Forum: **Disarmament and International Security Committee**

Issue: *The question of personal data collection by companies and lacking protection of this information.*

Student Officer: **Adar Yüksel, Frida Harder**

Introduction

United Nations Declaration of Human Rights (UDHR) 1948, Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

This year the Disarmament and International Security Committee will address the question of how personal data is collected by companies and the lack of protection of the aforementioned data.

Personal data is information that relates to a particular individual, this can be an email address including names of an individual, an **IP** address, or a phone number. If it can be used to identify somebody, even anonymous or encrypted data is classified as personal data. In order for the data not to be considered personal data, it must be anonymous so that the individual is no longer identifiable and that the anonymization is irreversible.

Companies collect and use personal data, which is used for marketing strategies giving them a responsibility to keep it safe. However, it can lead to situations that threaten national and international security, especially when this data is not protected properly. Therefore, it is the committee's goal to find methods of protecting consumers' personal data and holding companies accountable that do not take necessary precautions for all nations.

Definition of Key Terms

IP address, IP stands for Internet protocol. It allows communication between devices on a network and makes location information obtainable

Encrypted (Encryption) is a form of cybersecurity and is the process of encoding information

Hacktivism is a case of hacking done to garner attention to a specific social or justice issue

Ransom is a sum of money demanded for the return of something or someone which is being held captive

Whistleblower stands for a person who reveals crucial information to the public from a protected organization/connection

Background Information

As technology advances, so must the rules and regulations that protect us, however, different countries have different policies and rules.This leads to confusion and great difficulty tracking those who endanger data privacy protection. Many can find refuge where laws are not so clear on data protection and despite the issue being of great importance, not enough has been undertaken to find a suitable solution.

In 2013, people became aware how much of their personal data was being tracked and collected when Edward Snowden, an American **whistleblower** and former member of the CIA, leaked information about the NSA and other US intelligence agencies exposing that they had collected massive amounts of information on US citizens without their knowledge. This was a catalyst for more political action in terms of data privacy protection.

Data Leaks

In the United States, data privacy laws, while also not being very precise, can differ from state to state; this could be a reason why companies such as Facebook and Google, which are based in the US, have been sites for massive data leaks. In 2019, it was disclosed that at least 600 million passwords of Facebook users were being stored in plaintext files and that these were accessible by over 2000 Facebook employees. This is only one out of the several cases of privacy abuse.

Hacking

Hackers are prone to steal personal data such as bank details as the reselling of this information is very lucrative. They can also encrypt data and hold it for **ransom**. Poor protection makes it easier for such individuals or groups to access personal data, this is exemplified in the dating site, Ashley

Madison data breach, where profiles of several million users were made publicly available.

Timeline of Events (Relevant UN Treaties and Events)

21st January 2014 The right to privacy in the digital age A/RES/68/167

19th November 2014 The right to privacy in the digital age A/C.3/69/L.26/Rev.1 (Revision)

November 2017 Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda

25th May 2018 Introduction of the GDPR

11th October 2018 Personal data protection and privacy principles (setting a basic framework for processing personal data)

Previous Attempts to solve the Issue

The most significant pursuit of preventing the collection of personal data would presumably be the General Data Protection Regulation (=GDPR). To be precise, the GDPR is Europe's framework for data protection. This new regulation demands that companies must be able to provide safe custody for the data as well as prove the individual's consent and introduces the right to be forgotten which allows an individual to ask companies to erase their data completely. Yet, this does not allow an individual to erase themselves from the system entirely as institutions such as hospitals, government agencies, and even journalists are excluded. However, violations or data breaches are punished with high fines leading to **ransom** hacks. In many cases, companies would rather pay the hacker's little **ransom** than the high fines of the GDPR. Nonetheless, it is also important to consider China's Personal Information Protection Law (=PIPL) from 2021 which requires Chinese companies to collect only the barest minimum of data needed and offer easy resigning options. Most importantly, companies need government approval to transfer data overseas which altogether hinders the expansion of large tech companies.

Possible Solutions

First and foremost, the assurance of consensual collection and safe retainment of personal data by the companies are crucial to solving the issue which is why violations have to be penalized. However, in order to solve this issue permanently, the imposition of said penalties must be

regulated in an effort to make following the data protection laws more attractive to companies. This could aid with the prevention of issues such as **ransom** hacks. Moreover, a general data protection law for all UN members could minimize the chance of data leaks occurring in giant companies such as Google. Lastly, the companies' firewalls and other softwares with the aim of preventing hacking have to be as secure as possible in an effort to make hacking of their data as unlikely as possible.

Helpful Sites

Data Protection and Privacy Legislation Worldwide | UNCTAD

What Is a Data Broker and How Does It Work? - Clearcode Blog

Bibliography

UN Principles on Personal Data Protection & Privacy. FINAL (1) (1)

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

What is personal data? | European Commission (europa.eu)
Do the data protection rules apply to data about a company? | European Commission (europa.eu)
Collecting personal data | ICO
Protecting Personal Information: A Guide for Business | Federal Trade Commission (ftc.gov)
How Companies and Governments Do (and Don't) Protect Your Data | World101 (cfr.org)
Text - S.3300 - 116th Congress (2019-2020): Data Protection Act of 2020 | Congress.gov | Library of Congress
Personal Data Protection and Privacy | United Nations - CEB (unsceb.org)
What is the data privacy law PDPA in Singapore? PDPA - lawpilots GmbH
How and Why Businesses Collect Your Personal Data - businessnewsdaily.com
UNSDG | Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda
Facebook's Data Breaches - A Timeline - SelfKey