Oguzkaan Schools
JMUN
Special Committee I

Issue :

The Right to Privacy and Security in Digital Age

Forum: Special Committee I

Issue: The Right to Privacy and Security in Digital Age

Student Officers: Berk Yenici,Oğulcan Karaca, Kaan Aşıkoğlu, Defne Uraz, Efe Topoğlu

I. Introduction

As the technology advances, it becomes even more important to secure private information and prevent it from being convenient to abuse. Today, the position of technology has brought the problem to a much more serious point. Thus, the discussions upon this subject have grown in significance and become more popular around the world.

Technological devices, being a major part of our lives, store more personal information than expected. From one's location to contacts, most apps collect very detailed personal information from devices, claiming to "provide a better experience" to users. People accept the Terms of Use without reading, and it turns that those terms include sending personal information to third-party companies. A possible stealing of personal data could lead to worse; it is not difficult for hackers to reach to a bank account or a house address if they are not safely stored.

Throughout few previous decades, foreseeing the possible danger of developing technology and the overwhelming amount of personal data being stored, several acts and regulations were signed and brought into action. Since an average person couldn't tell a safe website and more people got hacked every day, it was obvious that a regulation regarding the storage of personal data and immediate spread of awareness was necessary.

Consequently, after the insufficient Data Protection Act, General Data Protection Regulation was adopted with great hopes by the European Union.

II. Definition of Key Terms

Personal Data: Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identify of that person. Examples include date of birth, sexual orientation and religion.

Cookies: The main purpose of a cookie is to identify users and possibly prepare customized web pages for them. When a user enters a website using cookies, they may be asked to fill out a form providing such information as their name and interests. That information is packaged into a cookie and sent to their browser which stores it for later use. The server can use the information to present them with custom pages.

Data Protection: The process of safeguarding important information from corruption, compromise or loss.

Privacy Breach: The loss of unauthorized access to, or disclosure of personal information. Most common privacy breaches happen when personal information is stolen, lost or mistakenly shared.

Hacking: A term generally referring to unauthorized intrusion into a computer or a network.

Hacker: The person engaged in hacking activities. A hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.

Phishing: The fraudulent practice of sending emails in order to induce individuals to reveal personal information, mostly passwords and credit card numbers.

Internet/Digital Security: The knowledge of maximizing the user's personal safety and security risks on private information and property associated with the usage of internet, and the self-protection from cybercrime.

Cyber Attack: The deliberate exploitation of computer systems, technology-dependent enterprises and networks which use malicious codes to alter computer code, logic or data, resulting in disruptive consequences that can jeopardize data.

Terms and Conditions: General and special arrangements, provisions, requirements, rules, specifications, and standards that form an integral part of an agreement or contract.

ICT: Information and Communication Technology (ICT), first appeared in the mid -1980s and was defined as "All kinds of electronic systems used for broadcasting telecommunications and mediated communications", with examples including personal computers, internet, etc.

Cybercrime: A crime in which a computer is an object. Cybercriminalsmay use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes.

Meddle: To interfere in something that is not one's concern.

Cybersecurity: Cybersecurity comprises an evolving set of tools, risk management approaches, technologies, training and best practices designed to protect networks, devices, programs, and data from attacks or unauthorized access.

Data Privacy Day: Being an international holiday, Data Privacy Day is celebrated annually by numerous countries on February 28th. Its main aim is to spread awareness among businesses, as well as internet users about data privacy and to emphasize the effects of the use of personal data by websites.

Identity Theft: It is also known as identity fraud. It is a crime in which an imposter obtains key pieces of personally identifiable information in order to impersonate someone else.

Cloud Computing: The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

III. General Overview

a) Current Situation and Legal Aspects

Users personal information is shared to dozens of websites from an online store to a social platform. They don't consider sharing their personal data on various platforms as dangerous, believing that it is fully private and won't be shared with third parties. Looking at the rapidly increasing number of cybercrimes, maybe the "cookies" that are allowed in every website, or the personal data users who give details to random websites, are not as innocent as they may seem.

In order to have the best understanding of the right to privacy, one must analyse the regulations correctly. In today's world, their information being collected or even being shared to a third-party company isn't really a big deal for most people. If the data subject's consent is given in the context of a written declaration,the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

'Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.' clearly states that the use of personal information is only possible with the full consent of the user, and by requesting it clearly and in a way that it is distinguishable from other matters.

Although there were several international laws concerning social media and digital privacy such as the "General Data Protection Regulation(GDPR)" passed by the European Union Parliament in 2016 which will

be further explained and detailed under a much more comprehensive title as well as the DATA PROTECTION ACT, theinadequacy of the execution and disobedience /violation determination process of those laws were undeniable.

Users discern the disturbing and obvious violations of cyber law on a daily basis yet the consequences seem innocuous. As a matter of fact,depending on the type of privacy violation users experience,they officially have the right to take legal action against the person/firm who violated their privacy.In addition, social security numbers, addresses, phone numbers, and other personal information must always be kept confidential.

Cloud computing has been one of the key innovations that is changing the landscape of technology and driving digital transformation across all industries. Despite its cost in the short run, cloud computing has been providing security, flexibility, mobility, collaboration, sustainability and broad control over two decades so far when it comes to personal data protection.

b) Main Examples of Personal Data Protection Violations

Yahoo! Privacy Breach

In the wake of 2013, Yahoo declared that around 500 million of their accounts had been breached. In November later that year, World leaked that Yahoo had allowed U.S. intelligence agencies to read through its user emails in search of red flag phrases or keywords. At the end of 2013, Yahoostated the number of the "hacked" accounts as a billion. Experts still argue if the breach was really a matter of hacking which is a low possibility. It is also very controversial if the number was around a billion in the manner Yahoo clarified. In such case, it could be the biggest privacy breach in history so far.

Google EU Data Privacy Rules Violation

France's data protection, Watchdog, fined Google 50 million euros for breaching EU online privacy rules, the biggest penalty levied against a U.S. tech giant. The EU's General Data Protection Regulation, the widest data privacy law in more than two decades, allows users to have a better control over their private data and gives regulators the power to impose fines.

The Personal Data Sharing on Facebook

One of the most scandalous events violating the protection of personal data was when Facebook shared the data of its users without permission. Mark Zuckerberg, the founder of Facebook, admitted having shared the data of eighty-seven million Facebook users to Cambridge Analytica for the purpose of political profiling.

Additionally, it turned out that Facebook gave "deep access" to Apple, Samsung, and other firms. Previously, Zuckerberg had stated that all Facebook users had "complete control" over whom they share their personal data with. After great public aggression. Facebook lost many users.

United States Government's Backdoor Demand

United States' federal government, or FBI, attempted to make Apple open a backdoor so it could peruse information in a suspect's smartphone. Apple CEO, Tim Cook, became a privacy advocate and defended the importance of the safety of personal data. The lawsuit brought up a question: If a government can bypass manufacturers in one instance, then what stops it from doing it over and over again?

IV.Timeline of Important Events

2014 Eu Court approved the right to be forgotten

2013 Edward Snowden revealed NSA surveillance operations

2000 Web bugs were introduced.

1995 Spyware started to become common and is transmitted through the internet

1994 HTTPS introduced to help secure web traffic

1990 Identity theft started to become common

1980 DNA fingerprinting started to become common

1976 Public-key encryption created to prevent the stealing of personal and business information

1928 US Supreme Court rules that seizures of electronic communications systems are constitutional.

1890 Fingerprints were first used to identify people; “The right to be let alone” introduced.

V.Promotion and Protection of the Right to Privacy

a) Responsibilities of the International Community

Despite negative trends within the digital era, the right to privacy continues to be championed as an ideal by most of the people. Multinational collaboration to preserve digital rights is on the rise. Nations are working together to establish "privacy-by-design" controls which will protect data in accordance with fundamentals that are commonly agreed.

The European Union has recently adopted the General Data Protection Regulation (GDPR), which went into effect in 2018. This regulation demands that individuals retain control of their data that they can see the information about them that is being collected and they ask for the removal of this information from internet platforms using their right to be forgotten. Organizations that collect information must employ a data protection officer, who will control that these privacy standards are upheld and personal data of those who requested to be forgotten are removed.

Multinational initiatives, which aim to protect people's digital rights, are supported by member states who participate. For instance, the International Conference for Data Protection and Privacy Commissioners (CDPPC), has been bringing together government stakeholders since 1979 to assist them fulfilling their directives by data protection officers who were sent by the member states to collaborate and work in harmony. The present UN Resolution on the Right to Privacy in The Digital Age also sets an excellent example on a positive multinational effort to protect privacy,

b) Responsibilities of Governments

Even though governments and authorities may seem responsible for violations against digital privacy, they are the tricks that can prevent and protect the digital privacy. Governments all around the world try constantly to improve their systems in order to protect right of privacy in digital age while maintaining the transparency of knowledge. It may seem like a paradox when these terms are put together, but with legislation and strict laws, authorities must protect the digital privacy of individuals, cooperations, and societies. In the era where international conflicts between nation-states often transform into a cyber war, cybersecurity is also mandatory for nations.

The Canadian Parliament's Privacy Commissioner's Guidelines for Online Consent and Brazil's "Internet Bill of Rights" could be presented as an example of government legislation to provide greater transparency of privacy practices.Such cases often seek to regulate the consent of the users and establish oversight into the interactions of individuals.

c) Responsibilities of Businesses

Even though customers are outrageous about their personal information shared and used without their consent, companies state that they have been signing "Terms and Conditions". Therefore, they have been approving companies to use their personal information, then the companies are mitigating some privacy

invasion, however, weight of the advantages and disadvantages of trading customer must be on equilibrium, with the assist of external services.

We can say that in this era where data driven technology is at peak, encrypting the personal data of individuals' is a viable solution. Furthermore, when governments could not regulate or maintain the secrecy of a personal data with an encryption, such as personal established financial networks, blockchain is an alternative technology that safeguards the right of individuals. Such efforts must be coordinated by a collaboration between businesses, organizations or even governments to protect digital privacy.

VI. Previous Attempts to Resolve the Issue

DPA (Data Protection Act)

One of the first major actions to secure personal data rightfully was "the Data Protection Act". The act was aiming to set the necessary measures to prevent the abuse of personal information which was published by the United Kingdom back in 1998.

It included many new points about data storage, demanding for the accuracy and lawfulness of personal data. After the establishment of DPA, personal information could no more be stored longer than necessary or processed without clear consent since it controls how personal data of citizens is used by companies or the government. DPA has strict control over how personal data is used, ensuring that the information is:

• used fairly, lawfully and transparently

• used for specified, explicit purposes

• used in a way that is adequate, relevant and limited to only what is necessary

• accurate and where necessary

• handled in a way that ensures appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction or damage. Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you.

These include the right to:

• be informed about how your data is being used

• access personal data

• have incorrect data updated

• have data erased

• stop or restrict the processing of your data

• data portability (allowing you to get and reuse your data for different services)

• object to how your data is processed in certain circumstances.

GPDR (General Data Protection Regulation)

It is also known as Data Protection Regulation, was agreed upon by the European Parliament and Council in April 2016. GDPR can be considered as an updated version of DPA that includes much more details and articles about the implementation of reasonable penalties to the violators, therefore requests the creation of safer websites.

It was replaced with the Data Protection Directive in 2018. GDPR is a regulation signed by the Member States of the European Union. Its aim is, as further explained below, ensuring the cybersecurity of EU citizens. In comparison to the former Data Protection Directive, the GDPR has increased penalties for non-compliance. It doesn’t have significant effects on crime rates due to various reasons. However, it prevented

many websites from stealing information thanks to its policy about non- compliance. The penalties are implemented in cases of non-compliance, and they can go up to twenty million US dollars. The penalty policy of this act is an important reason why most websites now try to avoid from security leaks. GDPR requirements apply to each member states of the European Union, aiming to create more consistent protection of personal data across EU nations.

Some key privacy and data protection requirements of the GDPR are: Providing data breach notifications, requiring the consent of individuals for data processing. The purpose of the GPDR is to impose a uniform data security law on all EU members, so that each member state no longer needs to write its own data protection laws.

Computer Misuse Act

This Act is the first legislation of the United Kingdom about the regulation of information technology. The Computer Misuse Act was adopted back in 1990, being one of the first precautions against the misuse of information technology.

The main point of it was prohibiting unauthorized access to a computer and the unauthorized modification of its files.

It has gone through several amendments since it was adopted. For example, in 2015, the penalty of breaking this law was amended to at most 14 years, depending on the severity of the crime.

VII. Relevant UN Documents

As the Board, we highly encourage you delegates all to take inspiration from the past actions taken by some of the international organizations and United Nations. Thus, our aim is to come up with various original solution ideas regarding our agenda item.

Article 12 of UN Universal Human Rights Declaration, 1948 (http://www.un.org/en/universal-declaration-human-rights/)

Many of the existent cyber security acts are based on this article, as it emphasizes the protection of personal data. Since this declaration was published in 1948, that article has needed to be modernized in order to be more effective upon the cyber security matters.

Resolution 68/167

(https://undocs.org/A/RES/68/167)

Resolution 68/167 is one of the few resolutions that is promoting the right to privacy while also putting special emphasis on digital security.

Even though it calls upon the member states to take measures to end the violations of right to privacy on digital platforms, a significant progress hasn't been made.

Resolutions 73/266 and 73/27 (https://undocs.org/A/C.1/73/L.27/Rev.1)

(https://undocs.org/A/C.1/73/L.37)

Although the agenda of our committee covers mostly personal security and privacy throughout cyberspace rather than cyberterrorism and multinational data theft, it is only for the sake of the documents and discussions during the formal committee sessions to examine the two resolutions submitted separately by the delegations of Russian Federation (Post Soviet Union) and the USA which were concerning the misuse of information technology and authority. The two resolutions were both adopted by the General Assembly in spite of their competence and contradiction.

VIII.Conclusion

The agenda at hand may have a very broad impact.However, it also contains some key roles for world leaders, international organizations and public figures to take action upon this issue.

To summarize the subject in general terms; data protection, privacy and security rights have emerged in parallel with development of the digital world and have managed to remain on the agenda until this time.

The need for urgent solution should be adopted by the entire international community and awareness studies should be initiated since the aforementioned ones, such as the Data Protection Act and General Data Protection Regulation, were inadequate. In order to prevent further violations of protection of personal information and current law disobedience, encouragement to the implementation of new laws regarding cybercrimes should be considered, since many Member States, including the USA, haven't adopted a data protection law.

A common ground about the limits of personal data storage by companies and States should be reached. A new protocol about website building could be published, since most websites, trying to avoid from higher payments are not very concerned about cybersecurity.

IX.Questions that a Resolution Must Address

1. How the Human Rights Council defines the important concepts of digital age and the right to privacy and their relation?

2. Which institutions can be created or consolidated in order to prevent hacking by non-state actors and to ensure data privacy for individuals?

3. What measures shall be taken in order to prevent digital privacy infiltration of States, is it a necessity to have limitations on this regard?

4. Does the collection of personal data by businesses without the consent of consumers constitute infiltration to privacy and human rights' violations?

6. Which human rights' violations can be caused by censorship, which limitations can be imposed on states for the regulation of censorship?

X.Bibliography

https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:02016R0679-20160504

https://www.gov.uk/data-protection

https://www.mirror.co.uk/tech/13-ways-your-privacy-violated-9479084.