GLOBAL ACADEMIC RESEARCH INSTITUTE

COLOMBO, SRI LANKA

GARI International Journal of Multidisciplinary Research

ISSN 2659-2193

Volume: 06 | Issue: 07

On 31st December 2020

http://www.research.lk

Author: Maathumai Paranthaman

UN, Sri Lanka

GARI Publisher | Human Rights | Volume: 06 | Issue: 07

Article ID: IN/GARI/ICSSH/2020/124 | Pages: 36-49 (14)

ISSN 2659-2193 | Edit: GARI Editorial Team

Received: 07.10.2020 | Publish: 31.12.2020

PRIVACY AND PANDEMIC: AN ANALYSIS ON DIGITAL RIGHTS VIOLATIONS DURING RECENT COVID 19 OUTBREAK

Maathumai Paranthaman

Program Support Officer (OHCHR, United Nations, Sri Lanka)

ABSTRACT

The topic has been chosen as it talks about some of the issues that are ignored or mistakenly forgotten during the ongoing Pandemic. The recent COVID pandemic started in later 2019 and rapidly became global phenomenon within a shorter-period of time. With deaths and economic depressions, the human rights are at stake with the increase of government restrictions and strict health measures. Right to life, right to access for a standard health care, freedom of expression and freedom of movement. Although the human rights activists and various civil society organizations are pressing the human rights violations happening in the pandemic, very few mentions about the human rights violations happening in the digital platforms. This research paper intends to pen down some of the key issues found in the digital rights and their silent violations during the time of pandemic. It is important to note that digital rights violations should be given equal priority as other human rights. Along with the spread of virus, bio surveillance and online tracking censorships are being taken as safety measures to control the spread of the virus, which are silently violating the digital rights. The research paper will focus on both international aspects as well as Sri Lankan aspects. The differences will be compared and analyzed with a focus on future developments that can be made in the digital rights area. In the conclusion part, the research paper will talk about the own view points of the author that should be given priority in the future in the area of digital rights violations and remedies with presenting recommendations and suggestions.

Keywords: Covid 19, digital rights, human rights

INTRODUCTION

The topic has been chosen as it talks about some of the issues that are ignored or mistakenly forgotten during the ongoing pandemic. The recent COVID pandemic started in later 2019 and rapidly became a global phenomenon within a shorter-period of time. With deaths and economic depressions, the human rights are at stake with the increase of government restrictions and strict health measures. Right to life, right to access for a standard health care, freedom of expression and freedom of movement are at stake. Although the human rights activists and various civil society organizations are pressing the human rights violations happening in the pandemic, very few mentions about the human rights violations happening in the digital platforms. This research paper intends to pen down some of the key issues found in the digital rights and their silent violations during the time of pandemic. It is important to note that digital rights violations should be given equal priority as other human rights. Along with the spread of virus, bio surveillance and online tracking censorships are being taken as safety measures to control the spread of

the virus, which are silently violating the digital rights.

Most of the times, the government fail to comply with the international human rights law and practices while introducing new restrictions or laws in order to control the diseases. The laws born out of no legal oversight often result human rights violations and with the limited knowledge and less awareness and thus human rights in digital platforms are in danger. Transparency and regulations are expected from state authorities before introducing new laws. Unfortunately, the COVID 19 situation makes it impossible to have a balanced appropriate and proportionate legal framework and it is essential to talk about slowly eroding human rights in the digital space. After the Cambridge Analytica scandal, the view from the common public towards the big data and tech companies are changed and the anti-trust is very much infringed within the mindset as of the pandemic digitalised our lifestyle thorough online shopping, zoom meetings and various online activities.

Since the realization of that the manual tracing is pointless and requires lot of resources and time, the world adopted to digital tracing so quickly and applications started controlling the day-to-day life. There are two sides of digital solutions. One is saving lives, creating health alerts and increasing physical check-ups. The other side is surveillances are tracing individual's locations and violating data protection rights, freedom of movement and freedom of information. The authorities have the responsibility to focus on the second side of digital solutions as it degrades the trust in public authorities and undermine the effectiveness of state's public health responses. The term "bio surveillance" denotes tracking and tracing people's movement and their health condition and keep a data of them. This is done by government or government aided private companies. The monitoring ways might include the phone data, CCTV footage, temperature checkpoints, airline, railway and other public transportation system checks, credit card payments, records of online shopping, information shared in the social media, facial recognitions and drones. The private companies might exploit the data they have for profit or any other reasons. If those data are disclosed, even the citizens will be able to trace and track down others' sensitive medical information. The World Health Organization suggests that the COVID 19 existence will take at least two years to be fully eliminated and with that fact there are some unanswered questions like "how long will this data be kept and how far it is secure enough?".

The research paper is going to be a theory – based analysis using secondary data. The essay will be sourced with scholarly articles, journals, news, interviews given by the experts in the field, documents and at the same time existing international and national statutory provisions such as treaties, declarations, documents, resolutions passed by United Nations General Assembly on digital rights, and the directives on safe mechanisms during pandemic and the situations of noticeable digital rights violations happened.

In this research paper, the cases and examples from different countries will be used to analyze the violations at the same time the case examples of the governments that have successfully overcome the digital dilemma and virus will be examined to provide solutions and recommendations for the problems identified during the research period. Further the research will address the digital divide between the computer literate society and the illiterate community and how does this divide challenge to overcome the barriers of digital rights awareness among common people. Since the world is slowly adjusting to new normal, online education and distance learning have become vital and

the question whether the students from all backgrounds are accessed to Internet facilities is not very stressed. In 2010 the easy access to internet was announced as a human right and it is an immediate need that governments should provide necessary internet and education facilities to study from home.

By enacting strong data privacy protection laws, creating an open and transparent dialogue between civic society and relevant authorities, using existing data protection laws as legal mechanisms to prevent digital rights violations, building trust among communities by disclosing the reasons behind receiving personal data and incorporating various CSOs and NGOs to monitor the digital rights violations, the cyber space can be protected especially in the times of pandemic. (Anglim, 2016) The research will focus on both international aspects as well as Sri Lankan aspects. The differences will be compared and analyzed with a focus on future developments that can be made in the digital rights area. In the conclusion part, the research paper will talk about the own view points of the author that should be given priority in the future in the area of digital rights violations and remedies with presenting recommendations and suggestions.

ANALYSIS

Privacy can be defined as "the desire of people to freely under what circumstances and to what extent they will expose themselves, their attitudes and their behavior to others". If a modern state becomes electronically active and if the Right to Privacy is infringed under the name of Digital Government, it should be dealt under the Supreme Court. That paramount importance can be given to right to privacy only if it is included in Fundamental Rights. (Richardson, 2020)

The digitalization caused by the pandemic created opportunities for increased social engineering attacks such as fraud, phishing, extortion, ransomware attacks on critical operation systems and various kinds of cyber-attacks on governments, companies and media units. The statistics suggests that after the pandemic phishing has been increased about 300% especially in the vulnerable environment where digital platforms are not very secured. After Covid-19, millions of malware emails related to the disease and health instructions and spam messages swamp in social media. By clicking them, the people and their details become visible to the anonymous hackers around the world and this makes the online platforms even more dangerous to use. (Meaker, 2020)

The ODL (Open Distance Learning) has become common in the pandemic lifestyle. In 2010, having access to internet was declared as human right, and still in the least developing countries, the right is not enjoyed by everyone. The online learning challenges the educational rights of the children at the same time creates a digital divide between those who have access to digital learning tools and those who are not. Further, the new methods of teaching through online has alarmingly increased the online abuse of children and the exploitation, says the United States National Centre for Missing and Exploited Children. (Article 19 , 2020)

The first and foremost solution to tackle down the challenges on privacy rights is to have a committed international collaboration. This means bringing vulnerable populations (digitally illiterate people who needs to be educated about the actual problems) and the multi- stake holders together for an action -oriented capacity building programs. The programs should reach cross border population so that a struggling nation can gain knowledge from successful cases. The Covid 19 pandemic is deeply monitored by the governments, international organizations such as WHO, various non-

governmental organizations and numerous health institutions. However, the question is whether this monitoring and evaluation are conducted in cyber space are reliable. While speaking about privacy issues on digital grounds it should be focused from cyber landscape. (Meyer, 2020)

Unfortunately, the outbreak and consequences started a most dangerous phenomena called unprecedented information flow in other words fake news. Campaigns and law enforcement activities should be introduced to increase awareness. Also, it is expected that just like the information sharing and reporting systems about the viruses and health guidelines, it is crucial to share the information regarding privacy rights and the methods to safeguard from unwanted violations. To achieve a successful output the government and the private sector cooperation is vital and inevitable. (Daskel, 2020). Right to privacy is very much connected with right to be left alone. The main scope behind the concept of right to be left alone is that the "certain zone of individual behavior and interpersonal relations should be left alone". The pandemic imposes many challenges to this right such as closure of national borders, restrictions of traffic, enforced remaining at home under threats and closure of public centers. One of the examples where these newly introduced measures on closures conflict with the existing statutory provision is the violation of Article 8(2) of the European Convention on Human Rights by the European Union Border closures. Freedom of movement is directly and indirectly connected with right to privacy as well. (United Nations Human Rights, 2020)

Apart from the border closures and restrictions on travel, most countries introduce some digital strategies to trace and tract contacts in order to prevent the spreading of virus. Although they are justified under national health, the ethics and admissibility of these measures are still questionable. China introduced facial recognition for contact tracing which cannot be categorized as ethical since the identity of the infected can be circulated. Israel and Iran use mobile phones to track and trace and detect the citizen's movements. Their approach is also criticized by human rights defenders since this technology is used to monitor the obedience practiced by the citizens in the quarantine centers. (Fund, 2020)

The people employed at the private companies are more vulnerable towards the privacy related problems. The companies and organizations are in a position to make digital platform secure but also forward looking. As the pandemic is continuing, the sectors need to come with accurate and transparent rules and regulations to share the personal data of the employees. The Personally Identifiable Information (PII) are the main personal details of the employees often asked by the Government to trace contacts. Some companies are expected to reveal some travel details of their clients, airline details, car service and insurance providers to track the time and location of purchases, the movement of that certain person and his/her activities for a period. Also, an individual's geo location data can also be obtained from cookies, pixels and other apps without knowingly. These are some of the violations of right to privacy. (Electronic Frontier Organization , 2020)

Thus, this is the perfect time for companies to review the regulations and privacy policies to disclose the Personally Identifiable Information to government agencies upon the requests justified under emergency purposes or public health priorities. The companies should educate their employees and they revise their framework of privacy policies. The framework shall incorporate the following mandatory questions: how a disclosure should happen, what are the standards that must be practiced throughout the

disclosure procedure, what are the post-release steps, the applicability of any data protection law, the sufficiency of the data collection, who is the recipient and finally if the recipient is not government but other nexus (other customers/ organizations) is it advisable to reveal the minimal PII. (Council of Europe , 2020)Apart from the above considerations, it is also equally important to reveal minimal information so that the impact on individual privacy rights will be less.

The European Union Freedom of Information Actions (FOIA) presented some considerations for private companies which are requested to submit the PII of their employees. First consideration is from where is the request coming from and what is it about? FOIA strongly advises to limit the relevant data to geolocation, travel data and person to person contact if the requesting party is unknown. The companies bear the ethical responsibility to analyze the legal consideration/legal obligation behind the inquiry. They must ask the government on what legal basis the information is needed (Eg: order, warrant or subpoena). The companies are advised to transparent about their privacy polices so that the clients can rely on them and to avoid any anti-trust issues.

Work from home becomes the new normal and so does the cyber threats relate to it. When companies encourage the employees to work from home, there is a possibility that increased migration of organization data to personal devices, paving a way to cyber hack without strong cyber protection. The people at risk at this juncture are the remote working inexperienced employees. The experts have set considerations to face this challenge as well such as providing infrastructure support, setting up requirements and drafting policies, training the employees about the dangers in connecting the unsecured networks, auditing, only using trusted sources, not providing security, personal, financial information when responding to online communication and not clicking on links or opening attachments contained unsolicited information.

Tracing without violating the privacy is possible if the developed applications focus mainly on privacy and security. North Macedonia practically made this possible by developing an app called Stopkorona which is ensured with maximum degree of privacy protection through allowing consent of data subject, anonymization, minimization, decentralization and time bound. The app uses a strategy of storing the data on the user's phone and the data is shared with health authorities only when the person is diagnosed with the disease. Nevertheless, this is not the case in other countries. In most states, authorities are collaborating with telecommunication service providers. In Turkey and Kirgizstan, a GPS based centralized app is used to trace the victims and contacts. Armenian legislature passed a new law permitting operators and medical personnel to share citizen's personal data, location and contacts to authorities. Montenegro government took an easier route by regularly publishing names and addresses of quarantined citizens on its official website.

The legality of the usage of surveillances to track down Covid-19 spread is vastly debated across the world and this is one of the main grounds where right to health and other human rights are conflicted. The experts define a certain criterion that the surveillance measures need to meet. The criteria include necessity of the surveillance measures (public health during epidemics or pandemics), proportionate, time bound, implementation among public with transparency and adequate oversight. The proportionality of the surveillance can be determined by asking two questions: What is done with the bulk data and who have access to it. The reasonableness is vested upon the disclosure of the answers to these

questions however after 9/11 the limitations are not being strictly followed. This led to other phenomena of judicial intervention in digital surveillance. In several states, data – sharing regimes have struck down by judicial review.

Requiring consent is an immediate ethical standard before starting a health surveillance. It would give a clarity to public at the same time create an awareness. In the post-privacy environment, the health surveillance data including heart rate, diet, hours of sleep along with location, rate of speed, altitude and mode of transport are collected through applications in other words, by combing the above-mentioned data, anyone could create a medical profile of a certain person. The Covid 19 outbreak also created a dilemma between data sovereignty and health surveillance. Example is that Centre for Disease Control created a "public health data surveillance and analytical infrastructure". Experts also argue why surveillance is not perfecting presenting following reasons such as installation of the particular app, notification to the authorities if they are diagnosed to Covid or exposed to any infected persons and finally allowing the discovery of personal data of an individual.

The case Handyside v UK and Klass v Germany reflected the interpretation of "legitimate aim" behind the digital surveillance. It must be justiciable under funding for terrorism, national security or preventing crimes. The cases further stated that if the legitimate aim is found the governments are permitted to have a quiet and intrusive surveillance but again the onus is on the state to prove that the surveillance was necessary and proportionate. Yet mass/bulk surveillance may be arbitrary as nowadays "Just in case" surveillances are done using telecommunication companies, Internet Service Providers and these are neither necessary or proportionate. As per the Guiding Principles on Business and HR published by Human Rights Council in 2011, if the company that conducts the digital surveillance shares the date or the user information to State that should fall under the violation of international law. Therefore, the Internet Service Providers and Other companies should adopt policies that respect human rights and the users must have the transparency of how the data are being gathered, stored and used. On the whole it could be summed up as lack of national legislation, weak procedural safeguards and ineffective oversight result the absence of accountability for arbitrary or unlawful interreference in the right to privacy.

Another example of the infringement right to privacy in Covid 19 time is using personal location data to track the infected and their contacts. The "cell phone tracking technologies" are used in Austria, Belgium, Italy, UK and Germany to observe the people's movements. This approaches not only violate the fundamental freedom of movements but also put right to privacy in jeopardy. This humanitarian crisis expects humanized empathy and support from governments and other relevant authorities especially in quarantine process. Ecuador authorized Geographical Positioning System tracking to observe quarantine and Israel authorized to use cell phone data to track infected persons through SMS alerts and warnings. South Korea in extreme level practices sending details about the infected persons through a hyperlink that takes to the detailed data about the location and the movements of the infected person. This is considered as the serious breach of medical privacy. Furthermore, revealing the details of the infected person would lead to a discrimination and virtual isolation as the disease imposes serious threats to livelihoods and people's mindsets. Apart from that most of the infected individuals are identified as patients of already existing respiratory

abnormalities and medical conditions and sharing their medical information would create more discrimination and panic than empathy.

As per the General Comment No 16 for the UNGA Resolution 68/167 by Human Rights Council the Right to Privacy shall promise the integrity and confidentiality of correspondence to be guaranteed de jure and de facto. Further the correspondence should be delivered to the addressee without interception being opened or otherwise read. At this juncture it is important to note the jurisdiction of European Court of Justice on Meta Data which follows as "the reality of big data is that once the data is collected it can be very difficult to keep anonymous" . A Metadata is used to know individual's behavior, social relationship, private, preferences beyond their identity. It is "taken as a whole may allow very precise conclusions to draw concerning the private lives of the persons whose data has been retained". Therefore, the highly controversial "Meta Data" in alliance with Artificial Intelligence are now used by the authoritarian governments under the justification of public health. China uses smart thermal scanners and facial recognition apps to find the travel of the virus and the famous Alibaba app shares the information with the government. The government of Poland demands it's citizens to upload selfies in the apps to make facial recognition easier. The necessity and proportionality of the technologies are dubious and the fear of how long the government is going to keep this information creates tensions among the human rights defenders and communities.

Another trend that deeply affects the privacy is governments partnering with private surveillance companies to monitor the situation. The collaboration of United States Authorities with Clearview AI and Palantir and Israeli surveillance company NSO selling data analysis to governments to map the people's location are some of examples. However, the clients should be notified transparently about the necessity of the privacy policies and how they contribute to slow down the pandemic.

Anonymized smartphone data are also frequently made advantage after Covid 19 and it is worthy to look at the point of view of Electronic Frontier Foundation as follows "many would invade our privacy, deter our free speech, and desperately burden vulnerable groups of persons…… governments must show such powers would actually be effective , science - based necessary and proportionate…".

Several countries could be studied as case studies of how anonymized smartphone data are implemented. In Hongkong people arrive from overseas should wear a tracker even if they are not infected. Singapore government recruit digital detectives to monitor those who are in quarantine. Israeli security agency Shin Bet has begun using advanced technology and telecom data to track civilians. Although these highly advanced technological measures contribute to prevent the extreme outbreak of the disease within society, on the other side the rights to privacy and right to be left alone should not be sacrificed.

Michael Abramowitz, the president of Freedom House says that "China enhancing censorship .. suppresses independent speech, increase surveillance, restrict fundamental rights… is not a healthy advisory to deal with the pandemic". Darrell West from Brookings Institution points out that "the post 9/11 tools will continue as normal even after pandemic and they are definitely going to clash with people's feelings and privacy.

With a considerable amount of digital literate population within the state and the vulnerable conditions of breaching the technology barricades to obtain one's personal information, it is important to consider the inclusion of right to privacy into the list of Fundamental Rights

protected by Sri Lankan Constitution because "a public value of privacy derives not only from its protection of the individual as an individual but also from its usefulness as a restraint on government or on the use of power." (Daniel J. Solove, 2018)

Article 17 and Article 126(1) of the Constitution suggest that if any infringements of fundamental rights by administrative and executive levels, the applications can be sent to Supreme Court of Sri Lanka. However, without provision that explicitly protects the right to privacy, the above Articles have no part in judicial activism. As a country which witnessed three decades of internal civil war and the latest Easter Sunday attacks, Sri Lanka has numerous examples where the national security or public order were given prominence over privacy concerns.

However, in 1997 and 2000 the proposed versions of draft constitutions considered right to privacy and family life as fundamental rights. The proposed 1997 October Constitution stated "Every person has the right to have his/her private and family life, home correspondence and communications respected and shall not be subjected to unlawful attacks on his/her honor and reputation" in its Article 14(1). The Article 14(1)(e) of the latest proposed constitution of August 2000 provided "the freedom, either by himself or in association with others, and either in public or in private, to manifest his religion or belief in worship, observance, practice or teaching". Now neither proposed draft constitution talked about right to privacy or right to privacy in the digital world in an explicit way. Nevertheless, they gave a sufficient rationale to Supreme Court to "employ constitutional doctrinal canons to interpret and carve out the privacy right in other relevant circumstances".

Privacy and Human Rights 2001: An International Survey of Privacy Laws and Developments published by the Electronic Privacy Information Centre, Washington DC, USA introduces the three approaches of privacy: Privacy as an expression, Privacy as a movement, and Privacy as an aspect of quality of life. (International, 1 September 2001)

Privacy as an expression - Approach 1

Privacy consists of four aspects: information, communication, bodily privacy and territorial privacy. This approach is built upon the arguments based on the fact that freedom of speech and expression cover the right to privacy. In online world, when we are asked to create an account by providing some personal details (Full Name, Email Address or Phone Number, a user name and a password) to get access into a website. This could be explained that the ownership of the website wants its users to create a strong password that cannot be exploited by hackers because hacking itself an infringement of right to expression of the website. Therefore, the automated command of asking some personal details from the website users is justified under the above ground.

Privacy as a Movement – Approach 2

It is very much connected with territorial privacy which may include a safe haven in an undisturbed habitat or freedom of movement without being threatened or followed. In Sri Lankan constitutional context, the rights related to territorial privacy interlinked with Article 14(1) that guarantees "freedom of movement, and of choosing his residence in Sri Lanka".

The overlapping nature of freedom of movement and right to privacy can be further elaborated through these extracts of the judgements of the following cases:

Justice Douglas in Apthekar v Secretary of State:

"The freedom of movement is the very essence of a free society, setting us apart. Like the right to assembly and the right to association, it often makes all other rights

meaningful – knowing, studying, arguing, explaining, conversation, observation and even thinking. Once the right to travel is curtailed, all other rights suffer just as when curfew or home detention is placed on a person" (Aptheker v. Secretary of State, 1964)

Justice Subba Rao in the case of KharakSingh :

"Where he can do whatever he likes, speak to whomsoever he wants, meet people of his choice without any apprehension, subject of course to law of social control… …If a man is shadowed, his movement is constricted, He can move physically, but it can only be a movement of an automation" (Kharak Singh v State of Uttar Pradesh , 1962). If the freedom of movement is violated through using new digitalized tools such as surveillance cameras and bugs, then it would eventually uncover the privacy as well. Parallel to the online world free movement gets the dimension as surfing or access to internet and it is imbedded by cookies, spyware or web bugs which is also considered as an interference of territorial privacy.

Right to Privacy as an aspect of the quality of life: Approach 3

According to the purposive approach of interpretation of statutes, the constitutional interpretations by Judiciary of Sri Lanka safeguard the "right to life" which is not included in the Fundamental Rights Chapter. The right to life means the right to quality of life that includes free and fearless life with affordable price. The lack of privacy protection would definitely question the quality of life. Apart from the above approaches, Privacy can be viewed as autonomy or the right to be left alone. This theory was first introduced by Samuel Warren and Louis Brandeis who further stated a legal right to privacy is to protect one's "inviolate personality" from intrusion. Initially before the swamp of digital devices this was only used in legal context of constitutionalism and Bill of Rights as a protection from government intrusion in one's personal affairs. Nowadays the right to be left alone is extended to unwarranted intrusions by not only governments but also private parties, corporate even into common law tort claims. The test relies on the matrix that whether the victim expected a reasonable privacy and the other party or the state entity infringed it without a proper justification.

"Informational Privacy" the newly developed branch of privacy law covers personal information. The danger of the violation of informational privacy is it can happen without the knowledge of the victim or even after the identification of such violation, the grieved party cannot trace back to the offenders sometimes since the information is easily separable from physical privacy and if the information is too intimate to the victim, that is the clear-cut violation of right to be left alone. Some may ask why not privacy torts in common law deal with the informational privacy do and the reason is common law torts are admissible only if the information is gained from the victim directly or by a third person. The insufficiencies left by the common law and the traditional constitutional law are another reason why most of the Data Privacy Legislation drafts fail at the initial stage. (Lin, 2002) That is why the United States Federal Governments introduced Fair Information Practices (FIPs) in their Data Privacy Laws to regulate the information gained from the general public and the FIPs also set exceptions for "routine use" - the notion came into practice after the Freedom of Information Act.

The last generation saw "industrial revolution" as a socio, economic, cultural turning factor and now "digital revolution" is happening on a scale matching or exceeding than industrial revolution. Jerry Berman and Deirdre Mulligan coin three major digital

developments that affect privacy root level: 1) data creation advancements and collecting vast amount of personal data in every modern interaction, 2) data market is very much globalized and anyone can examine it, and 3) lack of control mechanism to protect analog data. The "modern interactions" mentioned above include interactions with the internet, credit card transactions, bank withdrawal, magazine subscription etc. There are no records on paper about these transactions and they can be instantly sent around the global. The buyers use the information to collate and manipulate for their marketing, even for sinister purposes. With these changes not only affects privacy but also autonomy is also affected. When every single activity leaves a digital trail, government and private monitoring sectors care less about analog surveillance since it creates more "data mining". (Cody, 1999)

As of the introduction of new technologies in the digital market day by day, the privacy protection legislations are expected to adopt themselves as well. They should be amended and modified according to the newly emerging digital threats. The privacy battles are not going to end; thus, the privacy evolutions do not just need a framework but a very strong conceptual and legal stand. If we look into the privacy battles, we can understand how the metaphor "Big Brother" pointed by George Orwell comes relevant. The metaphor refers to the "ever-searching, omnipresent eye of government that has dominated the metaphoric landscape of the modern privacy debate". Obviously, the government's surveillance has created many laments among public in regards to "right to be left alone". (Solove, 2001)

The crime has reached the high tech and criminal investigation needs new tools. Since most of the crimes are digitalized, it is important for the Criminal Investigation Department of Sri Lanka should come up with new tools of digital technology. Unfortunately, the EU General Regulations on Data Privacy Protection do not suggest such strategies. The digital monitoring software called "Carnivore" developed by Federal Bureau of Investigation of the United States could be adopted into South Asian states as well. Internet Service Providers (ISPs) have the millions of customers and vast amounts of personal information and software like "Carnivores" can filter, scan, trace and tap the ISPs in short period of time. With the awake of Islamophobic terrorism after Easter Sunday Attacks, it is vital to that the right to privacy shall be protected by not only by legislation but also given a prominence in national security agenda. (Cohen, 2000)

To understand the depth of infringement of right to privacy and its long terms affects, it is needed to have a clear look on types of information that are circulated without the knowledge of the givers. Financial Information is often seemed as a digital gold for banks and other financial institutions. Data like customer names, addresses, social security numbers, income bracket and credit card status are valuable to marketers and other parties. As of current legal standards does not exceed to an individual's "reasonable expectation of privacy", the statutory regulations do not apply to financial institutions to gather the above data. This is dangerous when it comes to "transferring and re-using personal information that result misuse" (Privacy Rights in the Digital Age , May 2019).

The other information type is the public records documenting the ongoing affairs of the government, state-sectors and even individuals. These include birth certificate, immunization records, school loans and scholarships, driving records, marriage certificates, divorce proceedings, bankruptcy filings and social security benefits. Further if the individual was involved in any direct court or criminal proceedings, that records can also be

easily received. The open government system has become a night mare for privacy defenders. In the analog era public records were, however maintained in a save system difficult to locate. The digital age changed the rubric where every public record is connected to /internet, especially with the e-Sri Lanka Project, they are now easily accessible.

The sensitive type of information is medical information. The digital technology can save money and time and life by instantly sending the medical information between hospitals or doctors, also can heighten the possibility of mistake and misuse. Having the world known about the individual's health conditions, diseases and other information would be an embarrassing. (Winnick, 1994) Medical Privacy problems have two example effects: the genetic information of an individual is stored is personal medical files and there are chances of misusing it, second, information on drug prescription are stored in drug companies and they are often unintentionally released or misused.

The next dangerous set of information type is information aggregation or as Danie Solove calls this as "digital dossiers". The aggregation is done by both government and private sectors for profiling and marketing purposes. Sometimes Government used to build digital dossiers for monitoring and criminal investigative purposes, and this trend started after the 9/11 attacks. The good side of it that each member of a terrorist or extremist group will be screened, also the individual citizens who have nothing to do with those groups as well. (Brin, 1999). The above explanation of information types clearly answers the question on "why does old privacy framework fail" and the simple reason is they are unsuccessful in solving modern problems with modern information types. (Yilma, November 2018) The changes are wrought by evolving digital technology, and without incorporating the above "information branches" into the rubric, the privacy legislation would fail. The digital surveillance done by government can be justified under national security concerns. Nevertheless, even the private-party's information aggregation lack adequate concern. (Vries, 2003)

CONCLUSION AND RECOMMENDATIONS

The prevailing fear deals with preventing health surveillance measures to become commercial surveillances. The governments should come forward to make open and transparent dialogues guaranteed with the promise that the data they receive will only be used for health and not to be stored for long time. After Cambridge Analytica Scandal, the manipulation of stored data has become a serious threat to right to privacy and the conflict between "overly expanded privacy definition and minimalist privacy definition" has already begun. The first one prevents future innovation in science and technology and second one puts individual citizens in a vulnerable position. To stop extreme levels privacy infringements limitations should be introduced in collecting Personally Identifiable Information and more judicial and regulatory pressure should be made towards authoritarian regimes. Right to privacy and cyber security are inter connected and awareness programs should be conducted from the grassroot level to increase the digital literacy. Using Covid 19 as an opportunity to consider the way the government uses health data will shape the privacy laws and revisit the legal framework available to protect privacy. Allowing free speech on digital platforms is also vital to speak on privacy rights violations. Online criticisms against hackers and authoritarian regimes would

create much content and awake among common population.

The International Human Rights law defines how the safeguards on right to privacy should look like. They should be effective, adequately resourced with institutional arrangements, inclusion of all branches of government, and outlined with independent civilian oversight. Introducing judicial review for surveillance activities would give a judicial warranty and creating public interest advocacy would enable active citizenry regard to the protection of right to privacy. The main concern of these safeguards is "there must be no secret surveillance system that is not under review of an independent oversight and all interferences must be authorized through an independent body". To avoid confusion and fear among public some smart strategical framework shall be introduced with four components namely consent, oversight, virtual data acquisition and informed decision making. The component consent includes minimalizing the potential for state surveillance, snooping and vigilantism. Further, download, installation and use of application must be entirely voluntary. Turn on location services and notification receiving must be done upon obtaining the consent of the user. Second, a non-partisan oversight committee should be formed with the inclusion of public representatives. Virtual data acquisition policies shall include the prohibition of unwanted sharing of personal data with public, private or governments. Forth component is informed decision making involving all the sectors and public representatives to increase trust in health authorities and government.

Apart from the framework above mentioned, some effective strategies should be put in practice by government, health authorities and private organizations. Evidence based decision making is one of such strategies and that includes conducting pilot studies and risk assessments. Through an advanced coordination of national and regional health technologies government can hold a well-informed and evidence-based decision making. Requesting assistance from WHO and other regional organizations in developing digital surveillance applications would give a chance to review the existing apps and their flows and learn from other states. Further relying on evidence-based approach would also compel the authoritarian regimes to administer a transparent regime.

In preserving or storing the data collected, the temporality should become a norm. The digital health surveillance should not become a practice in future or an excuse for a state or any other private entity to collect details for various other purposes. Privacy law shall include a clause to put an end date to completely discard the data from the stored places once the purpose of the data is served. Non-discrimination is another virtue that should be given priority in surveillances. The collected data are also markers of identity such as sex, religion, ethnicity and race. With misuse, the data would cause social stratifications deepen further and might harm minority and marginalized groups in direct or indirect ways.

The remedies for Right to Privacy violation can be categorized in to three types: Legislative remedies, judicial forms and administrative forms. The international standards expect some characteristics from the remedies that the state promises to victims such as the remedies should be known to everyone and accessible to everyone, there must be a reasonable likelihood (Redgrave v UK, Mathews v UK), should have prompt impartial investigations, and capable enough to end the ongoing violations. Further if the incidents reach out of gross Human Rights violations, non – judicial remedies will not be adequate thus

criminal prosecution is needed. It is vital to contrivance "delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of self-regulation and co-operation".

As per the Guiding Principles on Business and HR published by Human Rights Council in 2011, if the company that conducts the digital surveillance shares the date or the user information to State that should fall under the violation of international law. Therefore, the Internet Service Providers and Other companies should adopt policies that respect human rights and the users must have the transparency of how the data are being gathered, stored and used. On the whole it could be summed up as lack of national legislation, weak procedural safeguards and ineffective oversight result the absence of accountability for arbitrary or unlawful interreference in the right to privacy.

IN CONCLUSION

There is a misinterpreted theory that the outbreaks of diseases would be controlled in authoritarian regimes and the theory is justified by exemplifying China, South Korea, Israel, Iran and other oppressive countries. Unlike that, the democratic governments should come forward to persuade the citizens about the necessity of the measures with maintaining the trustworthiness.

REFERENCES

Anglim, C. (2016). Privacy Rights in the Digital Age . Grey House Publishing .

Aptheker v. Secretary of State, 378 U.S. 500 (United States Supreme Court June 22, 1964).

Article 19 . (2020, April 02). Retrieved from Coronavirus: States use of digital surveillance technologies to fight pandemic must respect human rights: https://www.article19.org/resources/covid-19-states-use-of-digital-surveillance-technologies-to-fight-pandemic-must-respect-human-rights/

Brin, D. (1999). The transparent society: Will technology force us to choose between privacy and freedom? Harvard Journal of Law and Technology , Volume 12 No 02 , 378 .

Cody, J. P. (1999). Protecting Privacy over the Internt : Has the time come to Abandon Self Regulation . Catholic University Law Review Volume 48 Issue 4 , 1-55.

Cohen, J. E. (2000). Examined Lives: Informational Privacy and the Subject as Object . George Town Univeristy Law Centre .

Council of Europe . (2020, October 12). Retrieved from Digital solutions to fight COVID-19: shortcomings protecting privacy and personal data: https://www.coe.int/en/web/portal/-/digital-solutions-to-fight-covid-19-shortcomings-protecting-privacy-and-personal-data

Daniel J. Solove, P. M. (2018). Information Privacy Law Sixth Edition . New York : Aspen Casebook Series Wolters Kluwer .

Daskel, J. (2020, April 14). The Conversation . Retrieved from Digital surveillance can help bring the coronavirus pandemic under control – but also threatens privacy: https://theconversation.com/digital-surveillance-can-help-bring-the-coronavirus-pandemic-under-control-but-also-threatens-privacy-135151

Electronic Frontier Organization . (2020, December 10). Retrieved from COVID-19 and Digital Rights: https://www.eff.org/issues/covid-19

Fund, D. F. (2020, April 29). European Digital Rights (EDRI) . Retrieved from Why COVID-19 is a Crisis for Digital Rights: https://edri.org/our-

work/why-covid-19-is-a-crisis-for-digital-rights/

International, E. (. (1 September 2001). Privacy & Human Rights : An International Survey on Privacy Laws and Developments . Washington DC USA : Business & Human Rights Centre .

Kharak Singh v State of Uttar Pradesh , 1963 AIR 1295, 1964 SCR (1) 332 (Supreme Court of India December 18, 1962).

Lin, E. (2002). Prioritizing Privacy : A Constitutional Response to the Internet . Berkeley Technology Law Journal , 1086-1094.

Meaker, M. (2020, April 2020). World Politics Review . Retrieved from Are Governments Sacrificing Privacy to Fight the Coronavirus Pandemic?: https://www.worldpoliticsreview.com/articles/28682/coronavirus-contact-tracing-and-the-right-to-privacy-in-a-pandemic

Meyer, D. (2020, April 20). Fortune . Retrieved from More surveillance and less privacy will be the new normal after the coronavirus pandemic: https://fortune.com/2020/04/20/privacy-surveillance-coronavirus-pandemic-covid-19-tracking/

Privacy Rights in the Digital Age . (May 2019). Grey House Publishing .

Richardson, M. (2020). Advanced Introduction to Privacy Laws . Gloss UK : Edward PublishingLts .

Solove, D. J. (2001). Privacy and Power: Computer Databases and Metaphors for Information Privacy . Stanford Law Review .

United Nations Human Rights, U. H. (2020). Digital rights in the COVID-19 era .

Vries, W. T. (2003). Protecting Privacy in the Digital Age . BERKELEY TECHNOLOGY LAW JOURNAL, 283-311.

Winnick, R. (1994). SEARCHES AND SEIZURES OF COMPUTER AND COMPUTER DATA. Harvard Journal of Law and Technology Volume 1 No 2 , 77-78.

Yilma, K. M. (November 2018). The "Right to Privacy in the Digital Age" - Boundaries of the New UN Discourse . Nordic Journal of International Law , 485-528.