Shielding Privacy in the Surveillance Era: A Comparative Study of India, USA and South Africa

Submitted: 18 December 2023
Reviewed: 2 March 2024
Revised: 6 March 2024
Accepted: 18 March 2024

Article submitted to peer blind review

Stency Mariya Mark *
https://orcid.org/0000-0003-3991-5438

Dr. Aaratrika Pandey**
https://orcid.org/0000-0001-9961-3111

DOI: https://doi.org/10.26512/lstr.v16i2.51916

Abstract

[Purpose] The right to privacy has been gravely undermined in the pretence of "protecting national security and safety". Although the idea of privacy has been around for a while, it has only recently come to be acknowledged as a human right. The researchers have juxtaposed the jurisprudence developed surrounding privacy in India with that of South Africa and the United States to analyse its evolution and conceptualisation.

[Methodology] Comparative analysis, judgment analysis, deductive method and critical analysis have been adopted by the researchers.

[Findings] It was deduced that on comparison of the three nations, South African premise of privacy is significantly stringent when compared to the other two countries i.e. India and US.

[Practical Implications] The debate that commenced years ago is still going robust and revolves around whether the "right to privacy" of an individual should be prioritised before the state's utilitarianism. The Indian, American and South African governments have "valid" concerns about public safety and national security. However, the government must understand that protection must not come at the expense of the fundamental right to privacy or as a matter of fact any other human rights, especially when they are arbitrary. Obtaining access to personal data can be exploited for nefarious and arbitrary reasons under the pretence of national security. Upon analysis, it can be deducted that on comparision of the three nations, South African conceptualisation of the

*Assistant Professor of Law in Galgotias University, India, markstencymariya@gmail.com.
**Assistant Professor of Law, Manav Rachna University, Faridabad, India, pandeyaaratrika0003@gmail.com.

premise of privacy is significantly stringent when compared to the other two countries i.e India and US. US's structure and premise of privacy in the surveillance era looked weaker when compared to India and South Africa. India's tenents of the same can be positioned in the centre of spectrum/scale. The article further elucidates how Pegasus and Snowden revelations reveal the weak conceptualisation of privacy in US.
[Originality] There are various instances where the data is being used to monitor "targeted" people like journalists, activists and used to "silence" them. In reality, a targeted monitoring programme in accordance with global human-rights norms may be used to better address security risks like terrorism. This conceptualization of "silencing surveillance" is the original work of the researchers.

Keywords: Surveillance. Panopticon Model. Pegasus. Snowden Revelations. Privacy.

INTRODUCTION

Everyone has some private and inconspicuous aspects of their lives that cannot be revealed and shared with the public at large. Privacy is now acknowledged as a "fundamental" right; initially, the very right to privacy might not have been acknowledged, but the notion of privacy existed. The right to privacy evolved over time as a result of judicial pronouncements and discourses. In *R.* v. *Dyment*, it was held that "privacy is at the heart of liberty in a modern state […] Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order." However, this right to privacy over the years has been grossly exploited and violated. One can assert without a shadow of a doubt that we live in a monitoring, digital, and surveillance age. We live in an age of constant digital monitoring and observation, creating a surveillance state which deploys intrusive measures of data collection. The extent of surveillance has gone beyond that of GPS tracking; applications like smartwatches are nothing more than systems that continuously record human activity, body temperature, etc.

The authors have compared the rules governing surveillance in India with those in South Africa and the US. The main justification for considering South Africa and the United States is that both of these countries have democratic governments with strong judiciaries, much like India. The paper aims to provide a novel viewpoint based on a comparative analysis of these nations. The Part II of the article provides information on how the right to privacy was initially conceptualized and how it evolved over many years through legislative changes and significant legal precedents in South Africa, India, and the United States. Part III of the article reflects on the Snowden revelations in 2013 by a whistleblower, which revealed how the US engaged in illegitimate and violent

mass surveillance. The Part IV of the article reflects about the Pegasus spyware which was developed to facilitate the governments to do mass surveillance across the countries and violating the right to privacy of individuals.

EVOLUTION AND BURGEONING OF THE RIGHT TO PRIVACY

Pavan Duggal said "[m]an is a social animal but despite all his social leanings, there is a small area coming within the exclusive limits, which any man treasures and cherishes. This is the domain of individual privacy [italics]." (Duggal, 2018, p. 310) Since inception, the idea of "privacy" has been the subject of discourse, dispute, and consideration. Privacy had been around even prior to the 19th and 20th centuries, despite the premise that this is when it first became widely recognised as a right. (Konvitz, 1966, p. 272) The concept of privacy has a very long history, and its roots can be seen in primitive civilizations. Even within the Holy Book of the Bible, there are several chapters when the invasion of privacy first takes place. (The Holy Bible, Genesis 3:7 2013) Adam and Eve, who first began to conceal their nakedness with leaves in order to maintain their modesty and privacy. (The Holy Bible, Genesis 3:7 2013) Etymologically the term privacy has been derived from the Latin term 'privas' whose archaic meaning was being 'single'. (Hirshleifer, 1980, p. 651)

In the article titled "The Meanings of "Individualism," Steven Lukes argues how the sense of "individualism" has helped to shape and create the idea of privacy. (Thaorey, 2019, p. 161) The individualism idea holds that because God gave each person a life, they are independent beings who are entitled to all freedoms, including the right to privacy. (Thaorey, 2019, p. 161) Even John Locke, the English philosopher, thought that freedom and privacy go hand in hand and that privacy is an essential part of freedom. (Locke, 1689, p. 8)

The Indian Jurisprudence of Right to Privacy

Although the right to privacy is not stated explicitly as a fundamental right in the Indian Constitution, the judicial framework has ensured this through several judicial pronouncements and made it a fundamental right. Initially, the Indian legal system did not acknowledge the right to privacy as a basic fundamental right. The researchers have observed the Indian jurisprudential construction and shift in the right to privacy from its negation to its wide acceptance as a fundamental right. In *Kharak Singh* v *State of Uttar Pradesh and Ors*, it was held;

> "[T]he right of privacy is not a guaranteed right under our Constitution and therefore the attempt to ascertain the movements of an individual which is

> merely a manner in which privacy is invaded is not an infringement of a fundamental right guaranteed by Part III."

Even in *M P Sharma and Others* v. *Satish Chandra, District Magistrate & Others,* the Supreme Court didn't recognise the right to privacy being a fundamental right. But over the years, the jurisprudence of right to privacy has been shifted from denial to acceptance of the fact that the right to privacy is a part and parcel of the article 21.

It emphasises upon the right to life and personal liberty of individuals which can be curtailed only by the procedure established by law. Further in *People's Union of Civil Liberties (PUCL) & Anr* v. *Union of India & Anr,* it was held that telephone tapping is a substantial violation of personal privacy, and only the Home Secretaries of the State and Central Governments may issue a telephone tapping order pursuant to Section 5(2) of The Indian Telegraph Act, 1885. *In Justice K.S. Puttaswamy (Retd.) & Anr.* v. *Union of India & Ors.* it was held;

> "Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III."

The judgment of *Justice K.S. Puttaswamy (Retd.) and Another* v *Union of India and Others overruled Kharak Singh* v *State of Uttar Pradesh and Ors and M P Sharma and Others* v. *Satish Chandra, District Magistrate & Others* to the extent that they do not recognise the right to privacy as a fundamental right. The judgement also recognised informational privacy as a facet of "right to privacy" and this informational privacy focuses on people's interests in exerting authority over accessibility to data concerning themselves. (Watt, 2017)

> "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. […] The creation of […] a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state. The legitimate aims of the state would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits. (Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors)"

Although the right to privacy has been declared and secured as a fundamental right in India, no fundamental right is "absolute," and rights have always been guaranteed in a limited sense by imposing reasonable restrictions. The right to privacy is part of Article 21 of the Indian Constitution. The article in itself propagates the idea that life and personal liberty can be curtailed or limited by a "procedure established by law". So, generally speaking, the right to privacy can be lawfully invaded with a minimum of checks and balances through a wide range of legislative provisions. Usually, the right to privacy is compromised in the disguise of national security and safety. But how much surveillance is justified? With few checks and balances, surveillance has historically been considered a governmental entitlement to deploy intrusive tactics against its people.

The laws in India permit the government for lawful interception and monitoring like the section 5 of The Indian Telegraph Act, 1885. Other than that, under the Information Technology Act provisions like section 69 of The Information Technology Act, 2000 permits interception, monitoring or decryption of any information through any computer resources, and section 69B of The Information Technology Act, 2000 authorises monitoring and collection "traffic data or information" through any computer resource for the enhancement of the cyber security of the nation.

The American Jurisprudence of Right to Privacy

Just like the Constitution of India, the United States Constitution does not "expressly" mention the right to privacy, which has produced a plethora of challenges in defending individual privacy rights. (Kaur, 2018) In *Katz* v. *United States*, the United States Supreme Court reversed its prior decision in *Olmstead* v. *United States* and upheld the Fourth Amendment, which said that the Fourth Amendment gets triggered every time the government would be infringing on a citizen's "reasonable expectation of privacy." The First, Third, Fourth, Fifth, ninth, and Fourteenth amendments of the United States Constitution and innumerable landmark judicial pronouncements helped to develop the jurisprudence protecting the privacy rights of US citizens. (Kaur, 2018)

According to the decision in *Stanley* v. *Georgia*, the First and Fourteenth Amendments of the United States Constitution forbid the government from making it illegal to just have obscene material in one's personal possession. In this case, Justice Marshall noted that "if the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds." The Fourth Amendment was created to protect people from arbitrary

and unreasonable searches and seizures. It wasn't entirely apparent, though, if it was sufficiently inclusive to cover the right to privacy. Louis D. Brandeis and Samuel D. Warren's article "The Right to Privacy," which has been regarded as one of the most significant pieces of writing, is typically seen as the basis for the concept of the right to privacy. (Kramer, 1990, p. 703)

In *Roe* v. *Wade*, the Texas law that outlawed abortions was overturned by the Supreme Court. The court's ruling was predicated on the idea that a person's right to privacy includes their ability to get an abortion. However, the Supreme Court's decision in the case *Dobbs* v. *Jackson Women's Health Organization* struck down that which had been established by earlier rulings in the cases *Roe* v. *Wade* and *Planned Parenthood* v. *Casey*. This decision overturns the long-standing constitutional right to abortion and deprives women of their bodily integrity and right to privacy.

The judgement has "shaken" the very notion of the right to privacy in the US. In India, the conceptualisation and evolution of the right to privacy were evident in *Justice K.S. Puttaswamy (Retd.) & Anr.* v. *Union of India & Ors* while in US, *Katz* v. *United States* and *Roe* v. *Wade* highlighted and recognised the right to privacy of the people. However, wherein on one hand, the researchers observed Indian jurisprudential shift in the right to privacy from its negation to its wide recognition as a fundamental right. The same claim cannot be made for the US as from its acceptance as a pivotal and crucial right it has been devalued, denied and negated as observed in *Dobbs* v. *Jackson Women's Health Organization.*

Furthermore, there are some instances wherein the government purchases data from private entities in order to intercept, decrypt, and store the information for subsequent and unknown usage. (Richards, 2013, p. 1934) The use that follows data gathering, not the act of collecting the data itself, is what makes it dangerous. The privacy of an individual is threatened by the arbitrary use and abuse of the data collected. When data is used for purposes other than those for which it was originally intended, they are utterly arbitrary.

According to the statistics, in the United States, roughly 24,000 demands for user information from US law enforcement agencies were made to Google in the year of 2015, and it has almost tripled since 2010. (Rozenshtein, 2018, p. 114) Additionally, Facebook received approximately 37,000 additional demands for user information in 2015. (Rozenshtein, 2018, p. 114) Other 2013 statistics indicated that approximately 90,000 individuals or companies were monitored under the guise of Section 702 of the Foreign Intelligence Surveillance Act, 1978 (FISA) [If a person is outside of the United States and not inside, the government of the United States is allowed to undertake warrantless surveillance on that individual under Section 702] of the United States. (Rozenshtein, 2018,

p. 114) All of these searches used data from a commercial entity, and zero of them were carried out independently. This demonstrates how technological middlemen that assist in monitoring enable snooping. (Rozenshtein, 2018, p. 115)

The African Jurisprudence of Right to Privacy

According to Ian Currie and Johan De Waal, when an individual's personal privacy is unlawfully invaded or when private data about that person is unlawfully disclosed, their right to privacy has been breached. (Justice Mavedzenge, 2020, p. 11) The African Constitution has explicitly recognised the right to privacy in its section 14 unlike the Indian and US constitution.

One of the very first cases to recognise the right to privacy (Buthelezi, 2013, p. 783) was *O'Keeffe* v *Argus Printing and Publishing Co Ltd*. The concept of privacy has been defined in the case *Bernstein and Others* v *Bester NO* and Others that "[p]rivacy is an individual condition of life characterised by seclusion from the public and publicity. This implies an absence of acquaintance with the individual or his personal affairs in this state."

However, a report of surveillance conducted in six countries (Egypt, Kenya, Nigeria, Senegal, South Africa and Sudan) was prepared by Institute of Development Studies and the summary of surveillance of South Africa clearly stated that:

> "The state has been found guilty of using surveillance outside of the law. State surveillance powers have been used to monitor political opposition and business competitors. A challenge in the Constitutional Court found the state guilty of carrying out unlawful mass surveillance and foreign signal interception. Civil society has raised concerns about the rapid expansion of surveillance infrastructure including biometric registration, mandatory SIM registration, and CCTV surveillance. (Roberts et. al. 2021, p. 30)"

The legislation that was "developed" to protect the privacy of the citizens is the Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) Act 70 of 2002 but it was recently rules as "unconstitutional" by the Constitutional Court of South Africa in *AmaBhungane Centre For Investigative Journalism NPC and another* v *Minister of Justice and Correctional Services and Others; Minister of Police* v *AmaBhungane Centre for Investigative Journalism NPC and Others.* The court also emphasised that "RICA is considered unconstitutional to the extent that it fails to provide adequate safeguards to protect the right to privacy, as buttressed by the rights of access to courts, freedom of expression and the media, and legal

privilege". In all the three nations, surveillance is practised arbitrarily and is a common denominator.

Surveillance is usually compared to the Panopticon model developed by Jeremy Bentham. (Bentham, 1791, p. 5) The panopticon, a concept by Jeremy Bentham, is a well-known metaphor for surveillance. (Wacks, 2015, p. 3) The Panopticon Model is an architectural design intended to keep a check on inmates' actions and develop them into self-disciplined people who are always apprehensive about being watched. (McMullan, 2015) The model has a circular prison with a tower in the middle, and a bright light coming from the tower into the cells prevents the inmates from knowing who is watching them or even whether they are being watched at all, but it provides the guards the power to watch anyone and everyone they choose, exactly like the arbitrary targeted surveillance. (Bentham, 1791, p. 5)

Influenced by the panopticon, Michel Foucault related it to surveillance and said that contemporary civilizations were more concerned with monitoring and evaluating individuals in order to exert power over them and compel them to submit. (Foucault, 1977, p. 200) The Panopticon concept by Michel Foucault emphasises how people who are monitored would submit to the authorities. (Parikesit & Yudithadewi, 2020, p. 57)

Based on the above analysis, it can be deducted that on comparision of the three nations, South African conceptualisation of the premise of privacy is significantly stringent when compared to the other two countries i.e India and US and it is reflected in *AmaBhungane Centre For Investigative Journalism NPC and another* v *Minister of Justice and Correctional Services and Others; Minister of Police* v *AmaBhungane Centre for Investigative Journalism NPC and Others.* US's structure and premise of privacy in the surveillance era looked weaker when compared to India and South Africa. India's tenents of the same can be positioned in the centre of spectrum/scale. The article further elucidates how Pegasus and Snowden revelations reveal the weak conceptualisation of privacy in US.

SNOWDEN REVELATIONS

The definition of surveillance has evolved through time, and it can currently be broadly described as a ubiquitous, pervasive tool used in contemporary society that is intentionally and methodically exploited by powerful individuals. (Richards, 2013, p. 1934) Consequently, it is occasionally even used as a synonym for power. It focuses on gathering data on specific people and may be used as a covert kind of control. (Richards, 2013, p. 1934) In June 2013, Edward Snowden, a contractor for the National Security Agency,

exposed a plethora of data that revealed "classified" surveillance executed by the NSA in the United States. (Coyne, 2019, p. 65) GDPR rapporteur Jan Philipp Albrecht said "the revelation by Edward Snowden regarding the mass storage and analysis of details relating to our everyday lives by the secret services and their agents within the internet companies only served to demonstrate to us all how far things have already developed and how little regulation or effective control the people and society are able to muster." (Coyne, 2019, p. 70)

The discoveries made by Edward Snowden in 2013 (Rogers & Eden, 2017, p. 802) regarding the scope and complexity of governmental espionage (Završnik & Levičnik, 2015, p. 35) ignited a worldwide debate on surveillance. (Franks, 2017, p. 426) Information on the surveillance practises of the National Security Agency, also known as the NSA, was exposed by Edward Snowden. (Kwoka, 2015, p. 1398)

After his revelations, he was granted an "asylum" in the country Russia. (Kwoka, 2015, p. 1399) His leaks made a significant discovery regarding the NSA's internal surveillance of people who are residing within the territory of the USA. (Kwoka, 2015, p. 1399) In a testimony given to the European Parliament, Edward Snowden said:

> "One of the foremost activities of the NSA's FAD, or Foreign Affairs Division, is to pressure or incentivize EU member states to change their laws to enable mass surveillance. Lawyers from the NSA, as well as the UK's GCHQ, work very hard to search for loopholes in laws and constitutional protections that they can use to justify indiscriminate, dragnet surveillance operations that were at best unwittingly authorized by lawmakers. These efforts to interpret new powers out of vague laws is an intentional strategy to avoid public opposition and lawmakers' insistence that legal limits be respected, effects the GCHQ internally described in its own documents as "damaging public debate." In recent public memory, we have seen these FAD "legal guidance" operations occur in both Sweden and the Netherlands, and also faraway New Zealand. Germany was pressured to modify its G-10 law to appease the NSA, and it eroded the rights of German citizens under their constitution. Each of these countries received instruction from the NSA, sometimes under the guise of the US Department of Defense and other bodies, on how to degrade the legal protections of their countries' communications. The ultimate result of the NSA's guidance is that the right of ordinary citizens to be free from unwarranted interference is degraded, and systems of intrusive mass surveillance are being constructed in secret within otherwise liberal states, often without the full awareness of the public. (Austin, 2015, p. 109)"

Americans were horrified and upset by disclosures that their government was gathering data on their calls, messages, and web activities. (Wet &

Fairweather, 2013) However, they have less reason to be concerned than South Africans. Lawyer Mike Silber, a telecommunications expert, has claimed that the South Africans were subject to the same level of intrusive surveillance, if not worse. (Wet & Fairweather, 2013) He said "[i]t [The Regulation of Interception of Communications and Provision of Communication Related Information Act] […] [required] us to identify ourselves for internet services. What most people outside the industry do not know is that Rica also deals with lawful interception. One element of lawful -interception is so-called 'live' interception. This is where calls, emails, web sessions and other communication are forwarded to the Office of Interception Centres pursuant to a warrant so that the content of the communication is available." (Wet & Fairweather, 2013) The Guardian, a newspaper, has managed to get its hands on a classified document from the NSA which showed that the NSA had gained unfettered access to the networks of Facebook, Yahoo, search engines like Google, firms like Apple, Microsoft and many other US internet-associated firms. (Greenwald & MacAskill, 2013)

The document stated that this NSA access is a component of the PRISM programme, which allows authorities to gather information such as emails, (Edgar, 2017, p. 223) messages, audio, live interactions, videos, online activity, data transfer, etc. (Greenwald & MacAskill, 2013) PRISM is an acronym for "Planning Tool for Resource Integration, Synchronization, and Management". (Tariq, 2013, p. 372) PRISM was used as a code name by which the US NSA gathers internet communications from numerous US internet firms. (Tariq, 2013, p. 373)

India is ranked fifth out of all the nations targeted by NSA programmes, with millions of bits of data taken off its phone networks and computer infrastructure and networks. (Greenwald & Saxena, 2013) The Indian External Affairs Minister Salman Khurshid, responded to this surveillance by stating, "it is not actually snooping" (Bajoria, 2014) which in a way indicated his defence of mass surveillance being "normal".

The Snowden revelations didn't reveal any NSA spying on South Africa, but they did reveal the US government's ability to have unfettered access to surveillance on its own citizens and those of other countries. This means that, like the US government, governments in countries like India and South Africa clearly have the potency to do the same. The National Communications Centre (NCC) is South Africa's "national facility" for the government's collection and interception of electronic communications on behalf of the nation's surveillance and security services. (Human Rights Committee, 2016, p. 4) It comprises gathering and analysing information that comes from beyond South Africa's boundaries, travels through South Africa, or terminates there. (Human Rights Committee, 2016, p. 4)

The Matthews Commission (2008) concluded that the NCC engages in intelligence activities, such as widespread communication interception, in a way that is illegal and unconstitutional since it disregards RICA's rules. (Human Rights Committee, 2016, p. 4) Similarly, the Indian government has set up a central monitoring system (CMS) to intercept and monitor phone calls, landline calls, and internet traffic "lawfully." Such technologies are flagrant invasions of personal freedom, and it has been said that CMS is an "Indian PRISM," similar to the NSA's PRISM programme in the United States. (Kurup, 2013) The Edward Snowden revelations have brought to light the surveillance conducted by agencies such as the NSA and how governments have few laws and policies to protect privacy rights in theory, but fewer in practise and implementation.

PEGASUS: THE SPYWARE

The Canadian Citizen laboratory published about software in the year 2018 which was called “Pegasus”, a “spyware” developed and created by the NSO Group Technologies, an Israeli technology company. (Manohar Lal Sharma v Union of India). According to reports, this spyware can be used to infiltrate a person's electronic devices through zero-click vulnerabilities. (Rajan, 2021) Once the malware has gained unauthorised access to a user's device, (Shilliam 2022) it has access to all the data of the phone, like text messages, call records, etc. (Manohar Lal Sharma v Union of India) It is like the “entire control” can be remotely controlled by the “Pegasus user”. (Manohar Lal Sharma v Union of India) The NSO Group Technologies has claimed even on its own website that the “end users” of its software are “exclusively government intelligence and law enforcement agencies”. (Manohar Lal Sharma v Union of India)

Using spying spyware provided by the Israeli firm NSO Group Technologies (Targowski, 2021, p. 108), authoritarian governments have pursued human rights activists, reporters etc. all across the world. (Kirchgaessner, Lewis, Pegg, Cutler, Lakhani & Safi, 2021) In spite of this, NSO Group Technologies stated that it would “continue to investigate all credible claims of misuse and take appropriate action” and denied all the allegations against them. (Kirchgaessner, Lewis, Pegg, Cutler, Lakhani & Safi, 2021) Investigation during the following one to two years revealed some Indian journalists, court employees etc. were the targets of this spyware. (Manohar Lal Sharma v Union of India) A writ was filed, *Manohar Lal Sharma* v *Union of India*, in which the Supreme Court instituted a committee to find the “veracity” of the allegations (Naithani 2021) with respect to the Pegasus spyware. (Manohar Lal Sharma v Union of India) The Union of India has currently

refuted all the allegations and said that the said reports have "no factual basis". It was further contended by them that the Indian surveillance and interception laws are extremely stringent, making such serious invasions of privacy inconceivable. (Manohar Lal Sharma v Union of India) The case is pending in the Supreme Court.

In a report titled "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries" it was identified that 36 Pegasus operators were in existence in 45 countries, including India, (Kaldani & Prokopets 2022) South Africa and the United States. (Marczak, Railton, McKune, Razzak, & Deibert, 2018, p. 8) The operator name "GRANDLACS" (Marczak, Railton, McKune, Razzak, & Deibert, 2018, p. 14) has been active since 2017 and the operator name "MULUNGUSHI" has been active since 2018 in South Africa. (Marczak, Railton, McKune, Razzak, & Deibert, 2018, p. 15) The operator name "GANGES" has been active since 2017 in India. (Marczak, Railton, McKune, Razzak, & Deibert, 2018, p. 16) Various journalists have been targeted for surveillance in South Africa like Sam Sole, Stephan Hofstatter, Mzilikazi wa Afrika etc. (Stakeholder Report Universal Periodic, 2016, p. 12) They have confirmed that there were interception orders which were granted against them. (Perrigo, 2021)

GROSS VIOLATION OF HUMAN RIGHTS

Modern surveillance differs from conventional surveillance of telecommunications eavesdropping, monitoring, and interception. (Bernal, 2016, p. 246) The growth of social networks, the advancement of behavioural pattern monitoring systems, the rise of (smart) phone usage, and other similar technological advances have paved the way for geolocation and biometric data to become the new surveillance beacons. (Bernal, 2016, p. 247) These monitoring and surveillance tactics are used by both state and non-state entities to acquire private details and threaten journalists. States track the movements of journalists, human rights activists, etc. using spying technologies, frequently in disguise and under the garb of public safety or national security. For instance, The Pegasus Project found evidence of spyware used in planned and effective intrusions of journalists', government officials', and human rights activists' smartphones, which was created and licenced by the Israeli business NSO Group. A prominent journalist, Paranjoy Guha Thakurta's iPhone was verified by Forbidden Stories to be contaminated by "Pegasus", remarked, "I was not in the least surprised that I was targeted." (Perrigo, 2021)

Character assassination and legal proceedings are common tactics used to intimidate, "silence" and destroy investigative reporters who uncover

wrongdoing. (Londoño & Casado, 2020) Glenn Greenwald is an American journalist who has worked significantly to bring the Edward Snowden revelations to the limelight, and there have been attempts to intimidate him. To scare Glenn , intimidation tactics such as the detention of David Miranda, Glenn Greenwald's partner at the London airport, under Schedule 7 of the Terrorism Act of 2000, were used. In addition to not being able to have a legal representative, the officer who made the arrest would only identify himself by his number: 203654. Glenn was also not permitted to speak to David. (Greenwald, 2013) The researchers describes this form of surveillance as "silencing surveillance", which targets a person or a group of individuals in an effort to intimidate or menace them into omitting evidence or acting in a particular way. For example, a journalist named Glenn Greenwald, best known for disseminating stolen papers outlining the NSA's extensive monitoring and surveillance, was a target of criminal proceedings brought by Brazilian prosecutors. (Boadle & Brito, 2020) Stefania Maurizi, an Italian journalist who reported both WikiLeaks and Snowden for the Italian weekly L'Espresso, claims that throughout her investigation of Snowden, she was subjected to intrusive "physical monitoring" while visiting Berlin Park. (Mills, 2019, p. 697)

The idea of surveillance and monitoring in and of itself has fuelled and sparked numerous discourses about violations of human rights over the years. However, the researchers believe that both pro-surveillance and anti-surveillance debates have been sparked by surveillance. The researchers firmly believes that the type of surveillance needed is one that checks off all the criteria, from legally justified processes to legitimate aims in order to prevent crimes or larger concerns. For instance, privacy cannot take precedence over healthcare if data is gathered for healthcare purposes by governments to ensure the covid-19 infection is not rapidly spreading. However, the information gathered must be used for the intended purpose for which it was gathered, and that use must be justified.

Government agencies feel free to install cameras in public areas like roadways, parks, and lanes in order to monitor and track people's behaviour because there is no claim of privacy there. (Balkin, 2008, p. 20) The cameras installed in public spaces will be able to record number plates. This helps to track all the vehicles breaking traffic laws and regulations, automobiles being used as vehicles to carry out crimes, and even suspicious vehicles. (Balkin, 2008, p. 2) There is no doubt that information-driven technologies can be used in very constructive ways, but if they are not handled very carefully, these technological advancements pose very real hazards to inherent dignity, individuality, and privacy, as well as the exercise of rights generally. Article 12 of the Universal Declaration of Human Rights recognises the right to privacy as

a fundamental human right. A number of human rights are impacted by surveillance, most notably the right to privacy, but it can also, in some circumstances, have an impact on rights to equality and non-discrimination. Moreover, other liberties, such as the freedoms of speech and expression or assembly, can be impacted. To determine whether there has been a violation of human rights, Marko Milanovic has suggested a four-step parameter test, which is as follows:

a) Is there any intrusion on an individual's privacy rights?
b) If so, was such intrusion legally justified or in accordance with the procedure established by law?
c) If so, does such a pattern of intrusions have a legitimate aim?
d) If so, were such intrusions proportionate to the legitimate aim? (Milanovic, 2015, p. 133)

The rule of law, independence of Judiciary, consideration for individual liberties, and adherence to democratic governance norms, including accountability and transparency, are all requirements for government who engages in surveillance that are operating in a democratic nation. (Dimich et. al. 2022, p. 447). The necessity to regulate surveillance is one of the most important takeaways to be drawn from Cambridge Analytica, Pegasus, Edward Snowden, and other recent exposures, as all of these have flagrantly violated the right to privacy.

The greatest and most significant issue is that, despite the existence of legislation, no matter how stringent, and well-known verdicts that establish the standards for monitoring and surveillance, such arbitrary spying and "silencing surveillance" take place.

CONCLUSIONS

The debate that commenced years ago is still going robust and revolves around whether the "right to privacy" of an individual should be prioritised before the state's utilitarianism. The Indian, American and South African governments have "valid" concerns about public safety and national security. However, the government must understand that protection must not come at the expense of the fundamental right to privacy or as a matter of fact any other human rights, especially when they are arbitrary. Obtaining access to personal data can be exploited for nefarious and arbitrary reasons under the pretence of national security. There are various instances of such data being used to monitor "targeted" people like journalists and used to "silence" them. In

reality, a targeted monitoring programme in accordance with global human-rights norms may be used to better address security risks like terrorism.

Undoubtedly, individuals' rights to privacy are violated by surveillance. The need for robust privacy safeguards in surveillance regulations is a result of the significant power disparity between states and citizens. States are enacting new legislation to give themselves greater eavesdropping authority. The surveillance authorities contend that in the interest of safeguarding civilians from terrorist attacks and defending the security of the state, public order, and public safety, such expanded monitoring capabilities are indispensable. These ostensibly legitimate reasons for surveillance are then used to eavesdrop on media-related individuals such as reporters, journalists, human rights activists, opposition political parties, and, in some cases, doctors, who are being watched in ways that violate their privacy rights.

The researchers firmly believes that surveillance has assisted the government in addressing many contemporary issues, including sophisticated terrorist tactics used by terrorists and information about COVID-19 infected individuals gathered by a variety of applications that helped to keep the public safe. However, unauthorised and warrantless monitoring by governments and commercial corporations, which has the potential to be abused or utilised for reasons other than those for which it was originally gathered, is the bone of contention.

REFERENCES

AmaBhungane Centre for Investigative Journalism NPC and another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others 2021 (3) SA 246 (CC).

Austin, LM (2015). *'Lawful Illegality: What Snowden Has Taught us About the Legal Infrastructure of the Surveillance State' in Michael Geist (ed.), Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, University of Ottawa Press.

Bajoria, J (2014) 'India's Snooping and Snowden', Human Rights Watch, June 5, viewed 13 October, <https://www.hrw.org/news/2014/06/05/indias-snooping-and-snowden>.

Balkin, JM (2008) 'The Constitution in the National Surveillance State', Minnesota Law Review, Vol. 93, No. 1, pp. 1-25,

<www.minnesotalawreview.org/wp-content/uploads/2019/07/Balkin_MLR.pdf>.

Bentham, Jeremy (1791) *'Panopticon: The Inspection House'*. T Payne.

Bernal, P (2016) 'Data gathering, surveillance and human rights: recasting the debate', Journal of Cyber Policy, vol.1, no. 2, pp. 243-264, viewed 19 November, 2022 <www.tandfonline.com/doi/full/10.1080/23738871.2016.1228990>.

Bernstein v Bester NO 1996 (2) SA 751 (CC).

Boadle, A and Brito, R (2020) 'Brazil prosecutors charge The Intercept's Greenwald with hacking' Reuters, January 21, viewed 19 November 2022 <https://www.reuters.com/article/brazil-corruption-greenwald-idUKL1N29Q0SD>

Buthelezi, MC (2013) 'Let false light (publicity) shine forth in South African law', De Jure, vol. 46, no. 3, pp. 783-797, < http://www.scielo.org.za/pdf/dejure/v46n3/08.pdf>

Coyne, H (2019) 'The Untold Story of Edward Snowden's Impact on the GDPR', Cyber Defense Review, vol. 4, no. 2, pp. 65-79, <https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fall%202019/CDR%20V4N2-Fall%202019_COYNE.pdf?ver=2019-11-15-104104-157>.

Dimich, A. et. al. (2022). 'Collection and Use of Information by Counter-Intelligence in the Context of Human Rights Protection', The Age of Human Rights Journal, No. 18, pp. 445–461, <https://revistaselectronicas.ujaen.es/index.php/TAHRJ/article/view/6779>.

Dobbs v. Jackson Women's Health Organization 142 S. Ct. 2228 (2022).

Duggal, P (2018) *'Cyber Law 3.0: An Exhaustive Section Wise Commentary on The Information Technology Act Along with Rules, Regulations, Policies, Notifications Etc'* 2nd edn. LexisNexis.

Edgar, TH (2017) *'Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA'*. Brookings Institution Press.

Foucault, M (1977) *'Discipline and Punish: The Birth of the Prison'*. Random House Inc.

Franks, MA (2017) 'Democratic Surveillance', Harvard Journal of Law & Technology, vol. 30, no. 2, p. 425-489, <repository.law.miami.edu/fac_articles/473/> accessed 26 September 2022.

Greenwald, G 'Glenn Greenwald: detaining my partner was a failed attempt at intimidation', The Guardian, August 19, viewed 19 November 2022, <

https://www.theguardian.com/commentisfree/2013/aug/18/david-miranda-detained-uk-nsa> .

Greenwald, G and MacAskill, E, (2013) 'NSA Prism program taps in to user data of Apple, Google and others' The Guardian, 7 June, viewed 13 October 2022 <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

Greenwald, G and Saxena, S (2013) 'India among top targets of spying by NSA' The Hindu, 23 September, viewed 13 October 2022, < https://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece>

Hirshleifer, J (1980) 'Privacy: Its Origin, Function, and Future', The Journal of Legal Studies, vol. 9, no. 4, pp. 649-664, https://www.journals.uchicago.edu/doi/abs/10.1086/467659

Human Rights Committee, 'The Right to Privacy in South Africa', 116th Session, 2016, pp. 1-8, viewed 13 October, 2022 <https://privacyinternational.org/sites/default/files/2017-12/HRC_SouthAfrica_0.pdf>.

Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) SCC OnLine SC 996, para 185.

Justice Mavedzenge, A (2020) 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework which Guarantees Proportionality in Communications Surveillance', African Journal of Legal Studies, vol. 12, no. 3, pp. 360-390 <https://rm.coe.int/privacy-v-national-security-in-africa-justice-alfred-mavedzenge-2749-3/1680a1a510>

Kaldani, T& Prokopets, Z (2022) 'Pegasus Sypware and its impact on Human Rights' Council of Europe <https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8>.

Katz v. United States (1967) 389 U.S. 347.

Kaur, N 2018, 'Right to Privacy in the United States of America', The Leaflet, 28 May, viewed 07 October 2022,<https://theleaflet.in/specialissues/right-to-privacy-in-the-united-states-of-america-by-nehmat-kaur/#:~:text=The%20right%20to%20privacy%20with,penumbras'%20of%20the%20Fourteenth%20Amendment>.

Kharak Singh v State of Uttar Pradesh and Ors (1963) AIR 1295, para 17.

Kirchgaessner, S, Lewis, P, Pegg, D, Cutler, S, Lakhani, N and Safi, M, (2021) 'Revealed: leak uncovers global abuse of cyber-surveillance weapon', The Guardian, July 18, viewed 19 November, 2022 <https://www.theguardian.com/world/2021/jul/18/revealed-leak-

uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>.

Konvitz, MR (1966) 'Privacy and the Law: A Philosophical Prelude', Law and Contemporary Problems, vol. 31, no. 2, pp. 272-280, https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3108&context=lcp.

Kramer, I R (1990) 'The Birth of Privacy Law: A Century since Warren and Brandeis ', Catholic University Law Review, vol. 39, no. 3, pp. 703-724, <https://scholarship.law.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1818&context=lawreview>

Kurup, D (2013) 'In the dark about 'India's Prism', The Hindu, June 16, viewed 19 November, 2022, <https://www.thehindu.com/sci-tech/technology/in-the-dark-about-indias-prism/article4817903.ece> .

Kwoka, MB (2015) 'Leaking and Legitimacy', UC Davis Law Review, vol. 48, pp. 1387- 1456, <papers.ssrn.com/sol3/papers.cfm?abstract_id=2494375>.

Locke, J (1947) 'Two Treaties of Government'. Hafner Publishing Company.

Londoño, E and Casado, L(2020) 'Glenn Greenwald Charged With Cybercrimes in Brazil', The New York Times, January 22, viewed 20 November, 2022 < https://www.nytimes.com/2020/01/21/world/americas/glenn-greenwald-brazil-cybercrimes.html>

M P Sharma and Others v. Satish Chandra, District Magistrate & Others (1954) AIR 300.

Manohar Lal Sharma v Union of India, WRIT PETITION (CRL.) NO. 314 OF 2021.

Marczak, B, Railton, JS, McKune, S, Razzak, BA and Deibert, R (2018) 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', Citizen Lab Research, Report No. 113, University of Toronto, September 18 <https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf>

McMullan, T 2015 'What does the panopticon mean in the age of digital surveillance?', The Guardian, 23 July, viewed 02 October 2022 <https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham>.

Milanovic, M (2015) 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', Harvard International Law Journal, Vol. 56, No. 1, pp. 81-146, <www.ilsa.org/Jessup/Jessup16/Batch%202/MilanovicPrivacy.pdf>.

Mills, A (2019) 'Now You See Me – Now You Don't: Journalists' Experiences With Surveillance', Journalism Practise, Vol. 13, No. 6, pp. 690-707, < https://www.tandfonline.com/doi/pdf/10.1080/17512786.2018.1555006 >.

Naithani, P (2021) 'Pegasus and the Law', Economic & Political Weekly, Vol. 56, No. 49, < https://www.epw.in/journal/2021/49/letters/pegasus-and-law.html>.

O'Keeffe v Argus Printing and Publishing Co Ltd., 1954 (3) SA 244 (C).

Olmstead v. United States (1928) 277 U.S. 438.

Parikesit, B & Yudithadewi, D (2020) 'The Impact of Surveillance on Journalist Activism', UNES Journal of Social and Economics Research, Vol. 47, No. 2, pp. 55-63,<https://www.researchgate.net/publication/354778446_The_Impact_of_Surveillance_on_Journalist_Activism>.

People's Union of Civil Liberties (PUCL) & Anr v. Union of India & Anr (1997) 1 SCC 301.

Perrigo, B(2021) 'Governments Used Spyware to Surveil Journalists and Activists. Here's Why Revelations About Pegasus Are Shaking Up the World', Time, July 19, viewed 19 November 2022, <https://time.com/6081433/pegasus-spyware-monitored-journalists-activists/>.

Planned Parenthood v. Casey, (1992) 505 U.S. 833.

R. v. Dyment, (1988) 2 SCR. 417, para 17.

Rajan, N (2021) 'Explained: Pegasus uses 'zero-click attack' spyware; what is this method?', Indian Express, 3 August, viewed 19 November, 2022 < https://indianexpress.com/article/explained/zero-click-attacks-pegasus-spyware-7411302/>

Richards, NM (2013) 'The Dangers of Surveillance', Harvard Law Review, vol. 126, no. 7, pp. 1934- 1965, https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_richards.pdf.

Roberts, T et. al. (2021) 'Surveillance Law in Africa: A review of six countries', Institute of Development Studies < https://iapp.org/media/pdf/resource_center/surveillance_law_in_africa_review_of_six_countries.pdf>

Roe v. Wade, (1973) 410 U.S. 113

Rogers & Eden, (2017) 'The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures', International Journal of Communication, vol. 11, pp. 802-823, <researchgate.net/publication/313768564_The_Snowden_Disclosures_

Technical_Standards_and_the_Making_of_Surveillance_Infrastructures>.

Rozenshtein, AZ (2018) 'Surveillance Intermediaries', Stanford Law Review, vol. 70, no. 1, pp. 99-189, <https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/01/70-Stan.-L.-Rev.-99.pdf>.

Shilliam, R (2022) 'Foundations of International Relations'. Bloomsbury Publishing.

Stakeholder Report Universal Periodic 27th Session: The Right to Privacy in South Africa <https://privacyinternational.org/sites/default/files/2018-04/South%20Africa_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf>.

Stanley v. Georgia, (1969) 394 U.S. 557.

Targowski, A (2021) The Strategies of Informing Technology in the 21st Century. IGI Global.

Tariq, J (2013) 'The NSA's PRISM Program and the New EU Privacy Regulation: Why U.S. Companies with a Presence in the EU could be in Trouble', American University Business Law Review, Vol. 3, No. 2, pp. 371- 389, < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3156725>

Thaorey, P (2019) 'Informational Privacy: Legal Introspection in India'. ILI Law Review. Vol. 2, No. 2, pp. 160-179, https://ili.ac.in/pdf/pt.pdf

The Holy Bible (2013) Genesis 3:7. Intellectual Reserve, Inc.

Wacks, R (2015) 'Privacy: A very Short Introduction'. Oxford University Press. 2nd ed.

Watt, E (2017) 'The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance' 9th International Conference on Cyber Conflict (CyCon), viewed 21 November 2022, <https://ieeexplore.ieee.org/document/8240330/metrics#metrics>.

Wet, PD and Fairweather, A, (2013) 'Spying far worse in South Africa than the US', Mail & Guardian, 14 June, viewed 13 October 2022 <https://mg.co.za/article/2013-06-14-00-spying-far-worse-in-south-africa/>.

Završnik, A & Levičnik, P (2015) 'The Public Perception of Cyber Surveillance Before and After Edward Snowden's Surveillance Revelations', Masaryk University Journal Law Technology, vol. 9, no. 2, pp. 33-58, <journals.muni.cz/mujlt/article/view/2831>

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET