THREATS AND CHALLENGES TO THE PERSONAL DATA PROTECTION SYSTEM IN CYBERSPACE

Rakhimova Munisakhon Timur qizi
Master's degree candidate in International Law and Human Rights
University of World Economy and Diplomacy, Tashkent, Uzbekistan

Abstract: *The author in this article raised the issue of the increasing relevance of improving the system of personal data protection in Uzbekistan due to accelerated and inevitable digital progress and increased cases of mass data leaks on the Internet around the world.*

As an example and evidence base, the author analyzed the Cambridge Analytica case, which has become one of the largest and most scandalous leaks of Facebook user data in recent years.

Studying the global agenda, the latest challenges and threats in this area, the author raised the question of the need to transform and strengthen the institute of data protection in Uzbekistan.

Keywords: *digital progress, threats, data protection, cybercrime, leaks of data, Facebook, Cambridge Analytica, political blackmail, manipulation, digital footprints, and state security.*

In 2017, The Economist magazine recognized data as the most valuable asset on the planet[2]. Over the past few years, the number of digital footprints reflecting the actions of users on the network has increased rapidly. Modern individual leaves a huge amount of information about himself every day: social media activity, online payments and orders, data in documents, Internet search queries, as well as a variety of content in the form of text, photos or videos, as well as confidential data related to work and study.

Large amounts of data are everywhere, and although their sources are ambiguous, they are of great value because they contain important information about people's behavior and corporate secrets. Today, there are many questions and problems related to confidential data: their use in political and state interests, as an unfair competitive advantage, problems in the field of legislation on the protection and use of personal data, as well as constant leaks of information to the public.

This problem is becoming more and more urgent for ordinary users, and no institution can be completely protected from possible cyber attacks. A global analysis of leaks of confidential data of organizations from 2005 to 2018 showed that medical and commercial institutions are the most susceptible to incidents of this kind.

The problem of leaks of confidential data of organizations is also relevant in the context of Uzbekistan. In recent years, there have been several cases of data leakage of Telegram messenger users from Uzbekistan, and these are quite depressing figures. More than 50 thousand Uzbekistanis (as of July 2020) faced the leakage of their personal information on the Internet. The personal data that got into the public domain was used for

[2] «The world's most valuable resource is no longer oil, but data»// The Economist. URL.: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

calls, followed by debiting funds from the balance and making unwanted phone calls, which are popularly referred to as cold calls[3].

In July 2020, the Cybersecurity Center of the Republic of Uzbekistan announced the appearance of a Telegram user database on the Internet, which contained more than 40 million lines, of which 50,062 related to Uzbek cellular operators. Unfortunately, such incidents continue to occur, and leaks of personal data from medical institutions, social networks and commercial organizations in Uzbekistan have been observed with alarming regularity for the past 5 years.

According to data provided by DeviceLock in December 2019, about 2% of all cases of leakage of personal data of users in 2019 were carried out through IT specialists. Despite the small number of cases, the damage from such incidents is significant.

Experts, analyzing the organization of the data leakage process, including unloading from access control systems, the presence of service fields in data leaks and the availability of a full backup with a large number of records, came to a sad conclusion about the involvement of system administrators in these illegal actions.

As noted by DeviceLock Technical director Ashot Oganesyan, technological solutions that prevent leaks protect against fraudulent actions of employees of business units, but do not have such effectiveness against IT specialists, especially those with administrator authority. In addition, it is an order of magnitude more difficult to prove the guilt of an IT specialist who has basic concepts of information security than a manager who sells data via Telegram linked to a SIM card under his name[4].

Research shows that almost all major cases of information leakage (over 50 thousand records) occur with the participation and assistance of employees of IT departments.

The problem of personal data protection and cyber security of state structures was discussed at the international conference in Skolkovo in October 2019. Uzbek Prime Minister Abdullah Aripov noted that more than eight million incidents were registered last year alone. To combat this threat, the Government is taking comprehensive measures to protect information, primarily on the websites of various organizations and departments, as well as in financial institutions. Then A.Aripov called on the CIS countries to cooperate more actively and exchange information to improve communication channels and data protection systems.

There is an underestimation of the official statistics of data leaks due to the delay between the incident itself and its detection. Often, companies' information security monitoring systems turn out to be defective, and problems become visible only after the fact of a leak. Experts note that in 2020, the massive shift of employees to remote work and the imperfection of information security systems in some organizations have created favorable conditions for compromising confidential data, and so far not all cases of leaks during

[3] Personal data of 50 thousand Uzbek citizens appeared on the Internet // Sputnik.
URL.: https://uz.sputniknews.ru/20200706/Personalnye-dannye-50-tysyach-uzbekistantsev-okazalis-v-Internete-14479422.html

[4] Leakage of personal data: who leaks confidential information// Sputnik.
URL.: https://uz.sputniknews.ru/20191215/Utechka-personalnykh-dannykh-kto-slivaet-konfidentsialnuyu-informatsiyu-13014194.html

quarantine have become known to the public. This fact is confirmed by statistics, according to which the largest number of cases of information security related to new employees or updating of information systems is random. As a result, the actual number of data leaks in recent years significantly exceeds official statistics, and not all incidents become known to the public.

Studying and analyzing the latest trends in the field of personal data protection, I cannot but dwell in more detail on the case of Cambridge Analytica, which has become one of the most notorious scandals on the topic of personal data leakage. So, what is remarkable and instructive that a detailed analysis of this case can give us?

In December 2016, an investigation was published that mentioned Cambridge Analytica and its influence on the US elections and the Brexit referendum. It turned out that the company used stolen data from social networks, including Facebook, to manipulate public opinion. Subsequently, it was noted that Cambridge Analytica also worked on the Brexit referendum and with Le Pen's political party in France.

It is interesting to note that Cambridge Analytica has a reference to the most famous British university in its name for a reason, because it really has a connection with Cambridge University, where the Center for Psychometry is located. This center studies ways to measure psychological characteristics of a person. Previously, researchers have found that it is possible to measure personality by analyzing the digital footprint that a person leaves on social networks, such as likes, geological data and search queries. One of the scientists, Michal Kosinski, has developed a system that allows you to create a psychological profile of a person based on his digital footprint and data from his social networks. To do this, volunteers from the Internet were involved, who took tests in social networks and on websites – as a reward, and they simply received a description of their psychological characteristics.

The scientist notes that anyone with basic programming skills and access to the Internet can use such methods. He also points out that these methods have huge potential for improving marketing, career planning, psychological assistance and other areas. However, he warns that the same technology can be used against people. He believes that Alexander Kogan, his former colleague from Cambridge University, who later worked with Cambridge Analytica, was familiar with his research and used the methods developed by Kosinski for unethical purposes. Kosinski notes that he has always called for the ethical use of this technology and calls for the development of appropriate policies and procedures.

According to an investigation published by The New York Times on March 17, 2020, the concerns expressed by Kosinski about the ethics of using a new approach to psychometry are confirmed. American journalists found that Alexander Kogan, similarly to Kosinski, set up his model with the help of volunteers who took a special psychological test on the Internet (they were paid money for participation, a total of $ 800,000 was spent), while simultaneously collecting information about their Facebook profiles and their friends' profiles – at that time a social network provided such an opportunity to third-party applications.

Like Kosinski, Kogan assured the participants of the experiment that their data would be used exclusively for research purposes, but this turned out to be a deception. Former Cambridge Analytica employees told The New York Times that thanks to Kogan, the company gained access to the personal data of 50 million Facebook users, which made it possible to effectively customize political advertising.

Here are some examples of the use of psychological profiling during the American presidential election. Analysts have found that different people should present the candidate's opinion on the law on the free distribution of weapons in different ways, depending on their characteristics: people prone to nervousness can present weapons as a guarantee of security, and rich conservatives-extroverts - an image of duck hunting. Alexander Nix, one of the founders of Cambridge Analytica, proudly talked about this method at the Concordia summit for influential politicians and businessmen right during the presidential race.

Another example: residents of the Little Haiti neighborhood in Miami were shown information that Hillary Clinton refused to participate in aid after the earthquake in Haiti, and African Americans were shown a video where Clinton compared black men to animals. In addition, volunteers who worked on the US elections used the company's data, visiting the homes of voters and persuading them to vote for Donald Trump. They knew in advance who lived in each house, and could choose in advance the most effective strategy for persuasion.

According to the information received by journalists, Cambridge Analytica offered its services to the American Democrats, but they did not arouse much interest among those. However, Stephen Bannon, the former head of the conservative website Breitbart and a former adviser to Trump, showed interest and helped raise funding. He also became vice president of the company, although his role remained unofficial, and the amount of his investments, as well as those of the Mercer family, which amounted to only $ 15 million, was not publicly reported.

The results of the investigation caused a scandal affecting many participants in this situation. According to the authors of the article, Facebook representatives knew about the leak of user data and how they would be used. In response to the publication, the social network restricted Cambridge Analytica's access to its data.

It is also worth noting that Cambridge Analytica's activities were in a gray area from the point of view of US legislation, mainly due to the presence of company employees who are citizens of other countries.

However, the main aspect is that the horrors of manipulation using the theft of a large amount of personal information have become a reality, and not just a fantasy of those who are prone to technopessimism.

According to Kosinski's statement, in fact, the significance of the Cambridge Analytica story is not that they helped Trump during the election. He notes that this is just a commercial company that sought to make money. However, the bottom line is that previously, in order to compile a psychological profile of a person, it was necessary to ask him to fill out a questionnaire or take a test, and the subject was aware that his psychological characteristics were being studied. But now you can do the same without revealing to a person that his most personal characteristics are measured and evaluated. Just look at his digital footprint, such as social media posts, likes, browsing history on the Internet and search queries.

According to Kosinski, for the accurate compilation of a psychological profile of a user, it is enough to know only a few pages on Facebook that interest him. Using this data, it is possible to predict the user's answers to psychological test questions even better than his close relative. It is impossible to fight against this: even if you delete your profile on a social network, there will still be a huge digital footprint, which, as the Cambridge Analytica story shows, can not only be used by someone in theory, but is actually already being used now.

Thus, from all of the above, a natural and quite reasonable question arises – what if someone with a large amount of money comes to mind to interfere in the internal politics of Uzbekistan? Countries with enormous economic potential and strategic location are located in the very heart of the continent, located in territorial proximity with the strongest powers of our time – the Russian Federation and the People's Republic of China. Instagram Facebook, Instagram, VKontakte, Telegram, WhatsApp, etc. What if using the same psychological profiling mechanisms and simply transferring a couple of hundred million to the accounts of the managers of the next Cambridge Analytica, this someone, at the behest of a certain political elite, thinks of getting access to the personal data of Internet users from Uzbekistan, no matter through Facebook, Instagram, VKontakte, Telegram, WhatsApp, etc.? What if the consequence of another leak of Uzbek citizens' data is not private cold calls and fraudulent schemes for debiting money from cards of the Uzcard and Humo systems, but whole political machinations and manipulations aimed at rocking political sentiment and creating an unstable political atmosphere? In this case, how to protect citizens, ensure state security and the exercise of rights and freedoms in accordance with international legal norms and customs, given that the concept of state borders is completely erased on the Internet and it will take more than a day or two to detect a real data leak?

All these questions have one thing in common: the answer to them is an easy–to-understand, but difficult-to-implement truth - national and international legislation must constantly evolve as technology develops to meet the changing threats and challenges that constantly arise with technological progress in the field of personal data protection.

The Cambridge Analytica case highlights the need to strengthen regulation and regulatory mechanisms to protect personal data and prevent the misuse of such data in political and other contexts.

REFERENCES:

1. Нугманов Н.А. Формирование международного информационного права: вопросы теории и практики. Монография. – Ташкент: УМЭД, 2018. – 226с.

2. Иванова А.П. Утечка персональных данных: большая проблема в цифровую эпоху. – Москва: Реферативный журнал Государство и право, 2020. - № 4. 100-107с.

3. Швыряев П.С. Утечки конфиденциальных данных: главный враг внутри. МГУ им. М.В. Ломоносова. – Москва: Государственное управление. Электронный вестник, 2022. - №91, 226-241с.

4. «The world's most valuable resource is no longer oil, but data»// The Economist. URL.: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

5. Personal data of 50 thousand Uzbek citizens appeared on the Internet // Sputnik. URL.: https://uz.sputniknews.ru/20200706/Personalnye-dannye-50-tysyach-uzbekistantsev-okazalis-v-Internete-14479422.html

6. Leakage of personal data: who leaks confidential information// Sputnik. URL.: https://uz.sputniknews.ru/20191215/Utechka-personalnykh-dannykh-kto-slivaet-konfidentsialnuyu-informatsiyu-13014194.html