 14, no. 3 (2013).

O'Malley, George. "Hacktivism: Cyber Activism or Cyber Crime." Trinity College Law Review 16 (2013).

Pattnaik, Abhilash, and Soumya Kumar Palo. "Cyber Sovereignty: A Dichotomy." GNLU Law Review 5 (2018).

Qiang, Xiao. "The Road to Digital Unfreedom: President Xi's Surveillance State." Journal of Democracy 30, no. 1 (January 2019): 53-67.

Rodrigues, Viola. "Cyber Stalking Issues of Enforcement in Cyber Space." International Journal of Law Management & Humanities 3 (2020).

Roy, Anish. "Privacy Issues in Cyber World." International Journal of Law Management & Humanities 3, no 3 (2020): 1388-1397.

Rozenshtein, Alan Z. "Surveillance Intermediaries." Stanford Law Review 70, no. 1 (January 2018).

Sales, Nathan Alexander. "Regulating Cyber-Security." Northwestern University Law Review 107, no. 4 (2013).

Shruti, Ashutosh Kumar, and Priya Ranjan. "Prevailing Cyber Security Law." Supremo Amicus 29 (2022).

Sihabudin, "Expanding the Limitations of the Protection and Processing of Children's Personal Data: An Overview of Current Regulations, Challenges, and Recommendations." Brawijaya Law Journal 10, no. 1, (2023), p.59. DOI: https://doi.org/10.21776/ub.blj.2023.010.01.04

Simpson, Brian, and Maria Murphy. "Cyber-Privacy or Cyber-Surveillance: Legal Responses to Fear in Cyberspace." Information & Communications Technology Law 23, no. 3 (2014): 189-191. http://dx.doi.org/10.1080/13600834.2014.978551.

Singh, Prabhjot. "Data Encryption and Surveillance." Supremo Amicus 18 (2020): 639-643.

Solis, Gary D. "Cyber Warfare." Military Law Review 219 (2014): 1-52.

Tafoya, William L. "Cyber Terror." FBI Law Enforcement Bulletin 80, no. 11 (November 2011): 1-7.

Tsaugourias, Nicholas, "Borders and the Territorialisation of Cyberspace." Indonesia Journal of International Law 15, no. 4, (2018) p.545-550

Tsuchiya, Motohiro. "Japan's Response to Cyber Threats in the Surveillance Age." Seton Hall Journal of Diplomacy and

International Relations 17 (2015-2016): 7-20.

Weisburd, Kate. “Punitive Surveillance.” Virginia Law Review 108, no. 1 (March 2022).

Yadin, Gilad. “Virtual Reality Surveillance.” Cardozo Arts & Entertainment Law Journal 35, no. 3 (2017): 707-742.

Zavrsnik, Ales, and Pia Levicnik. “The Public Perception of Cyber-Surveillance before and after Edward Snowden's Surveillance Revelations.” Masaryk University Journal of Law and Technology 9, no. 2 (2015): 35-37. https://doi.org/10.5817/MUJLT2015-2-3.