Page 1352 - 1372 **DOI:** *https://doij.org/10.10000/IJLMH.113714*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 5

2022

Countering Terrorism through Communications Surveillance: A Human Rights Perspective

YAGYA BHARADWAJ[1]

ABSTRACT

Terrorism, communications surveillance, and human rights are closely connected with one another in the sense that the presence of terrorism makes the use of communications surveillance somewhat necessary as a tool of countering it, and both of these affect the human rights of the people who are subjected to them.

So, how do we proceed with something that, on the one hand, serves as an important tool for countering terrorism, but on the other, raises questions about upholding the human rights of the mass?

This paper seeks to understand and analyze the system of communications surveillance by States for the purpose of countering terrorism and any other threats to the national peace and security of the country, while also discussing what it means for the rights of the people and to what extent the two can co-exist to achieve a world without terror and politically motivated and premeditated use of violence on large scales around the globe. It further emphasizes on the need for applying the International Principles on the Application of Human Rights to Communications Surveillance, also known as the Necessary and Proportionate Principles.

I. INTRODUCTION

The meaning and scope of almost all socio-political concepts change significantly with time. How the world approaches, discusses, and deals with these is also dynamic as a result. What words like 'terrorism', 'surveillance' and 'human rights' entail has not only widened but their interpretations have also become quite subjective from different points of view.

Before we delve into an elaborate discussion on countering terrorism through communications surveillance, while at the same time, upholding the human rights of people, let us first approach these words separately and understand their meanings.

Terrorism is a form of psychological warfare that seeks to spread fear, mistrust, and helplessness

[1] Author is a Student at Chanakya National Law University, India.

 [ISSN 2581-5369]

among the ordinary citizens of a society[2]. Or, as Bruce Hoffman[3] put it in the Netflix series 'Turning Point: 9/11 and the War on Terror', terrorism can be best defined as violence or the threat of violence designed to achieve fundamental political change.

Those who commit acts of terror seek to terrorize and demand political change that suits their extremist agendas. There are also those who are motivated by highly misinterpreted religious notions and the fear that if they do not do what they do, they will be subjected to it themselves.

Now, surveillance has been a method of countering threats to the national security and peace for a long time. In the modern times, the approach to surveillance extends to that of communication between parties as well. Thus, communications surveillance is the monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communications networks to a group of recipients by a third party[4].

The Office of the High Commissioner for Human Rights (OHCHR) defines human rights as the rights we have simply because we exist as human beings - they are not granted by any state. These universal rights are inherent to us all, regardless of nationality, sex, national or ethnic origin, color, religion, language, or any other status.

Terrorism, communications surveillance, and human rights are closely connected with one another in the sense that the presence of terrorism makes the use of communications surveillance somewhat necessary as a tool of countering it, and both of these affect the human rights of the people who are subjected to them.

So, how do we proceed with something that, on the one hand, serves as an important tool for countering terrorism, but on the other, raises questions about upholding the human rights of the mass?

This paper seeks to understand and analyze the system of communications surveillance by States for the purpose of countering terrorism and any other threats to the national peace and security of the country, while also discussing what it means for the rights of the people and to what extent the two can co-exist to achieve a world without terror and politically motivated and premeditated use of violence on large scales around the globe. It further emphasizes on the need for applying the International Principles on the Application of Human Rights to

[2] Terror on the Internet: Questions and Answers, United States Institute of Peace, https://www.usip.org/publications/terror-internet-questions-and-answers

[3] Bruce Hoffman is Shelby Cullom and Kathryn W. Davis senior fellow for counterterrorism and homeland security at the Council on Foreign Relations.

[4] Communications Surveillance, Privacy International, https://privacyinternational.org/explainer/1309/communications-surveillance

 [ISSN 2581-5369]

Communications Surveillance, also known as the Necessary and Proportionate Principles.

II. TERRORISM IN THE DIGITAL AGE

(A) How have terrorists used the digital world to commit acts of terror?

The use of modern ways of communication has brought the world closer and made it easier to access information and stay connected to each other. But with this ease, the threats posed by the use of modern technologies, especially the internet, have increased and it is frequently used by terrorist groups for their extremist agendas.

Let us look at how terrorists have used communication networks in the past to terrorize and kill innocent people.

It should not be surprising to know that now many terrorist organizations have their own websites through which they not only spread their propaganda, but also keep a lookout for current and potential supporters who could fund them and help them further their propaganda.

The level of threat that terrorist use of internet exposes the society to, was seen in 2001, when the 9/11 attacks wreaked havoc and had the intended impact on the United States and the world alike.

The terrorists used the internet to keep track of flights, buy plane tickets, steal social security numbers, and communicate with each other to coordinate their acts[5]. They also used pre-decided code words to send messages and carry out their plans.

Mohamed Atta, who was the leader of the 9/11 attacks, sent a coded message to 18 other terrorists that read, "*The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering*."

These 'faculties' referred to in the message were, in fact, the targets of attack, like, 'the faculty of urban planning' meant the World Trade Center and ' the faculty of fine arts' meant the Pentagon[6]. So, the use of internet and communication networks is what made 9/11 possible, and as a result, a total of 2,996 people were killed, including the 19 terrorists responsible for it[7]. Another instance where the terrorists used technology to carry out their extremist acts was the 26/11 attacks in Mumbai.

In 2008, there were a series of attacks from November 26 to November 29 at different places in

[5] Terror on the Internet: Questions and Answers, United States Institute of Peace, https://www.usip.org/publications/terror-internet-questions-and-answers

[6] Ibid.

[7] September 11 Attacks, History, https://www.history.com/topics/21st-century/9-11-attacks

 [ISSN 2581-5369]

Mumbai. These attacks were carried out by 10 terrorists, believed to be the members of Lashkar-e-Taiba. Google Earth was used[8] by the conspirators to show them the routes to their targets in the city and an internet phone was set up to route calls through New Jersey in order to disguise the location and divert the attention of the authorities. The terrorists had also made online search for their targets of attack, and used a satellite phone to communicate with the masterminds of the attacks[9].

Thus the terrorists used different communication networks to plan their attacks, mark their targets, and stay in constant touch with each other to carry out their acts in coordination with each other.
Unfortunately, clues related to their plans and the involved members were missed by different intelligence agencies of the world, and because they couldn't be pieced together to get a bigger picture, the attacks could not be prevented, and as a result, about 200 people lost their lives in Mumbai.

On July 22, 2011, Norway witnessed two violent acts of extremism by a far-right domestic terrorist named Anders Breivik. Before his attacks, he posted a 12-minute video on YouTube and sent his 'manifesto' to 1,003 email addresses[10]. The terrorist used the internet (e-Bay) to buy body armour, weapon components, and bomb ingredients. He also used social media for propaganda purposes[11].

Breivik used the web as a primary tool for his acts of terror. He had spent a lot of time online, preparing for his attacks and trying to amplify his extremist ideas.

In September 2013, five bombs exploded at four landmark places in Delhi: Connaught Place, Karol Bagh, Greater Kailash and India Gate. The responsibility for the blasts was claimed by Indian Mujahideen (IM), which is an Islamist terror group. They sent an e-mail to news organizations after the first blast, threatening more blasts, and writing, *"Indian Mujahideen strikes back once more. Within 5 minutes from now... This time with the Message of Death, dreadfully terrorising you for your sins. And thus our promise will be fulfilled. Inshallah...Do whatever you want and stop us if you can[12]."*

[8] James Glanz et al, Big clues missed in 26/11 Mumbai terror attacks, mint, https://www.livemint.com/Politics/fwNUIk5bVvqYUR3BTOTKrO/Deadly-nearmisses-in-spycraft-history-resulted-in-2611.html
[9] Indrajit Basu, Mumbai Terror Attacks Drive India to Tighten Control on Communication Networks, Government Technology (July 27, 2010), https://www.govtech.com/public-safety/mumbai-terror-attacks-drive-india-to.html
[10] National Criminal Investigation Service, Norway (Kripos)
[11] Ibid
[12] Serial Blasts In Delhi, Outlook (September 13, 2008), https://www.outlookindia.com/website/story/serial-blasts-in-delhi/238372

 [ISSN 2581-5369]

Prior to this, there had been blasts in Jaipur and Ahmedabad earlier that year, for which the responsibility was claimed by the IM through e-mails as well, only they had been sent before the blasts.

A week before the Delhi bombings, intelligence agencies had intercepted phone calls between members of IM, but could not calculate the relevance of that phone call, which eventually led to the terror plans of the IM becoming a reality and claiming innocent lives. It was only after the blasts had gone off that the pieces were put together.

Another horrifying incident where extremism was connected to the internet was the 2019 mass shootings in two mosques in Christchurch, New Zealand. Brenton Tarrant, who described himself as an ethno-nationalist and a fascist in his manifesto[13] (The Great Replacement) that he had published online prior to the attacks, opened fire in two different mosques and killed the worshippers there and also some people who were outside . He also live-streamed his first shooting on Facebook, which was then replicated and shared by others on different platforms like YouTube and Twitter[14]. The video and his manifesto were later banned in New Zealand and in Australia (where he was from).

The live-streaming of such a violent act that killed 51 people and the online publication of his hateful manifesto gives an in-depth view of how internet is used for terrorist purposes and for amplifying the hatred that one radicalized person or group has.

There have been numerous other cases where technology and communications channel have been used by terrorists and terror groups to plan their attacks, or communicate with each other, or spread their extremist ideas.

(B) Terrorist use of communication networks

The use of communication networks, primarily the internet, by terrorists encompasses a range of activities to suit their destructive agendas. For countering terrorism through surveillance of communication networks, it must first be understood how and to what extent the terrorists use them for terrorist purposes, because the approach to counter terrorism needs precision and effectiveness.

In the previous section, we acquainted ourselves with some incidences where phones and the internet were used by terrorists to plan their attacks, and spread their propaganda to the mass.

[13] Joey Garrison, 'Violent terrorist': Who is the white supremacist suspected in New Zealand mosque shootings?, USA Today (March 15, 2019), https://www.usatoday.com/story/news/nation/2019/03/15/new-zealand-christchurch-mosque-shootings-who-brenton-tarrant/3172550002/

[14] Jane Wakefield, Christchurch shootings: Social media races to stop attack footage, BBC (March 16, 2019), https://www.bbc.com/news/technology-47583393

 [ISSN 2581-5369]

Such usage can be categorized under broader heads that we identify as purposes for which the terrorists use the communication networks.

1. Propaganda

Terrorist use the internet widely for dissemination of their propaganda. Such propaganda are often in the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of their terrorist activities. These may include virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organizations or sympathizers[15]. Violence is at the center of all that the terrorists seek to achieve through dissemination of their propaganda and internet makes it easy for them to reach a large audience all over the world without having to use other communication methods such as news channels, DVDs, or magazines, which may evaluate the credibility of their content and edit them to remove any provocative elements in them.

The terrorists make heavy use of their propaganda, focusing on both potential and current supporters to further their ideas, and to recruit, radicalize, and incite such supporters, and also to keep their financers updated about the execution of their terrorist attacks[16]. It is a whole system within itself that relies on networking and the ease of access to the internet.

2. Recruitment

One of the objectives for which the terrorists distribute content laced with propaganda is recruitment of individuals who are most responsive to their propaganda into their extremist groups. They seek out the sympathizers and potential recruits and provide them with online spaces and forums where they can learn about terrorist organizations and support them through engagement and involvement in actions that are in furtherance of their terrorist objectives.

These terrorists play to the social positions, sentiments, radical notions, and the feeling of exclusion or humiliation of the people in the society. They observe and factor in everything-from age to gender to economic or social circumstances, and use the vulnerability of the people as a means to manipulate them into joining their terrorist groups[17].

3. Radicalization

Radicalization is usually the step before recruitment. Radicalization refers to the process of an individual or a group adopting radical viewpoint on political, social, or religious matters with

[15] The use of the internet for terrorist purposes, United Nations Office on Drugs and Crime, Vienna (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
[16] Ibid
[17] Ibid

 [ISSN 2581-5369]

motivation to change the status quo. The radicalization of persons or groups fills them with violent and extremist ideologies which suits the agendas of terrorist groups, and for the purpose of which, they distribute their radical propaganda to the faceless mass.

Sometimes when someone who is in the process of being radicalized, or has already been radicalized, is taken through the de-radicalization process, but it is possible only if such persons are identified and contacted.

4. Incitement

It is not uncommon for terrorists to find ways to incite acts of terrorism. Their presence in the digital world is not only for disseminating propaganda, or recruiting potential terrorists, or radicalizing individuals and groups, but also to incite them to commit acts of terrorism.

Article 20 (2) of the International Covenant on Civil and Political Rights states that any advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence shall be prohibited by law[18].

There have been debates on what kind of content constitutes 'incitement'. It has to be distinguished from mere propaganda and basic freedom of expression because inciting violent or extremist acts is a crime and especially when radicalized individuals or groups are encouraged to carry out terror attacks, it becomes imperative to prevent and deter them.

5. Financial Support

Another purpose for which terrorists organizations, as well as their supporters use the internet is financing acts of terrorism. There are four categories under which the terrorist use of the internet to raise and collect funds can be generally placed: direct solicitation, e-commerce, the exploitation of online payment methods, and through charitable organizations. These may involve donations from supporters, distribution of books, audio and video recording to them or using online payment gateways to make it easier for the supports to fund them[19]. Such payment gateways could also be used to divert the money transferred for seemingly innocent purposes to their actual parties having illegal purposes.

As we have also seen in the terrorist attacks where the terrorists received guidance and orders through it, internet is also used by them for training and for planning their attacks. All of these revolve around each other, the whole process of how one is radicalized and recruited, and how

[18] International Covenant on Civil and Political Rights, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[19] The use of the internet for terrorist purposes, United Nations Office on Drugs and Crime, Vienna (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

 [ISSN 2581-5369]

they take active part in carrying out terror attacks.

6. Spying

Just like intelligence agencies use the internet to track and monitor radicalized individuals, potential terrorists, or terrorists, terrorist organizations also make use of the internet for countering the intelligence gathered by them. They use technology to deceive intelligence agencies, to sabotage their operations, and to gather information about security measures and military equipment.

Being aware of the changes made to laws and policies, employment of new security measures and military weapons and technical advancements gives the terrorists ideas on how to evade and disguise their terror plans so that they are not caught.

7. Claiming Responsibility for Attacks

In the last decade, terrorist organizations have taken to the internet to claim responsibility for their attacks. Sometimes they send emails to news organizations claiming responsibility for the recent attacks, like Indian Mujahideen did in 2013 for the serial blasts in Jaipur, Ahmedabad, and Delhi. Sometimes they use their websites, or news channels to claim responsibility, or upload videos of doing the same.

Anders Breivik, before his attacks, uploaded a video on YouTube, and in doing so, along with his admission of the crime, claimed responsibility for the Norway terror attacks that happened in 2011.

Claiming responsibility for terror attacks by uploading videos on the internet or by sending emails before or after the attacks takes one of the worst forms of use of internet for terrorist purposes.

(C) Steganography

Steganography is one of the most modern and dangerous ways in which terrorists use the internet for their extremist agendas. It refers to the art and science of communicating in a way which hides the existence of the communication. It has been observed that terrorist organizations these days have been employing advanced steganography techniques to pass sensitive messages across the web without being detected[20].

There have been many instances of terrorist organizations using steganography to plan and coordinate their attacks, including the 9/11 attacks where the terrorists used a coded message to

[20] Stephanie R. Betancourt, Steganography: A New Age of Terrorism, https://www.giac.org/paper/gsec/3494/steganography-age-terrorism/102620

 [ISSN 2581-5369]

inform the members about the places of attack.

When there are endless things accessible on the internet, in different forms and on different platforms, it is very easy to hide sensitive, or in the case of terrorists, extremist propaganda, or plans of attack etc. among the plethora of content that we find on the internet.

Steganography takes many forms, and even though it proves to be a sound way of sending sensitive information that may concern national security or some private matters, it also provides ease to those with criminal intentions to hide them well under the guise of innocent messages.

III. COUNTERING TERRORISM

The rise of terrorism has led to the international community and State governments employing and initiating new methods of countering it. The global campaign against terrorism, or the War on Terror, as it is called, was led by America as a response to the 9/11 terror attacks in the U.S. As this war continued, it changed the world politics and international relations and cooperation against the threat terrorism poses to the whole world.

Countering terrorism has had a multidimensional impact on social, political, and economic dynamics around the world. Nations and regions have advanced their security measures and strengthened their collective defence to meet the requirements of countering terrorism effectively and efficiently and widen the scope of international cooperation in the fight against terrorism of all kinds.

Terrorism and the methods and measures of counter terrorism have also impacted human rights of people around the world. While the threat of life and liberty that terrorism exposes one to is severe, countering terrorism also comes with its problems, like infringement of privacy and racial profiling. The extent to which they are justifiable is debatable, but it remains true that the existence of terrorism, and as a result, the global campaign against it, have both affected human rights, international relations, and several other aspects of the globe.

The world organizations like the United Nations have taken a number of steps to prevent terrorism and radicalization that leads to individuals and groups joining extremist groups. One such step is the Plan of Action to Prevent Violent Extremism[21]. It is clear that violent extremism and terrorism have become synonymous with each other, as one is conducive to another.

The approach to counter terrorism encompasses preventive, security-based, punitive measures

[21] The United Nations Global Counter-Terrorism Strategy, Seventieth session, General Assembly (December 24, 2015)

 [ISSN 2581-5369]

and collective effort. One such measure is communication surveillance by the State. The next section of the paper focuses on what it is and what it means for human rights.

IV. COMMUNICATIONS SURVEILLANCE BY THE STATE

(A) The scope of surveillance

Surveillance, whether it is targeted or mass, has become an integral part of government strategies. In the past few decades, there has been a shift from surveillance of targeted individuals to that of the general mass. Some States have taken authoritarian approach to it, and others have been relatively liberal, but for whatever purpose, national security, tackling crimes, or political subservience, the scope of surveillance by governments has widened, and questions are constantly raised about its need and its impact on the liberty and privacy of citizens.

It is a fact that surveillance has been an effective for identification, tracking, monitoring, and analyzing data for national security and public order. With criminal minds finding new ways of carrying out their plans and terrorist organizations using more and more radicalized individuals for terrorist activities, it somehow becomes necessary to prevent their plans from taking effect, and if, unfortunately, they have been successful, to track them down and punish them. However, it comes with a price, which the violation of one's privacy. Of course, it can be argued that national interest comes before individual interest, but its extent varies and the purpose behind surveillance is subjective.

Among the various forms of surveillance by the State, one is communications surveillance. The modern world, which relies heavily on technology, has created space for surveillance to be done through communication networks. As this paper focuses on communications surveillance, the scope of our discussion will be limited on only that form of surveillance.

(B) The Rise of Communications Surveillance

The rise of communications surveillance is directly linked with the fear of terrorism in the aftermath of the 9/11 attacks, and the digital revolution[22], which saw a sharp rise in the number of cell phone and internet users.

Suddenly, the war on terrorism was at its peak and thus began a new phase of surveillance, invasions, arrests, etc. Added to the fear caused by 9/11 and the digital revolution, some other conducive factors to the rise in communications surveillance were the decrease in logistical barriers to surveillance, the falling cost of storing and mining large sets of data, and the

[22] Ewen MacAskill, Gabriel Dance, NSA FILES: DECODED- What the revelations mean for you (November 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

provision of personal content through third party service providers[23].

The term 'communications surveillance' encompasses the monitoring, interception, collection, analysis, use, preservation and retention of, interface with, or access to information that includes, reflects, arises from, or is about a person's communications in the past, present, or future[24].

The surveillance through communication networks involves the collection of metadata by governments or law enforcements, which summarizes basic information about the data, helping in categorization and specification of particular data to work with. What makes the gathered information 'metadata' is the content of the communication, for example, the metadata of an email is the content of that email, which can be worked upon and examined.

What makes metadata a vital part of surveillance is the observation of psychological and sociological behavior of the communicators, as causes of terrorism include these two factors, and so the collection of metadata gives government agencies the information they need to identify potential terrorists and terrorist networks[25].

As more and more communications networks are being used by terrorist organizations for terrorist purposes like radicalization, recruitment, incitement, financial support, and planning attacks, the scope of communications surveillance is expanding in order to prevent and curb the threats posed to the society through electronic communication channels. Data collection is done through wiretapping, government Trojans, wiretap Trojans and keyloggers[26].

When talking about surveillance and metadata, the name of Edward Snowden naturally comes up, because his documents revealed numerous things that were previously unknown to the people, and his actions had a worldwide impact and also raised questions on surveillance and privacy issues.

(C) The Snowden Revelations

In 2013, Edward Snowden changed the way the world understood government systems and strategies. Back then, he was a National Security Agency (NSA) employee and a subcontractor for the Central Intelligence Agency (CIA), and because of his gradually developed doubts with the programs he was involved in, he raised his concerns through internal channels, but because

[23] International Principles on the Application of Human Rights to Communications Surveillance, Necessary & Proportionate (May, 2014)
[24] Ibid.
[25] Surveillance and Interception of Communications, Privacy, Investigative Techniques and Intelligence Gathering, UNODC (July, 2018)
[26] Surveillance metadata, WhatIs.com, https://whatis.techtarget.com/definition/surveillance-metadata

of lack of response, eventually revealed information relating to global surveillance programs.

In the many revelations by Snowden, one was PRISM, which is a program that allows officials to collect material including search history, email content, file transfers and live chats of the users of firms like Apple, Google, and Facebook, among others[27]. This undisclosed program came into light through the leaks from NSA, and there was a detailed chart prepared by the NSA which elaborated on the breadth of the data that the PRISM program is able to obtain[28].

There were other classified and controversial disclosures by Snowden that started discussions and debates on numerous matters, created awareness among people about how exactly their data is collected and used, and what measures and tools are used by government agencies in cooperation with telecommunication companies and other governments and agencies for surveillance.

However, as this paper focuses countering terrorism through communications surveillance and analyzing it from a human rights perspective, we will not get into the details about other things that came to the front in the wake of the Snowden revelations.

In 2015, it was reported that the Islamic State of Iraq and the Levant (ISIS) studied revelations from Snowden about how the United States gathers information on militants[29]. According to this report, they used Snowden's documents to evade intelligence authorities, as being aware of how they are being subjected to surveillance helped them hide their footprints, including their online presence.

Thus, the changing face of communications surveillance, its knowledge, the access to the leaked information by Snowden regarding it, have impacted each other.

(D) How Communications Surveillance is used to Counter Terrorism

When the access to communications networks is used by terror groups for terrorist purposes, it becomes a necessity to use those communications networks to prevent and counter acts of terrorism, including radicalization and recruitment of individuals by terror groups, incitement to violence and acts of extremism etc. The digital age has led to a sharp rise in cyber terrorism, a form of cybercrime which involves the use of cyber space by terrorists to carry out terrorist activities. Communications surveillance, as has been discussed, encompasses monitoring,

[27] Glenn Greenwald, Ewen MacAskill, NSA Prism program taps in to user data of Apple, Google and others, The Guardian (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[28] Ibid.
[29] Pamela Engel, ISIS is reportedly using information leaked by Edward Snowden to evade intelligence authorities, The Economic Times (July 22, 2015), https://economictimes.indiatimes.com/news/international/world-news/isis-is-reportedly-using-information-leaked-by-edward-snowden-to-evade-intelligence-authorities/articleshow/48170453.cms

collecting, intercepting, analyzing, using, preserving, and retaining data relating to a person's past, present, or future communications.

Using this, terrorists can be monitored, tracked, their conversations with other terrorists be intercepted, encrypted messages can be decoded and analyzed and so on. Eminent threats can also be protected against by knowing before-hand about planned terror attacks by terrorists.

Sometimes, clues relating to terror attacks are missed by intelligence agencies, or not put together, as had happened in the Mumbai terror attacks in 2008, where the governments failed to realize what was going on and share information with each other[30]. Continuous surveillance and intelligence sharing between governments and international cooperation in this process is vital to prevent terror attacks and associated disasters.

The effectiveness of communications surveillance is sometimes measured by counting the number of thwarted attacks, number of lives saved, number of terrorist organizations destroyed, and the number of criminal cases that drew on intelligence gathered[31]. It is true that if surveillance fails to achieve its objective, which in this case is countering terrorism, then it is ineffective and of very little significance for maintaining peace and security.

In 2013, after the Delhi bombings, even though the failure of intelligence agencies to put together the terror plan from the intercepted call resulted in five blasts in the capital, it was communications surveillance which eventually led the police to Batla House, where the terrorists were residing in a flat[32].

In various other incidences, surveillance of communications networks have helped governments and intelligence agencies in thwarting terror attacks, tracking down terrorists, and gathering intelligence on terror organizations[33].

V. BALANCING COMMUNICATIONS SURVEILLANCE WITH HUMAN RIGHTS

Human rights are inseparable part of an individual's life. These are the basic rights that a person has by the virtue of them being human, and they must be upheld at all times.

The world is moving towards, and adapting to the expanding digital environment.

[30] James Glanz et al, Big clues missed in 26/11 Mumbai terror attacks, mint, https://www.livemint.com/Politics/fwNUIk5bVvqYUR3BTOTKrO/Deadly-nearmisses-in-spycraft-history-resulted-in-2611.html

[31] Michelle Cayford, Wolter Pieters, The effectiveness of surveillance technology: What intelligence officials are saying, Taylor&Francis Online (March 08, 2018)

[32] Arvind Ojha, 7-minute call that led cops to Batla House: A look at the encounter 11 years on, India Today (September 19, 2019), https://www.indiatoday.in/mail-today/story/revisiting-batla-house-11-years-after-encounter-1600634-2019-09-19

[33] Tim Lister, Paul Cruickshank, Intercepted communications called critical in terror investigations, CNN (June 11, 2013)

 [ISSN 2581-5369]

Communications take place through different channels or networks, and the reliance on technology has seen an astronomical increase as a result of Covid-19 pandemic. Thus the protection of human rights becomes important even in the digital environment.

The right to privacy is a fundamental human right. Article 12 of the Universal Declaration of Human Rights states, "No one shall be subjected to arbitrary interference with his (or their, to make it more inclusive) privacy, family, home or correspondence, nor to attacks upon his (their) honour and reputation. Everyone has the right to the protection of law against such interference or attacks." The same has been enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) as well.

Being under surveillance is, undoubtedly, an infringement upon a person's privacy, which is a right recognized by the international human rights law, and ensures the realization of other human rights such as the right to freedom of expression. Privacy also establishes the ability of an individual to determine who holds information about them and how that information is used[34].

In its General Comment No. 16[35] with reference to Article 17 of ICCPR, the Human Rights Committee pointed out that compliance with Article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Further, that surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.

Therefore, while it is imperative that terrorism be combated and its threats minimized, it is equally crucial to make counter terrorism measures consistent with human rights.

In the pursuance of this objective, it must be ensured that communications surveillance is regulated by law, and done only for achieving a legitimate aim and protecting national security, public order, public health or morals and the rights and freedoms of others, and confirms to the principle of proportionality[36], which stands true for both the right to privacy and the freedom of movement.

The freedom and equal status that a human being is born with must not be compromised in the name of peace and security, because peace and security can be maintained only through the

[34] A/HRC/23/40, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Human Rights Council (April 17, 2013)
[35] Human Rights Committee, Adopted on April 8, 1988
[36] Ibid at 33.

 [ISSN 2581-5369]

realization of the fundamental rights of individuals. If the privacy and personal freedom and liberty of people is restricted and tampered with, no individual would be able to call themselves safe and at peace.

VI. INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATIONS SURVEILLANCE

The International Principles on the Application of Human Rights to Communications Surveillance, also called the 'Necessary and Proportionate Principles', or 'the Principles' is a document which attempts to explain how international human rights law applies in the current digital environment, particularly in the light of the increase in and the changes to communications surveillance technologies and techniques[37].

The principles are the outcome of a global consultation with civil society groups, industry, and international experts in Communications Surveillance law, policy, and technology, and seeks to provide the stakeholders with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

The Preamble of the document reaffirms the importance of privacy as a fundamental human right and how it crucial it is for democratic societies. Privacy being essential to human dignity and reinforcing other rights, such as freedom of expression and information, and freedom of association, should not be compromised with unless it is there is an absolute necessity. Even then, measures like Communications Surveillance are justified only when they are prescribed by law, are necessary for achieving a legitimate aim, and are proportionate to the pursued aim[38].

The Necessary and Proportionate Principles enunciate the duties and obligations to be carried out by States when it comes to Communications Surveillance. These principles are-

Principle 1: Legality

According to this principle, any limitation to human rights must be prescribed by law, as has been stated in different General Comments of Human Rights Committee as well. If there is an absence of an existing publicly available legislative act which meets a standard of clarity and precision sufficient for ensuring advance notice and foreseeability of application to individuals,

[37] International Principles on the Application of Human Rights to Communications Surveillance, Necessary & Proportionate (May, 2014)

[38] A/HRC/23/40, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Human Rights Council (April 17, 2013)

the State must not take up a measure that interferes with human rights[39].

Principle 2: Legitimate Aim

The permission of Communications Surveillance should be given by law to specified State authorities only when it's to achieve a legitimate aim in furtherance of some legal interest of utmost importance to a democratic society. The application of such measures should not be discriminatory on the grounds of race, colour, sex, language, religion, political or other opinion, nationality or social position, property, birth or other status[40].

Principle 3: Necessity

The necessity to achieve a legitimate aim should be the only justification for conducting Communications Surveillance, or when in case of multiple means of achieving such an aim, it is the means least likely to infringe upon human rights. The onus of proving such justification always falls on the State[41].

Thus, Communications Surveillance by the State should be done only when a matter of legitimate importance necessitates it, and it's a means of least of a hindrance to human rights.

Principle 4: Adequacy

This principle states that any instance of Communications Surveillance authorized by law must be appropriate for fulfilling the specific legitimate aim[42].

Although, it has been clarified by courts in several states of America that 'adequacy' or 'appropriateness' do not mean that the measures at issue have to be entirely successful, and that measure must not just be logically linked to its objective, but also prove to be effective in its achievement[43].

Principle 5: Proportionality

The intrusion that communications surveillance exposes the society to, infringes with human rights and is a threat to a democracy. Decisions regarding it must consider the data collected and also the severity of the human rights infringement.

This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting communications surveillance for the necessary and legitimate aims:

[39] Principle 1, Necessary and Proportionate Principles
[40] Principle 2, Necessary and Proportionate Principles
[41] Principle 3, Necessary and Proportionate Principles
[42] Principle 4, Necessary and Proportionate Principles
[43] https://www.ohchr.org/documents/issues/privacy/electronicfrontierfoundation.pdf

 [ISSN 2581-5369]

1. There is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out.
2. There is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought.
3. Other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option.
4. Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged.
5. Any excess information collected will not be retained, but instead will be promptly destroyed or returned.
6. Information will be accessed only by the specified authority and used only for the purpose and duration for which authorization was given.
7. That the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms[44].

Principle 6: Competent Judicial Authority

The impartiality and independence of a competent judicial authority is imperative for determining matters related to communications surveillance. Such an authority must be:

a. Separate and independent from the authorities conducting communications surveillance

b. Conversant in related issues and competent in making judicial decisions about the legality of communications surveillance, the technologies used in conducting it, and human rights

c. Having adequate resources in exercising the functions assigned to them[45].

Principle 7: Due Process

The established law requires that States respect and ensure individuals' human rights by ascertaining that lawful procedures governing any interference with human rights are properly set forth, practiced consistently, and available to the general public. An individual, in the furtherance of their fundamental rights, is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except when there is an emergency concerning imminent risk of danger to human life[46].

[44] Principle 5, Necessary and Proportionate Principles
[45] Principle 6, Necessary and Proportionate Principles
[46] Principle 7, Necessary and Proportionate Principles

 [ISSN 2581-5369]

Principle 8: User Notification

This principle states that those whose communications are being surveilled should have the knowledge beforehand that they are going to be under surveillance so that they have enough time to challenge the decision of such surveillance. The person should also have access to the materials presented in support of the application for authorization[47].

Of course, the question comes up, "will the notification not defeat the purpose for which communications surveillance has been authorized?" The answer is, the notification can be delayed in case it would seriously jeopardize the purpose of communications surveillance, or if there is an imminent risk of danger to human life.

The obligation of notifying the individual is primarily upon the State, but the service provider should have the freedom to notify the user of such surveillance, either voluntarily or on request.

Principle 9: Transparency

Transparency is an essential part of a stable democracy. States should be transparent regarding the use and scope of surveillance laws, regulations, activities, powers, or authorities. There should be enough information provided to the individual by the State so that the individual can fully comprehend the nature, scope, and application of laws that permit communications surveillance. States should practice non-interference when it comes to service providers publishing the procedures they apply in the course of assessing and complying with State requests for the surveillance[48].

Principle 10: Public Oversight

Oversight mechanisms should be established by States for ensuring transparency and accountability regarding communications surveillance. Such mechanisms should have the authority to keep a check on the State's activities related to communications surveillance and evaluate the lawfulness and accuracy of the way it works. It has to be ascertained that the Transparency principle is obliged with[49].

Principle 11: Integrity of Communications and Systems

The integrity, security, and privacy of communications systems has to be ensured, as any compromise in the security for State purposes leads to compromise in security in general. So, States should not compel service providers or hardware/software vendors to attach or build any

[47] Principle 8, Necessary and Proportionate Principles
[48] Principle 9, Necessary and Proportionate Principles
[49] Principle 10, Necessary and Proportionate Principles

 [ISSN 2581-5369]

monitoring systems into their products.

The anonymity of individuals is their right, and State should not interfere with or compel identification of users[50].

Principle 12: Safeguards for International Cooperation

With the developments and changes in the way information flows, and how communications technologies and services operate, the need for assistance from foreign service providers and governments grows. In the pursuance of this, Mutual Legal Assistance Treaties (MLATs) and other such agreements are entered into, to ensure that whenever laws of more than one State are applied to Communications Surveillance, then the standard with the higher level of protection of individuals is applied.

The mutual legal assistance processes and agreements should be well-documented, publicly available, and subject to guarantees of procedural fairness[51].

Principle 13: Safeguard Against Illegitimate Access and Right To Effective Remedy

Legislations should be enacted to criminalize illegal communications surveillance by both public and private actors. There should be effective civil and criminal penalties, protection for whistleblowers, and redressal mechanism for those whose rights have been violated.

Any information gathered in a manner inconsistent with these principles should be inadmissible as evidence, and should not be considered in any proceedings. Further, laws should provide that no information obtained from communications surveillance, after it has been used for the purpose for which it was so obtained, is retained. All such information should either be destroyed or returned to those affected[52].

These principles have been adopted globally by more than 400 organizations. Even though some changed had to be made in the language of the document for translation purposes, the intention and impact of the principles have remained the same. They have ensured the basis and framework of how communications surveillance, if they must be done, will work so as to uphold human rights and not interfere with the privacy, freedom, or liberty of individuals.

VII. CONCLUSIONS AND RECOMMENDATIONS

The digital revolution came with its boon and bane. Its expansion brought unprecedented opportunities, as well as threats. Advancements in technology has given us ease in access to

[50] Principle 11, Necessary and Proportionate Principles
[51] Principle 12, Necessary and Proportionate Principles
[52] Principle 13, Necessary and Proportionate Principles

 [ISSN 2581-5369]

information, communication, opportunities etc. and the world has witnessed a gradual but revolutionary shift in how communications techniques and technologies work. This has led to a change in how terrorists use these for their terrorist purposes, and how States conduct communications surveillance as a means to combat terrorism. But such surveillance comes with its questionable aspects regarding human rights, and therefore, it is important that States keep themselves updated with the dynamics and regulations of communications surveillance so as to respect and protect the human rights of individuals.

As pertinent as communications surveillance can be in combating terrorism and maintaining peace and security, it may be equally intrusive to a person's privacy and freedom. States need to ensure that individuals' rights are protected, as the infringement of one right means that another right cannot be exercised in its entirety. Countering terrorism does require some extreme measures like communications surveillance, as it has proved to be effective in thwarting terrorist attacks, or monitoring and tracking terrorists, or discovering radicalized individuals, but States should do so only when it is prescribed by law, is out of necessity, is for a legitimate aim, and is proportional to the threat or crime that has given effect to it.

A democratic society requires transparency and accountability to work in the long run. The need for the State to be transparent about the use of communications surveillance and give the public access to information so that they can comprehend and understand how it works with respect to the applicable laws and the techniques involved, is crucial for ensuring that the above mentioned elements of a democracy is upheld. States should have oversight mechanisms for this purpose.

One way of gaining public trust when it comes to communications surveillance is to inform the public about how communications networks are used by terrorists and to what extent, so that the need for communications surveillance can be understood, and individuals may come to terms with the fact that under necessary and legitimate circumstances, intrusion into their privacy could help protect lives of many and maintain security.

At the same time, States should devise a strong legal framework for regulating communications surveillance and criminalize the illegal surveillance by private or public actors.

Terrorists are sometimes discreet, and sometimes not-so-discreet in their use of technology for disseminating their propaganda. They use it for a range of things, like radicalization, recruitment, claiming responsibilities for terror attacks etc. It's only when we get into the depth of how intricate their plans are that we may be able to counter them. All of us, as world citizens, have a responsibility of not letting crime and destruction consume our security and peace. Countering terrorism is primarily the duty of the State, however, an individual, in their own

 [ISSN 2581-5369]

capacity, should be aware and alert and not fall into traps set by terrorists using social media platforms or the internet or technology in general.

In the pursuance of the goal of maintaining peace and security and countering terrorism, States must take necessary measures, because there is the question of the greater good involved, but respecting and protecting the human rights of individuals should be a priority, because ultimately, it is the people of the nation that States seek to protect through measures like communications surveillance.

*****

 [ISSN 2581-5369]