CYBER SECURITY REGIMES AND THE VIOLATION OF INTERNATIONAL LAW IN THE CONTEXT OF PEGASUS CONTROVERSY

Farooq Umair Niazi
Assistant Professor
Punjab University Law College
Lahore – Pakistan
farooqumair1967@gmail.com

Hassan Sattar Sharif
Lecturer
School of Law
University of Gujrat
Gujrat – Pakistan
hassan.sattar@uog.edu.pk

Rimshah Zubair
Law Scholar
School of Law
University of Gujrat
Gujrat – Pakistan
17161624-078@uog.edu.pk

Abstract:

The right to privacy has been articulated in all major international and regional human rights legislations including United Nations Declaration of Human Rights, 1948. The right to privacy protects individuals against arbitrary and unjustified use of power by states and other institutions. However, this right is subject to violations for centuries through conventional and unconventional means of surveillance by governments and other agencies on an international scale. Recently, The Pegasus controversy has wreaked havoc in the international community. This infringement of right to privacy has produced dire consequences for both individuals and governments with a threat to destabilize the whole economic and social systems of the world. Unfortunately, there is no legal framework in international law to handle such cyber-attacks against civilians and governments. The present study discusses, by adopting through doctrinal and empirical approaches, the significant challenges to

privacy with reference to the misuse of Pegasus spyware by the governments. The study highlights the necessity of an international legal framework to address the issues of cyber-attacks. Powerful institutions of different governments do often abuse laws by finding loopholes in international as well as their respective municipal laws to invade the privacy of individuals.

Keywords: International Law, International human rights law, breach of human rights, cyberattacks, cybersecurity, right to privacy, doctrinal, empirical, Pegasus, surveillance.

Introduction:

> ***There has been a never-ending conflict between those who make the laws and those who break them since creation's peaceful dawn was interrupted by the death cry of the murdered Abel, and Jehovah marked Cain as a "fugitive and a vagabond," cursed from the earth that had opened its mouth to receive his brother's blood from his hand.***[1]

Criminals always finding ways to satisfy their urgency of violence through different mediums. In this era of advance technologies where the mysteries of the world are a click away and the internet has brought the globe at our finger tips, guilty minds have advanced to and have become crafty digital criminals.

Right to Privacy:

Privacy, trust and security are interconnected with each other to the extent that the violation of one entails a threat to others. All of the three are important from the ethical as well as of legal point of view. To combat cybercrime, amendments to national substantive legislation (e.g., declaring cybercrime a criminal offence) , are essential, as well as criminal procedural law (i.e., to establish the procedures for criminal investigations and prosecutions). The Convention is a mutual legal assistance pact (i.e., a treaty between countries to assist in the investigation and prosecution of specified and/or all crimes prohibited by both parties' national laws; Maras, 2016). For countries that do not have one, the Convention establishes mutual assistance guidelines and serves as a mutual legal aid treaty (i.e., a pact between countries to collaborate in the investigation and punishment of specific and/or all crimes). Despite the lack of a universal definition of privacy, due to

[1] Quotation by Guy H. Thompson, reproduced by F. Gregory Lastowka and Dan Hunter, "Virtual Crime", New York Law School Review. July 2004

social, cultural, legal and economic diversity, it has been universally acknowledged that right to privacy comes under the much broader principle 'ethic of care'. Fundamental rights are those which are fundamental to humans' growth, development, wellbeing and existence. Such rights can neither be created nor derogated from under any circumstances. Humans possess these rights by virtue of their quality of being humans. The right to privacy is an undeniable human right which ensures safeguard against all types of intrusions of one's personal space and information. The apex feature of this right is to shield the personal dignity of a person. It supports the fundamental principle of personal respect and honor. The right to privacy broadens beyond data protection, protects the respect of family rights, religious, political and sexual preferences, the interference of communications, the use of hidden cameras, digital surveillance and genetic testing etc. For a long time, people have been concerned about their privacy in various ways. However, today's unparalleled innovation in information technology may jeopardise a person's safety, necessitating the creation of appropriate protection measures. (Im, 2003). The right to privacy is incorporated in various international and regional human rights treaties and conventions. The UDHR (1948), ICCPR (1966), ECHR (1950), Britain's Human Rights Act (1998), Britain's Data Protection Act (2018), the constitutions and the laws of different states incorporate the provisions regarding the protection of the right to privacy.

Cybercrimes and Cybersecurity:

As they say, everything good comes at a price, the internet came at a very high price of violating basic privacy rights of individuals and states. In the modern world, access to the world of internet or simply the internet has become a necessity rather than a luxury. The socio-economic wellbeing of the people and the interest of the investors in investing in the Information Technology (I.T) industry, resulting in a healthy competition between/among the Internet Service Providers (ISPs), have made access to the internet very much cost-effective. Cybercrimes in the 21st century have become a threat to everyone. No one feels safe, not unless they lock themselves away in a coffin and never touch a digital device. Individuals are fighting for their privacy while states are striving to protect their sovereignty, their internal and external defenses and concerned policies. Cybersecurity is an emerging question which haunts every single person and entity who are threatened by breach of privacy and internal security. The issue of cybersecurity is increasing rapidly and the world is moving towards cyberwars. This can be seen from the cyberwars between the U.S and China and between Pakistan and India. It would not be wrong to say that brains behind cybercrimes are more dangerous than those behind physical ones due their surreptitious nature.

The significant rise in digital crimes and surveillance were witnessed during the second half of the 19th century, when people started using personal computers (P.Cs). The hackers would send spywares, malwares etc. through emails and attack the computers by stealing other's sensitive personal information and gaining access to other sensitive information of such nature. With the passage of time, cybersecurity became a serious concern for states as hackers now broadened their "playing fields" by attacking national and international governmental databases. Nations felt the need to legislate on the issue. The purpose of cybersecurity is to keep the sensitive personal information safe from digital hackers and attackers. The depiction of this security is to deal with threats and figure out the origins and Internet Protocol (IP) addresses of these threats against the network system. The prime object of cybersecurity is to govern cyberspace in an appropriate manner, keep a check on the unbridled use of cyberspace that infringing the liberty and privacy of an individual, to facilitate and ensure a peaceful and cordial flow of information and communication and lastly to creating normalcy on the use of internet by holding those accountable who infringe/violate the liberties and privacy of others. The privacy issue is like a double edged sword that needs a careful balance between protecting a user's privacy and sharing data for convenience and other benefits. (Im, 2003)

International and Regional Instruments on Cyber Security:

With the passage of time, cybercrimes made their way in international community by infiltrating the privacy of states and posing a threat to their sovereignty. Consequently, there are now international and regional treaties on cybercrimes and cyber security. The 2001 Convention on Cybercrime of the Council of Europe is a good example. The goal of this convention is to harmonize national legislation while also strengthening cybercrime investigation tactics and regional cooperation. It also advises signatories on the steps that must be taken adjustments additions to national substantive legislation (e.g., making cybercrime a criminal offence) and criminal procedural law to combat cybercrime (i.e., to establish the procedures for criminal investigations and prosecutions). The Convention is a mutual legal aid pact (i.e., an agreement between countries to cooperate on investigations and prosecutions of certain and/or all offences outlawed by both parties under national law; Maras, 2016). The Convention gives instructions on mutual assistance and functions as a mutual legal aid treaty (i.e., an agreement between countries to cooperate on investigations and prosecutions of certain and/or all offences) for countries who do not have one.

There are also regional cybersecurity treaties:
• The 2001 Agreement on Cooperation in Combating Computer-Related Offenses.

• Arab Convention on Combating Information Technology Offenses (Arab Convention on Combating Information Technology Offenses) (Arab Convention on Combating Information Technology

• The Shanghai Cooperation Organization's Agreement on International Cooperation in the Field of Other than regional and international instruments, states have their own laws to curb digital crimes. An instance of this is the Prevention of Electronic Crimes Act, 2016. However, cybercrimes are alarmingly increasing. One incident which has taken a big toll on the international community is the aftermath of the "Pegasus Controversy".

"It's horrifying, because you think that this tool that you're using is encrypted, you can use it… but then you realize that NO, The moment you're on the internet they watch you," said Khadija Ismayilova, A journalist from Azerbaijan who's only one of 50,000 victims of the notorious spyware called "Pegasus" developed by Israel-based cyber security company. One's right to privacy and freedom of expression are fundamental human rights which are explicitly declared to be the lynchpin of democracy. But modern problems require innovative and out of box solutions. The advancement of technology does not give anyone the right to infiltrate into the private lives of individuals. The Pegasus software was designed to compromise mobile phones sophisticatedly without using the conventional methods of spying. This software is sold to Governments to advance their criminal justice systems. The objective that entailed the development of Pegasus software were allegedly National Security concerns of different totalitarian states yet the developers oversaw the atrocities humans can commit against each other when given the opportunity, not to forget Notpetya and wannacry ransome cyber-attacks. A facet of a big intrusion in Privacy came to light in 2016 when cyber-attacks through Pegasus were revealed in a leaked list of 50,000 mobile phone numbers which were potential targets of this software. Consequently, a collaborated investigation was started by the international media under the aegis of International Consortium of Investigative Journalists (ICIJ). The investigation revealed cyber-attacks on civilians including journalists, Human Rights activists, Lawyers and prominent Political opponents of the governments of different states. Pegasus investigation sparked an outrage in the international community because this violation of privacy could destabilize whole economic and social system of different states and, resultantly, the ideals of democracy of the free world and could spread chaos.

Violation of Right to Privacy by Governments and their Agencies:

Human beings value their privacy and the protection of their personal sphere of life. (Philosophy, 2019). According to Merriam Webster dictionary, Privacy is described as a circumstance in which someone violates a person's right to privacy by disclosing personal

information. One, who knowingly intrudes, physically or otherwise, into another's solitude or seclusion, or his private affairs or concerns, is responsible to the other for invasion of privacy, according to the American Law Institute's Restatement of the Law of Torts, (1976). A person who knowingly intrudes, physically or otherwise, into another's solitude or seclusion, or his private affairs or concerns, is responsible to the other for invasion of privacy if the invasion would be exceedingly disagreeable to a reasonable person. In Whalen v. Roe, the United States Supreme Court made the most extensive attempt to define the right to privacy to date, covering both physical and mental private encompassing an "individual interest in avoiding disclosure of personal matters" and (ii) an "interest in independence in making certain kinds of important decisions". (Whalen v. Roe, 1977) Thus, privacy is a fundamental right essential to the autonomy and protection of human dignity. (International, 2017) The autonomy is essential in making humans free agents who can make their decisions independently and choose freely. The rules that protect privacy give us the ability to assert our rights in the face of significant power imbalances. (International, 2017). These power imbalances are of structural nature which goes to the very root of us being human. The violation by governments of the Right to Privacy of Individuals has been carried out through centuries. Specialized governmental agencies are tasked with the duty of spying and carrying out surveillance upon its individuals. The act of surveillance carried out by the governments and their respective agencies make the states Orwellian-states. Power inflicts responsibility, so goes a saying. This abridgement of privacy and individual liberty in carried out in two manners:

i) Through Conventional Means:

Conventional means of invading a person's privacy include but are not limited to eavesdropping, employing government agencies and agents to carry out spying on a person, wiretapping, snooping et al. It is to be noted that spying on a person is contradistinguished with spying on other states and governments. With the end of the industrial age, the conventional means of invading a person's privacy are fast becoming redundant.

ii) Through Unconventional Means:

With the advent of post-industrial and Information Technology age, there is now a virtual Internet of Things (IOT). Everyone has access to the internet and nearly everyone has got a smartphone. Now, most people can access things online, from access to research papers to online shopping, from availing online medical counselling to online banking, from trading in stocks to online learning. As smartphones are becoming ubiquitous, the world is just a click away from people but this comfort is fraught with its own

consequences in the form of hacking through malwares, spywares, cyberbullying, cyberstalking, electronic surveillance, data collection and storage etc. People can enjoy facilities but at the same time their privacies, freedoms and liberties are at risk and hence they are more insecure than before.
According to the Fourteenth Amendment to the American Constitution famously known as the due-process clause, "no state shall deprive any person of life, liberty or property, without due process of law".

A sphere of action in which society, as distinguished from the individual, has, if any, only an indirect interest: comprehending all that portion of a person's life and conduct which affects only himself, or, if it also affects others, only with their free, voluntary, and undeceived consent and participation. When I say only him, I mean directly and in the first instance; for what- ever affects him may affect others through him. This, then, is the appropriate region of human liberty. (Mill, 1859)

7. Is Digital Surveillance A Threat to The Global Social, Political And Economic Order?

Digital surveillance by the governments and the mushroom growth of dark web has increased the threat of global disorder to an unprecedented scale. Through anonymous digital surveillance through unencrypted messages, the moods of different stakeholders can be manipulated to such an extent that the international socio-political and socio-economic are in jeopardy. As seen in the 2016 American Presidential elections, the moods of the voters were cleverly manipulated by the use of digital surveillance and breaching through emails of a presidential candidate by leaking the sensitive information to the press. By breaching the encrypted emails of a U.S presidential candidate in the sole superpower and a practicing democracy, the very principles and ideas of democracy were put at risk. Through this, the dark web was instrumental in subsiding the importance of popular votes, as seen by the fact that the emails of one of the U.S presidential candidates were leaked to the journalists.

As the world stands today, the importance of modern technology cannot be underestimated as it has become the lynchpin and a necessity of living. It is the need of the hour to develop and implement such framework(s) that the world is not steeped into chaos. It can be done, on one hand, by developing such firewalls and software that combat the threats to progress, prosperity and development while ensuring peace, order and stability and, on the other hand, by making and implementing laws that combat threats to cybersecurity on a global scale as well as encouraging the UN member states to legislate and implement, in their municipal laws, the recommendations passed by an international

convention, especially convened to address issues of cybersecurity and threats to it called by the UN.

8. Digital Surveillance-A Threat to Human Rights:

Technology-where it has granted opportunities, equality and liberties to the people, it is also marred with its dark side. The scholars and researches call it the Dark Web and it is becoming an instrument in limiting and restricting the autonomy and liberty of people. Thus, individual liberty is becoming at stake. Liberty makes us humans because of the choices that people make. Freewill includes exercising one's choice of one's own accord in such a way that it leads to one's growth and development and without interference from external factors and circumstances. Freewill, liberty and freedom are the rights that define us as humans, grant humans' autonomy and cannot be derogated from in and under any circumstances. All these are the part and go to the root of human agency. As the world is fast becoming a global village due to the onslaught of IOT, humans are becoming more vulnerable in their online interactions. This aspect was underscored by firstly but not lastly by the Swedish blogger Julian Assange and then by a former employee of the America's premier spy agency, Central Intelligence Agency (CIA), Edward Snowden.

Though there is cultural relativism debate as to what constitutes privacy and her breach, scholars and researchers are able to put universal aspects on it. These are legal and ethical, societal and environmental principles which would constitute the norms of privacy and her breach. Breach of human rights, of which individual liberty is but only a part, is considered to be against the norms, principles and spirit of democracy. This was seen during the Watergate Scandal in which a sitting President of the United States of America, of the Republican Party, had to resign because of him ordering, while in office, the wiretapping of the communications of the members of the opposition party. The Watergate Scandal proved to be the tipping point of how and to what extent the restrictions on individual liberty could and would be tolerated.

9. Necessity for International Rule Of Law To Address Cyber-Security Issues:

It is the need of the hour to chart out a framework to address the issues of privacy and cybersecurity. Currently, there are different cybersecurity regimes that deal with the issues of protecting and safeguarding individual liberties. But the need is to develop a coherent and global regime that adheres to protecting individual human liberty, autonomy agency. Such a framework would protect the interests of individuals and prevent from infringing individual autonomy. As article 38(1)(c) of the Statute of International Court of

Justice (ICJ) lists General Principles of Law recognized by the Civilized States as one of the sources of International Law and refers that while hearing a dispute between or among the subjects of International Law, the World Court would resort to it, after treaties and International Customs, in making a decision.

If a global framework has to be formed, it should also look at the different cybersecurity regimes operating in different states and then forming a coherent outlook. The United Nations Security Council (UNSC), as an executive organ of the United Nations (U.N), should play her role in enforcing and implementing the cybersecurity regime and sanctioning the breaches of privacy.

It would be appropriate to refer to a few case studies regarding the extant of the breach of privacy and data protection.

Case 1

Spyware has always been a murky subject in terms of spying between governments. Spyware has long been recognized as a significant form of online surveillance since it is considered critical to track and target users who may be involved in criminal or terrorist activities. On the other hand, it is highly contentious because, in the name of combating criminal activity, such groups, multi-national corporations (MNCs), and companies may attack civil citizens or protestors in any location. This is an important point to remember since such meddling might result in a cyberwar or cyberattack, which could affect the political system of a country like Estonia. The Pegasus case has brought to light the forthcoming cybersecurity challenges.

Case 2

During a bitter court battle over custody of their children, Sheikh Mohammed bin Rashid al Maktoum, the absolute ruler of Dubai, was found to have ordered the deployment of one of the world's most powerful malware strains against Princess Haya bint Hussein, his former wife and a member of the Jordanian royal family.

The publicized judgements also indicated that meticulous InfoSec work by Canada's Citizen Lab, an academic surveillance research organisation, had assisted in uncovering the spying and alerting its victims. Princess Haya, her UK legal team, her physical security detail, and others in her entourage were all targeted by the Sheikh's agents.

NSO informed the High Court that its contract with the United Arab Emirates had been cancelled.

Case 3

The Pegasus spyware program, which is used by governments to infiltrate iPhones used by criminals, journalists, and activists, was developed by NSO Group has been sued by Apple Inc.

Pegasus is NSO Group's most well-known spyware technology, ostensibly designed to combat criminal behavior but inadvertently used against innocent people. Apple launched a lawsuit against both NSO Group and its parent firm in an attempt to block preventing the company from continuing to provide Pegasus to its customers.

Apple Inc. wants NSO Group to be held accountable for spying on some Apple users. In addition, the lawsuit seeks an injunction prohibiting NSO is prohibited from using any Apple products, services, or gadgets

Following reports from the Pegasus, the lawsuit was filed.

"State-sponsored actors like the NSO Group spend millions of dollars on sophisticated surveillance technologies without effective accountability. That needs to change," Craig Federighi, Apple's SVP of Software Engineering, stated. "Apple devices are the most secure consumer hardware on the market -- but private companies developing state-sponsored spyware have become even more dangerous."

"While these cybersecurity threats only impact a very small number of our customers, we take any attack on our users very seriously," Federighi continued, "and we're constantly working to strengthen the security and privacy protections in iOS to keep all our users safe."

Along with the filing, Apple has said it will be contributing $10 million and damages from the lawsuit to organizations related to cyber surveillance research and advocacy.

Apple is also assisting Citizen Lab, a group that Apple commends alongside Amnesty Tech in uncovering and researching the intrusions and surveillance abuse, by providing pro-bono technical, threat intelligence, and engineering assistance for Citizen Lab's research. Apple is also offering the same assistance to other organizations in the same space.

The lawsuit has been applauded by Citizen Lab director Ron Deibert for holding NSO Group "accountable for their abuses, and hope in doing so Apple will help bring justice to all who have been victimized by NSO Group's reckless behavior."

10. Conclusion:

The right to get access to modern means of communication and the use of modern technology has become an inalienable right of today's living. The right is fraught with not only great opportunities but also with great risks. These risks are of such nature as to bring the whole debate of autonomy and liberty into question. Sometimes the collective moods of the people of a community are tampered with. Sometimes the liberties of people are under the watchful eyes of governments and sometimes by organizations and corporation and such other entities. Thus, a common framework of the international community is required to cope with the challenges produced by this menace.

References:

Bernal. P. (2016). Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy, 1*(2), 243-264, Full article: Data gathering, surveillance and human rights: recasting the debate (tandfonline.com)

https://plato.stanford.edu/entries/it-privacy/

Mills, J. S. (1859). *On Liberty* (1st ed.). John W. Parker and Son.
http://ntia.doc.gov/page/chapter-5-technology-and-privacy-policy

What Is Privacy? | Privacy International
Privacy: The new generations | International Data Privacy Law | Oxford Academic (oup.com)