ST. FRANCIS' COLLEGE MODEL UNITED NATIONS '19

BACKGROUND GUIDE

UNHRC

AGENDA:

EVALUATING THE POTENTIAL HUMAN RIGHTS INFRINGEMENT BY TECHNOLOGICAL DEVELOPMENT.

LETTER FROM THE EXECUTIVE BOARD

Greetings Delegates,

As part of the Executive Board, it is our responsibility to facilitate your educational experience of the simulation of the United Nations Human Rights Council at SFC MUN 2019.The agenda under discussion would be, “Evaluating the potential human rights infringement with by technological development.”

This background guide will give you an overview of the topic at hand and the work for the committee. It contains some basic elements on the topic that will guide your research, further specific links that will prime you on your country’s policy, as well as the questions that have to be answered in the document that you may propose. However such mentions do not limit the scope of discussion in the committee at all.

We expect from all delegates an active participation in the proceedings of this committee in order to have a fruitful discussion on a pertinent global problem. For that purpose, extensive and thorough research is expected of you over and beyond this study guide. Think of this study guide as merely an initiation to your research, defining the broad aspects.

UNA-USA Rules of Procedure shall be adhered to for the due course of this committee simulation. For all those participating in a Model UN conference for the first time, and otherwise, kindly refer to the link for understanding the procedure.
https://static1.squarespace.com/static/5457f2ece4b0a485997c0d67/t/5a318b52e4966b0b6edbbdcb/1513196371261/UNA-USA+Procedure.pdf

This goes without saying, if you have any questions or doubt regarding your preparation for the committee please feel free to contact any of us.

We wish you all the best in your preparation for this committee and we are looking forward towards a good debate expectantly.

Yours Sincerely,

Yash Gupta (President)
Rakshit Bajpai (Vice-President)
Aaryan Kumar (Rapporteur)

MANDATE OF THE COMMITTEE

"The Office of the High Commissioner for Human Rights (OHCHR) is mandated to promote and protect the enjoyment and full realization, by all people, of all rights established in the Charter of the United Nations and in international human rights laws and treaties. OHCHR is guided in its work by the mandate provided by the General Assembly in resolution 48/141, the Charter of the United Nations, the Universal Declaration of Human Rights and subsequent human rights instruments, the Vienna Declaration and Programme of Action the 1993 World Conference on Human Rights, and the 2005 World Summit Outcome Document.

The mandate includes preventing human rights violations, securing respect for all human rights, promoting international cooperation to protect human rights, coordinating related activities throughout the United Nations, and strengthening and streamlining the United Nations system in the field of human rights. In addition to its mandated responsibilities, the Office leads efforts to integrate a human rights approach within all work carried out by United Nations agencies"[1].

"The mission of the Office of the United Nations High Commissioner for Human Rights (OHCHR) is to work for the protection of all human rights for all people; to help empower people to realize their rights; and to assist those responsible for upholding such rights in ensuring that they are implemented.

In carrying out its mission OHCHR will:

Give priority to addressing the most pressing human rights violations, both acute and chronic, particularly those that put life in imminent peril;

Focus attention on those who are at risk and vulnerable on multiple fronts;

Pay equal attention to the realization of civil, cultural, economic, political, and social rights, including the right to development; and

Measure the impact of its work through the substantive benefit that is accrued, through it, to individuals around the world.

Operationally, OHCHR works with governments, legislatures, courts, national institutions, civil society, regional and international organizations, and the United Nations system to develop and strengthen capacity, particularly at the national level, for the protection of human rights in accordance with international norms.

Institutionally, OHCHR is committed to strengthening the United Nations human rights programme and to providing it with the highest quality support. OHCHR is committed to working closely with its United Nations partners to ensure that human rights form the bedrock of the work of the United Nations"[2].

"The United Nations human rights programme has grown considerably since its modest beginnings some 60 years ago. Organizationally, it started as a small division at United

[1] https://www.ohchr.org/EN/ABOUTUS/Pages/Mandate.aspx
[2] https://www.ohchr.org/EN/AboutUs/Pages/MissionStatement.aspx

Nations Headquarters in the 1940s. The division later moved to Geneva and was upgraded to the Centre for Human Rights in the 1980s. At the World Conference on Human Rights in 1993, the international community decided to establish a more robust human rights mandate with stronger institutional support. Accordingly, Member States of the United Nations created OHCHR by a General Assembly Resolution in 1993.

The growth in United Nations human rights activities has paralleled the increasing strength of the international human rights movement since the United Nations General Assembly adopted the Universal Declaration of Human Rights on 10 December 1948. Drafted as 'a common standard of achievement for all peoples and nations', the Declaration for the first time in human history set out basic civil, political, economic, social and cultural rights that all human beings should enjoy. It has over time been widely accepted as the fundamental norms of human rights that all Governments should respect. December 10, the day of its adoption, is observed worldwide as International Human Rights Day. The Universal Declaration, together with the International Covenant on Civil and Political Rights and its two Optional Protocols, and the International Covenant on Economic, Social and Cultural Rights, form the "International Bill of Human Rights."Alongside the development of international human rights law, a number of United Nations human rights bodies have been established to respond to changing human rights challenges. They rely on OHCHR for both substantive and secretariat support in discharging their duties. These bodies can be either Charter-based and political bodies consisting of State representatives with mandates established by the United Nations Charter, or they can be treaty-based committees with independent experts set up, with the exception of one, by international human rights treaties and mandated to monitor State parties' compliance with their treaty obligations. The United Nations Commission on Human Rights, established in 1946 and reporting to the Economic and Social Council, was the key United Nations intergovernmental body responsible for human rights until it was replaced by the Human Rights Council in 2006. In addition to assuming mandates and responsibilities previously entrusted to the Commission, the newly created Council, reporting directly to the General Assembly, has expanded mandates. These include making recommendations to the General Assembly for further developing international law in the field of human rights, and undertaking a Universal Periodic Review of the fulfillment of each State of its human rights obligations and commitments"[3]

INTRODUCTION

Technology can be a powerful tool for human rights. Increased access to the internet and the development of social media tools have enabled activists to organise and spread their message more quickly and to broader audiences. Emerging technologies, such as artificial intelligence, may significantly expand the availability and quality of data upon which to make informed decisions for the benefit of society. Supporters of these technologies believe that they will unleash new opportunities, increase efficiency, and help maximise human potential.

[3] https://www.ohchr.org/EN/AboutUs/Pages/BriefHistory.aspx

At the same time, rapid developments in artificial intelligence, automation and robotics raise serious questions about potential impacts on human rights and the future of work, as well as who will benefit and lose from their expansion. There is a risk that the use of machines to increase productivity will result in mounting inequality through downward pressure on wages and loss of jobs. The growth of the “gig economy”, facilitated by technology, has contributed to changing the nature of work by increasing the availability of flexible positions that provide opportunities for some while negatively affecting the livelihoods of others. In addition, the mass collection of data can lead to violations of the right to privacy and make it easier for governments to monitor the activities of activists.

Many of these impacts are yet unknown. Human rights organisations are currently exploring how to ensure that these technological advances can benefit all people and do not exacerbate inequality for those who are already among the most marginalised.

IMPACT OF AUTOMATION AND DIGITAL DEVELOPMENTS ON HUMAN RIGHTS

The Internet of Things

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

How does it work?

Devices and objects with built in sensors are connected to an Internet of Things platform, which integrates data from the different devices and applies analytics to share the most valuable information with applications built to address specific needs.

These powerful IoT platforms can pinpoint exactly what information is useful and what can safely be ignored. This information can be used to detect patterns, make recommendations, and detect possible problems before they occur. The information picked up by connected devices enables us to make smart decisions about which components to stock up on, based on real-time information, which helps in saving time and money. With the insight provided by advanced analytics comes the power to make processes more efficient. Smart objects and systems mean you certain tasks can be automated, particularly when they are repetitive, mundane, time-consuming or even dangerous. Naturally, sharing of information has its own risk, and sharing information on such a widespread platform, makes it vulnerable to prying eyes which can be potential dangers. Therefore, to protect civillians against such, laws have come into existence.

The first laws governing the use of personal information came out of Europe in the 1970s when it became clear that new forms of communication needed new forms of protection. Since then, the UN has stated, "the rights held by people offline must also be protected online." In 2013, the UN adopted a resolution to reaffirm and outline the right to privacy in a digital age, which calls upon governments to be transparent and proactive in how they handle two key privacy vulnerabilities: surveillance and misuse of personal data.

Surveillance

Surveillance can enhance the workings of corrupt agencies and corporations. The dangers of government surveillance and non-governmental surveillance, are just as alarming. Surveillance can empower individuals or governments monitor and disarm political dissent, thereby hindering democracy. It can concentrate knowledge in the hands of the powerful few and allow commercial entities to influence consumer behavior. Spyware, as in extreme cases like the Syrian Civil War, or rather any war poses a great threat.

Misuse of Personal Data

Exposing personal data can be catastrophic. However, even if it isn't catastrophic, it's still a violation of rights. Personal data can be gathered digitally, biometrically, genetically, and via video and other media.

Protecting consumer privacy becomes increasingly difficult as the IoT becomes more prevalent. More devices are connected to different types of devices and this increase in connectivity and data collection results in less control. Both control of data and control of the very devices that are connected are at stake.

Innovation in this realm means that companies must alter the privacy policies that are in place as well as how they interact with these devices. Companies will need to take another look at the policies that they have in place to ensure that consumers are offered opportunities to access and control their own data. Consumers will become increasingly aware of the privacy implications of this level of connectivity through interaction with the IoT and exposure to the policies that companies provide to them

Security Issues

Because IoT devices are connected to the Internet, they are vulnerable to the same kinds of cyber-attacks that can afflict consumer, commercial, industrial, and governmental computer systems. In September 2016, weak security in IoT devices was exploited on a massive scale by the "Mirai" botnet, which gained control of hundreds of thousands of such devices, and subsequently used them to launch massive distributed denial of service attacks, capable of effectively shutting down targeted websites. Because IoT devices rely on connectivity to function, they create a common attack vector for hackers to gain access to an entire network. Many IoT devices are built using very similar underlying hardware and software, and are frequently not designed with cybersecurity in mind, which increases the risks they pose.

IoT Can Increase Privacy Protections

IoT systems extensively use Encryption and other security measures to protect the data. Encryption reorganizes information into an unreadable format, accessible only by an encryption key. Robust encryption can ensure that certain messages and thus certain personal data are safe from prying eyes. In many cases, this can help support the right to freedom of expression, association, and assembly—especially among vulnerable people groups like oppositional political groups or those fleeing persecution or abuse.

However, there's a bad side to it too— it can assist illegal communications to take place safely and thus hinder individual or National security.

Therefore, privacy and security are seen in opposition to each other.

The defenders of mass surveillance programs have quite blatantly given the choice to choose either privacy or security, liberties or protection.

This is a simplistic way of looking at the issues and it has been tampering with our ability to identify sound public policies that strike a sensible balance between these concerns.

The question that should be asked is: is it right for the state to store, and share, information about people's personal phone calls, emails and social media interactions… potentially indefinitely?

The answer should be guided by the principles of the UDHR, which, according to its Article 12 states: People have a right to privacy. But also, it's the State's responsibility to safeguard the nation from any potential threats, so, governments should only be looking at an individual's information if, and only if, they have probable cause to suspect wrongdoing.

The main aim of the laws should be focused on attaining the highest degree of both-Privacy AND Security, in consonance with each other.

Automation

Automation, can be defined as the application of machines to tasks once performed by human beings or, increasingly, to tasks that would otherwise be impossible. Although the term mechanization is often used to refer to the simple replacement of human labour by machines, automation generally implies the integration of machines into a self-governing system. Automation has revolutionized those areas in which it has been introduced, and there is scarcely an aspect of modern life that has been unaffected by it.

In general usage, automation can be defined as a technology concerned with performing a process by means of programmed commands combined with automatic feedback control to ensure proper execution of the instructions. The resulting system is capable of operating without human intervention. The development of this technology has become increasingly dependent on the use of computers and computer-related technologies. Consequently, automated systems have become increasingly sophisticated and complex. Advanced systems represent a level of capability and performance that surpass in many ways the abilities of humans to accomplish the same activities.

Automation technology has matured to a point where a number of other technologies have developed from it and have achieved a recognition and status of their own. Robotics is one of these technologies; it is a specialized branch of automation in which the automated machine possesses certain anthropomorphic, or humanlike, characteristics. The most typical humanlike characteristic of a modern industrial robot is its powered mechanical arm. The robot's arm can be programmed to move through a sequence of motions to perform useful tasks, such as loading and unloading parts at a production machine or making a sequence of spot-welds on the sheet-metal parts of an automobile body during assembly. As these examples suggest, industrial robots are typically used to replace human workers in factory operations.

Effect of Automation

"Will 2018 be the year a robot takes my job? That is the question many workers are asking themselves. While the number of jobs that will be lost to automation is a hotly contested topic, there is no denying that the growing use of advanced robotics and artificial intelligence will have significant impacts on workers, wages, and human rights more broadly. It is therefore critical that the global community begin to think through the necessary legal and policy responses to increased automation and ensure that the future of work places human rights front and center"

-Sarah McGrath, Former Legal and Policy Director, International Corporate Accountability Roundtable

It is highly believed that the greatest threat posed due to automation is by the low paid officials for low ranking jobs (mainly physical labor) and even some white collar jobs like

data analysis is said to be replaced by Machine learning (a narrower application of artificial intelligence).

Impact on the individual

Nearly all industrial installations of automation, and in particular robotics, involve a replacement of human labour by an automated system. Therefore, one of the direct effects of automation in factory operations is the dislocation of human labour from the workplace. The long-term effects of automation on employment and unemployment rates are debatable. Most studies in this area have been controversial and inconclusive. Workers have indeed lost jobs through automation, but population increases and consumer demand for the products of automation have compensated for these losses. Labour unions have argued, and many companies have adopted the policy, that workers displaced by automation should be retrained for other positions, perhaps increasing their skill levels in the process. This argument succeeds so long as the company and the economy in general are growing at a rate fast enough to create new positions as the jobs replaced by automation are lost.

Of particular concern for many labour specialists is the impact of industrial robots on the work force, since robot installations involve a direct substitution of machines for humans, sometimes at a ratio of two to three humans per robot.

Impact on society

Besides affecting individual workers, automation has an impact on society in general. Productivity is a fundamental economic issue that is influenced by automation. The productivity of a process is traditionally defined as the ratio of output units to the units of labour input. A properly justified automation project will increase productivity owing to increases in production rate and reductions in labour content. Over the years, productivity gains have led to reduced prices for products and increased prosperity for society.

A number of issues related to education and training have been raised by the increased use of automation, robotics, computer systems, and related technologies. As automation has increased, there has developed a shortage of technically trained personnel to implement these technologies competently. This shortage has had a direct influence on the rate at which automated systems can be introduced. The shortage of skilled staffing in automation technologies raises the need for vocational and technical training to develop the required work-force skills. Unfortunately the educational system is also in need of technically qualified instructors to teach these subjects, and the laboratory equipment available in schools does not always represent the state-of-the-art technology typically used in industry.

On one hand , automation has created more job opportunities for the skilled personnel while it has compromised on the physical labour class, thus directly concerning to Right of fair and decent work . It has also propelled the standards of the living conditions for not only the upper class but also the lower middle class by increasing production and thus bringing down the prices of commodities as well as luxuries.

Therefore, all of these factors should be taken into consideration while formation of laws and it is critical that workers and labour unions be at the centre of discussions and decision-making about how automation can be utilised to benefit all. Under the UN Guiding Principles on Business and Human Rights, companies have the responsibility to avoid causing or

contributing to adverse human rights impacts, such as violations of the risk to decent work, through their own activities and address such impacts when they occur.

Therefore, companies increasing their use of automation should help in mitigating negative impacts on workers by investing in new skill development opportunities.

RIGHT TO PRIVACY

Article 12 of the Universal Declaration of Human Rights states:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the International Covenant on Civil and Political Rights states:

No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

Everyone has the right to the protection of the law against such interference or attacks.

The United Nations General Assembly Resolution on the right of privacy in the digital age, passed on December 18, 2013 and the General Comment of the United Nations Human Rights Committee on the right of privacy, family, home, correspondence, and protection of honour and reputation, under the International Covenant of Civil and Political Rights (ICCPR), expressed in 1988, demands that working of State Surveillance be subject to legality through clear and precise law, which law itself must look to safeguard the right to privacy.

The General Assembly affirmed that the rights held by people offline must also be protected online, and it called upon all States to respect and protect the right to privacy in digital communication. The General Assembly called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data and emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law.

Internet censorship and surveillance by country

HUMAN RIGHTS & NATIONAL SECURITY

What are Human Rights?

Human rights are not conferred by any ruler, constitution or statute. A human being is born with human rights. Giving new dimensions to Article 21 of the Constitution, the Supreme Court, in the cases noted below, has declared that right to live as guaranteed under Article 21 is not merely confined to physical existence but it includes within its ambit the right to live with human dignity. The right to live is not restricted to mere animal existence. It means something more than just physical survival.

The right to 'live' is not confined to the protection of any faculty or limb through which life is enjoyed or the soul communicates with the outside world but it also includes "the right to live with human dignity", and all that goes along with it, namely, the bare necessities of life such as, adequate nutrition, clothing and shelter and facilities for reading, writing and expressing ourselves in diverse forms, freely moving about and mixing and commingling with fellow human being. Anything which impedes the right to lead life with dignity and decency is violative of human rights.

Life without dignity is like a sound i.e. not heard. Dignity speaks, it has its sound, it is natural and human. It is a combination of thought and feeling and it deserves respect even when the person is dead and described as a 'body'. Quality of life ensures dignity of living and dignity is but a process in realizing the sanctity of life. The quality of life depends upon the life in our years.Adding to the length of life must bear a functional nexus with the quality of life. Human sufferings must have significance not only in terms of how long we live but also in terms of how well we live. The right to live with dignity also includes the smoothing of the process of dying in case of a terminally-ill patient or a person in PVS with no hope of recovery.

Human Rights are rights that belong to every person and they are not dependent on specifics of the individual. Human Rights are moral, pre-legal rights and cannot be granted by people or taken away by them. Human Rights have been recognized by the Universal Declaration of Human Rights and adopted as Fundamental Rights in Part III of our Constitution[4].

With the declaration of human rights on December 10, 1948, India became one of the signatory countries of the world having made commitment to respect and protect the human rights declared and accepted by the United Nations Organizations. The UNO had required the signatory countries to incorporate the universally acknowledged human rights in their Constitutions and domestic laws.

National Security

National Security is one of the most crucial agenda any government would focus upon. The safety and welfare of the citizens of a country comes first, always. In todays world, with terrorism at its peak and emergence of other radical groups, national security has become the priority of most of the governments. Since, this is a matter of concern for the member nations, even the United Nations cannot impose anything on them and its word will just have persuasive value. National Security involves the use of Intelligence Agencies for gathering

[4]National Legal Services Authority Vs. Union of India, (2014) 5 SCC 438.

information which may be in the form of HUMINT (Human Intelligence, gathered by the field agents), MILINT (Military Intelligence, which provides information about the cross-border threats), Electronic Surveillance, Covert/Overt Surveillance, Satellite Imagery, etc. Since, the priority of these Intelligence Agencies is on gathering information at any cost, they tend to ignore the basic human rights at the cost of national security.

There must be a balance between the methods of information gathering and human rights. Human Intelligence is gathered by creating a network of spies and is first hand information which is completely unfiltered, the good thing about human intelligence is that it is rarely obtained in an encrypted form and can be used as it is. Human Intelligence as such is not very violative of the basic human rights of the people, but in certain cases, when the spy network tries to manipulate and induce certain incidents in a person's life, it deprives the person being targeted of his/her Right to Live with Dignity and Freedom. As far as Military Intelligence is concerned, it is primarily used by the armed forces of a country to acquire information related to cross-border terrorism, smuggling, infiltration, etc. The Electronic Surveillance is one of the main concerns of the human rights activists, as it violates the right to privacy and many other basic human rights. One must understand that these methods are there to ensure national peace, security and integrity. However, things go wrong when the existing regime use them for malafide purposes and eventually depriving the people of a certain set of fundamental rights.

Balancing Security & Human Rights

The "Hague Approach Principles" can be considered as a source, based on which a model for balancing national security and human rights could be devised. "The goal of this project was to identify best practices and guidelines for strengthening peacebuilding and establishing the rule of law in conflict-affected settings. Building on ideas from those who have lived in conflict-affected situations and know what life is like without the rule of law, interim-project outcomes were drafted and tested. A lot of experts and researchers participated in this process, and were invited to collaborate in expert meeting"[5].

Principle 1 (Conflict Prevention) and 2 (Fostering a Rule of Law Culture) in particular provide a way out of this problem. If the national security analysts are able to frame a network of electronic surveillance and human intelligence keeping a balance between the two and ensuring that both of them run complimentary to each other, this problem might end.

For, e.g. Netherlands is making to conflict prevention and fostering a rule of law culture abroad. The Dutch army regiments stationed in Mali provide support to the ongoing UN mission in the region, training police and government forces. Dutch police forces in South Sudan protect public safety in refugee camps. In the Western Balkans, Dutch judges train their local counterparts and build partnerships that improve the judiciary and enhance accountability. Local leaders, authorities, community organizers and teachers are key partners in all these efforts.

However, as the issue in front of the committee also involves the aspect of technology, it is very important that the human rights council address the issue of government databanks used by the intelligence agencies and are prone to be misused by a single person or a group of people for their personal gains. For e.g. the organized data possessed by these agencies if sold to any private/commercial entity might help them make profit, but it will compromise the security and privacy of the subject of that database, which might be catastrophic.

[5] http://www.thehagueinstituteforglobaljustice.org/projects/the-hague-approach/

Therefore, it is possible to maintain a balance between the human rights and the security of the country. The need of the hour is a system of checks and balances which could monitor the large pool of information possessed by the intelligence agencies.

Infringement of Right to Privacy

Due to the emergence of new technology and Science progressing towards the world of Artificial Intelligence, the debate on human rights on a public forum has become very reactive, piecemeal, and often impractical. Given that so many dimensions of society have been disrupted by digital technology, it has been difficult for policymakers to see the bigger trends, to understand the relationship between the parts, and to assess top priorities. Therefore, its high time that the policymakers become more proactive and holistic, and to advance practical solutions to several priority global human rights challenges.

"One traditional human rights concern that has been aggravated by digital technology is global inequality. This is caused by the lack of access to technology, rather than technology itself. While those of us who live in the digital ecosystem can't remember what daily life is like without Internet connectivity or our digital devices, the majority of people in the world have zero digital experience. Globally, nearly six out of ten people are not connected to the Internet. Even more stark is the fact that roughly 65 percent of people in the developing world do not yet use the Internet. And women generally have less access to the Internet (another expression of gender inequality), as do people living in rural areas.

These digital divides have the potential to significantly exacerbate existing global inequality and lead to conditions where conflict is more likely. Nearly all of the UNSustainable Development Goals adopted in September depend on expanding access to information and communications technology infrastructure around the planet. But the prospect of reaching the UN goal of universal Internet access in the developing world by 2020 does not look realistic at the current rate. Narrowing the digital divide must be ranked as a top human rights priority"[6].

Case Study : Social Credit Policy of China & Electronic Surveillance

In an "old school" dimension of its digital social-monitoring system, China apparently employs two million Internet police who are tasked with monitoring online activity of citizens and sifting through millions of messages on social media and micro-blogging sites. This data is compiled into government reports about the potential for social unrest and is used to clamp down on political and social activity.The Chinese digital credit rating system is a state-of-the-art example of where big data could facilitate Big Brother at a whole new level. This social-credit rating blends comprehensive online monitoring with algorithms aimed at establishing correlations between negative social behaviour and Internet activity. It is currently being used to assess financial credit worthiness, but its intended future use may be for much broader social control — reportedly to assess citizen's overall trustworthiness and honesty, and to assign citizenship scores based on "patriotic criteria. As it appears, anyone having a malafide intention could misuse this data to his/her benefit and the loss will be suffered by the people and the government.

Countries facing terror threats, imposition of vague and expansive cyber-related laws without adequately considering or protecting human rightshas led to erosion of some very basic

[6] https://www.hrw.org/news/2016/03/25/digital-disruption-human-rights

human rights principles (e.g., that surveillance programs must be both necessary and proportionate). Ambiguous, imprecise, and unnecessarily intrusive counterterrorism laws have been replicated around the world by governments of all stripes. Even governments that see themselves as human rights champions have found it difficult to bring their counterterrorism activities under the rule of law.

For example, "notwithstanding all the post-Snowden uproar in Europe about US mass surveillance, the French parliament adopted a "Law reinforcing measures relating to the fight against terrorism" in November 2014 that raises issues of compatibility with the rights to free movement, to the presumption of innocence, and to free expression. The UK's Investigatory Power's Bill, in its current form, would legalize mass global surveillance by UK security agencies, and allow extraterritorial hacking of computers, phones, and networks. And some members of the Freedom Online Coalition — a group of 29 governments convened for the specific purpose of reinforcing human rights protections online — continue to call for backdoors or exceptional access to encryption for themselves, without recognizing that such actions not only threaten the protection of human rights and privacy, but also undermine their security.The saddest aspect of this trend is the role-modeling dimension: Governments that see themselves as human rights-respecting democracies are modeling practices that are being replicated in other more repressive environments. They are also giving a form of cover and permission to undermine human rights. Respect for rights and adherence to the rule of law, even and especially in the context of terrorism, is a hallmark of strength in democratic systems, and a principled distinction with authoritarian systems. These governments must engage in urgent self-examination of whether and how their counterterrorism policies practices meet universal human rights principles, and should become vocal advocates for adherence to the rule of law in the digital context"[7].

The Right to Privacy has been upheld as a fundamental human right in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR). Beyond the ICCPR General Comment No.16: Article 17 (Right to Privacy) in 1988 and the 2010 report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, the right to privacy was hardly referenced within the UN human rights mechanisms. It becomes very clear as to how does mass scale electronic surveillance makes the preservation of Human Rights difficult.

Human Right Violations on a Digital Platform by the Non-State Actors

As we all know, the IT wing of most of the violent Non-State Actors like the Lashkar-e-Taiba, Boko Haram, Al Qaeda, Islamic State, etc. has been very instrumental for them while spreading their propaganda. The digital crimes committed by such organizations involve hacking into the database owned by any country and manipulating that database to the extent of their profit.

"Terrorist groups incite individuals, often young people, to leave their communities across the world and travel to conflict zones, primarily in Iraq and Syria and increasingly in Libya. The way recruits are targeted and radicalized has shifted, with a greater focus on social media and other digital channels.Biometric data is of increasing importance in identifying foreign terrorist fighters and preventing them from crossing borders, while we also promote the exchange of battlefield data between the military and police"[8]. These digital networks not

[7] https://www.hrw.org/news/2016/03/25/digital-disruption-human-rights
[8] https://www.interpol.int/en/Crimes/Terrorism

only help them in recruitment of foreign fighters, but also to incite uprisings and rebellions in many countries.

Usually, people tend to settle on the fact that it's better to compromise the right to privacy and other basic human rights with national security than to face the other end of the barrel accompanied by cyber attacks on them, done by the non-state actors.

(i) Threat of Cyber Warfare Among the States

"The most serious cyber warfare threats facing the West come from China and Russia, that much is undebatable, with Iran and North Korea a step or two behind. Those CRINK nation states occupy most of the strategic mindshare within the defense and intelligence agencies charged with keeping us safe. But now Lt.-Gen Vincent Stewart, former deputy chief of U.S. Cyber Command and director of the Pentagon's Defense Intelligence Agency, has warned that we need to urgently broaden our thinking.Much of the cyber threat focused on military, critical infrastructure and commercial targets in the West is developed by so-called Advanced Persistent Threat (APT) groups allied with and funded by nation state agencies, but not embedded within them. We have seen these often arms-length entities double-hat their activities, conducting likely state-mandated operations while freelancing for personal gain as well.With this in mind, Stewart has warned that if al-Qaeda or ISIS were able to purchase cyberattack capabilities or even services from such a group then swathes of critical infrastructure could be at risk. Russia and China have such capabilities, but play the balance between impact and implications—causing damage but stopping short of prompting devastating repercussions. Terror groups have no such constraints and often operate at the margins of their capabilities"[9].

CURRENT MEASURES IN PLACE

One of the biggest concerns regarding advancement of technology is the change which can be observed in the nature and the medium through which crimes are being committed. All this has resulted in the emergence of cybercrimes in the society. International cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. No matter, in developing or developed countries, governments and industries have gradually realized the colossal threats of cybercrime on economic and political security and public interests. However, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale.

---

[9] https://www.forbes.com/sites/zakdoffman/2019/09/13/cyber-dirty-bomb-terrorist-threat-is-real-warns-us-cyber-general/#66774efb679f

Although there is no specific treaty, convention or a declaration regarding implementation of cyber security provisions or any limitations regarding the use of Artificial Intelligence in the defence industry. However, from time to time various bodies of the United Nations have been expressing their concern on this issue.

“Advances in information communication technology are dramatically improving real-time communication and information-sharing. By improving access to information and facilitating global debate, they foster democratic participation. By amplifying the voices of human rights defenders and helping to expose abuses, these powerful technologies offer the promise of improved enjoyment of human rights.But at the same time it has become clear that these new technologies are vulnerable to electronic surveillance and interception. Recent discoveries have revealed how new technologies are being developed covertly, often to facilitate these practices, with chilling efficiency. As the previous High Commissioner cautioned in past statements [September 2013 and February 2014], such surveillance threatens individual rights – including to privacy and to freedom of expression and association – and inhibits the free functioning of a vibrant civil society.

In December 2013, the United Nations General Assembly adopted resolution 68/167, which expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights. The General Assembly affirmed that the rights held by people offline must also be protected online, and it called upon all States to respect and protect the right to privacy in digital communication. The General Assembly called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data and emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law.

As General Assembly resolution 68/167 recalled, international human rights law provides the universal framework against which any interference in individual privacy rights must be assessed. The International Covenant on Civil and Political Rights, to date ratified by 167 States, provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. It further states that “Everyone has the right to the protection of the law against such interference or attacks.”

Other international human rights instruments contain similar provisions. While the right to privacy under international human rights law is not absolute, any instance of interference must be subject to a careful and critical assessment of its necessity, legitimacy and proportionality.”[10].

In 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation. In 2000 the UN GA adopted a resolution on combating the criminal misuse of information technology. In 2002 the UN GA adopted a second resolution on the criminal misuse of information technology.

[Refer - http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/events/2010/wg1/docs_wk1/Marco_Gercke_Regional_and_International_Trends_in_Information_Society_Issues_HIPCAR_WG-1_workshop01_20100308.pdf]

Apart from all this, Asia-Pacific Economic Cooperation (APEC) is an international forum that seeks to promote promoting open trade and practical economic cooperation in the Asia-

[10] https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx

Pacific Region. In 2002, APEC issued Cybersecurity Strategy which is included in the Shanghai Declaration. The strategy outlined six areas for co-operation among member economies including legal developments, information sharing and co-operation, security and technical guidelines, public awareness, and training and education.

In 2001, the European Commission published a communication titled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".In 2002, EU presented a proposal for a “Framework Decision on Attacks against Information Systems”. The Framework Decision takes note of Convention on Cybercrime, but concentrates on the harmonisation of substantive criminal law provisions that are designed to protect infrastructure elements.

“The Economic Community of West African States (ECOWAS) is a regional group of west African Countries founded in 1975 it has fifteen member states. In 2009, ECOWAS adopted the Directive on Fighting Cybercrime in ECOWAS that provides a legal framework for the member states, which includes substantive criminal law as well as procedural law”[11].

LINKS FOR REFERENCE

- https://www.weforum.org/agenda/2017/12/how-are-today-s-biggest-tech-trends-affecting-human-rights/
- https://www.business-humanrights.org/en/technology-and-human-rights
- http://archive.unu.edu/unupress/lecture4.html
- https://www.hrw.org/news/2016/03/25/digital-disruption-human-rights
- https://www.cambridge.org/core/books/new-technologies-for-human-rights-law-and-practice/technology-and-human-rights-enforcement/46A87E79DEB11BB9910273F41AF5CC8D/core-reader
- https://www.accessnow.org/digital-rights-101-understanding-how-technology-affects-human-rights-for-all/
- http://phrg.padovauniversitypress.it/system/files/papers/2017_2_4.pdf
- https://theconversation.com/why-technology-puts-human-rights-at-risk-92087
- https://www.openglobalrights.org/technology/

[11]- http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/events/2010/wg1/docs_wk1/Marco_Gercke_Regional_and_International_Trends_in_Information_Society_Issues_HIPCAR_WG-1_workshop01_20100308.pdf