

MASS SURVEILLANCE AND PRIVATE COMPANIES

Sinisa Domazet^{1a}

¹ Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica,
Republic of Serbia, sdomazetns@gmail.com

Received: 26th June 2023

Accepted: 4th August 2023

Review paper

Abstract: *The rapid development of information and communication technologies, in addition to a large number of positive effects, also brings with it certain dilemmas, one of which is the biggest misuse of modern technologies for the purpose of mass surveillance. Practice has confirmed the existence of a large number of examples of mass surveillance around the world. In the paper, attention is paid to mass surveillance by private companies. It was established that private companies participate to a large extent in mass surveillance, either on their own or if they are left to do so by a special decision of public authorities. Some examples of such activities are analyzed in the paper. The normative method was used in the paper, as well as the legal-logical methods of induction and deduction.*

Keywords: *law, security, internet, mass surveillance, private companies*

(introductory lecture of the forum - work by invitation)

1. INTRODUCTION

The extremely fast development of information and communication technologies, and especially artificial intelligence, has brought numerous challenges, and not only positive effects. As one of the main challenges in the modern world, various technologies for mass surveillance appeared, which very quickly entered every pore of people's lives. It can be said that these technologies have caused a double effect. On the one hand, the supporters of these technologies as an argument in favor of their use point out that in this way it is possible to improve the safety of citizens, reduce the number of criminal acts, and in some places these technologies are also used for the purpose of rewarding citizens for positive forms of behavior in society (such as the case with the social credit system in China). On the other hand, there are also numerous negative features of these technologies.

For example, Privacy International states that mass surveillance “include the direct mass interception of communications, access to the bulk communications stored by telecoms operators and others, mass hacking, indiscriminate use of facial recognition technology, indiscriminate surveillance of protests using mobile phone trackers, and more” (Anon, n.d.).

^a ORCID: 0000-0002-5964-2249

Technologies for mass surveillance are very often the reason for mutual accusations between states. In this regard, the criticisms of Western countries directed at China, due to the social credit system based on mass surveillance technologies, which in this way violate the right to privacy and human rights in general, stand out. As Domazet, Lubura, Susak-Lozanovksa and Ilik said “it is not without reason that the mentioned system, which is essentially based on evaluating and ranking the behavior of officials, businesspeople, and ordinary citizens (with rewards and penalties) has become the subject of wide discussions, not only in the scientific and professional circles in China but also around the globe, primarily in the Western world” (Domazet et al., 2021).

Practice shows that mass surveillance is not always and exclusively carried out by states, but that many private companies around the world are increasingly involved in this activity. In the paper, attention is paid to mass surveillance by private companies. It was established that private companies participate to a large extent in mass surveillance, either on their own or if they are left to do so by a special decision of public authorities. The paper will analyze the activity of private companies in terms of mass surveillance, and then some characteristic examples of such behavior will be listed.

2. ACTIVITIES OF PRIVATE COMPANIES IN PERFORMING MASS SURVEILLANCE

The private sector is becoming more and more present in the field of development and use of mass surveillance tools, as evidenced by numerous publicly available data. Thus, there are data according to which “the mass surveillance industry is a multibillion-dollar industry that has undergone phenomenal growth since 2001” (Anon, 2013). The Wall Street Journal reports that “Intelligence agencies in the U.S. and abroad have long conducted their own surveillance. But in recent years, a retail market for surveillance tools has sprung up from “nearly zero” in 2001 to about \$5 billion a year, said Jerry Lucas, president of TeleStrategies Inc.” (Valentino-DeVries et al., 2011). According to Carnegie, “between 2011 and 2023, at least seventy-four governments contracted with commercial firms to obtain spyware or digital forensics technology” (Feldstein & Kot, 2023).

This report also states that “Israel is the leading exporter of spyware and digital forensics tools documented in the global inventory: fifty-six out of seventy-four governments have procured commercial spyware and digital forensics technologies from firms that are either based in or connected to Israel, such as NSO Group, Cellebrite, Cytrox, and Candiru” (Feldstein & Kot, 2023).

According to some reports, such as “the Report "Video Surveillance Market by Offering (Hardware (Camera, Storage Device, Monitor), Software (Video Analytics, VMS), Service (VSaaS)), System (IP, Analog, Hybrid), Vertical and Geography (North America, Europe, APAC, RoW) - Global Forecast to 2027" “The video surveillance market is projected to grow from USD 48.7 billion in 2022 to USD 76.4 billion by 2027; it is expected to grow at a CAGR of 9.4% during the forecast period” (Anon, 2022).

According to the same report, “Major vendors in the video surveillance market include Hikvision (China), Dahua Technology (China), Axis Communications (Sweden), Bosch Security and Safety Systems (Germany), Hanwha Techwin (South Korea), Avigilon (Canada), Teledyne FLIR (US), Honeywell International; (US), Panasonic i-PRO Sensing Solutions (Japan), Pelco (US), Uniview (China), Agent Video Intelligence (US), CP PLUS (India), Genetec (Canada), Huawei Technologies (China), NEC (Japan), NICE Systems (Israel), Qognify (US), Tiandy Technologies (China), VIVOTEK (Taiwan), MOBOTIX (Germany),

Morphean (Switzerland), Verkada (US), Camcloud (Canada), and Ivideon (US)” (Anon, 2022).

Overall, in the last decade, private companies have taken the lead in the field of mass surveillance technologies. This should not be surprising, taking into account the economic profitability of these technologies, the growing demand around the world, and the fact that the existing legal regulations around the world have greatly limited the room for maneuver of states in exercising surveillance over their citizens. The affair surrounding Edward Snowden showed all the dimensions of indiscriminate mass surveillance of American citizens, and beyond. At the same time, this case has fully opened discussions around the world regarding the preservation of the right to privacy and the mechanisms of its protection.

In terms of legal regulation at the international level, the right to privacy has been the subject of attention of the UN Human Rights Council, as well as the UN General Assembly, whereby it was pointed out that “the same rights that people have offline must also be protected online, including the right to privacy” (United Nations General Assembly, 2015). According to Domazet and Dinic, „privacy is also recognized as a human right in the UN Universal Declaration of Human Rights (Art. 12), as well as in the 1966 International Covenant on Civil and Political Rights“ (Domazet & Dinic, 2022).

In Article 8. of the Convention for the Protection of Human Rights and Fundamental Freedoms, one can also observe the important attitude that “everyone has the right to respect for his private and family life, his home and his correspondence”. It is important to note that this Convention foresees the possibility of suspending the right to privacy, but only “when prescribed by law and necessary in a democratic society in the interests of national security, public security or economic well-being, to prevent disorder or crime, to protect health or morals, or to protect the rights and freedoms of others“.

In addition to this convention, the right to privacy is also important in the Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as well as the African Union Convention on Cyber Security and Data Protection.

When it comes to national regulations governing the right to privacy, most states have their own legislation in this area, where the right to privacy is guaranteed by the constitution in some places, and in some by criminal legislation. Also, in many countries there is special legislation related to the protection of personal data (including Serbia), but there are still countries "where the right to privacy is not recognized as an autonomous right (for example, in the United Kingdom and China)" (Domazet & Dinic, 2022).

Whatever the regulations governing the protection of personal data, i.e. the right to privacy, the fact is that the practice of mass surveillance of citizens in itself causes numerous controversies. On the one hand, there are supporters of the practice of mass surveillance of citizens, who justify it by the need to protect national security from all threats, including terrorist attacks. To this end, it is considered a lesser evil to violate the applicable regulations and some rights of citizens (including the Right to privacy), compared to the danger that is avoided in this way. A typical example is the famous Patriot Act in the USA, passed after the events of September 11, 2001, which provided for surveillance and the possibility of eavesdropping on citizens by security agencies (especially the FBI and NSA), without the prior approval of the judicial authorities. At the same time, this applied to all citizens, not only those

who represent a real security threat to the US, thus legalizing the indiscriminate surveillance of citizens. Practically, the legal regulation that required a court order to be obtained in order to collect sensitive data about citizens was called into question. This was particularly contributed by the rapid development of information and communication technologies and the development of new surveillance technologies, which only made the work of the services easier and made their activities, especially abuses, even less visible than before. It can be argued without exaggeration that services or other bodies that carry out surveillance could practically collect citizens' data without fear of legal consequences and sanctions.

On the opposite side are bitter opponents of the practice of mass surveillance, who believe that mass surveillance must not be allowed under any circumstances, given that it has been shown that in this way the guaranteed human rights of citizens are violated, but also the foundations of modern democratic states are violated. The case of Edward Snowden only gave them a "wind at their backs".

When it comes to practical examples of the actions of private companies in mass surveillance, the famous case of the Pegasus spyware, developed by the Israeli NSO group, should be mentioned. The mentioned software caused a real scandal around the world. It turns out that several member states of the European Union have acquired this software for tracking citizens' mobile phones, under the pretext of preserving national security and fighting terrorism.

According to the media, this is "an advanced type of spyware, that is, a tool used for deep infiltration, primarily in mobile devices, whether they run on Android or EOS Apple's operating system. The possibilities of 'Pegasus' are truly enormous [...] you can access the most diverse content in the phone, practically everything from messages, video content, photos taken, contacts, and the like" (Anon, 2022).

It was the same with the Predator software, which turned out to be even more dangerous than Pegasus. According to open sources, "Predator and its Alien loader have been around since 2019 and are part of a suite of mobile spyware sold by Intellexa." The software, which is designed to spy on and extract data from devices it has entered, is available for Google Android and Apple iOS... This includes recording audio from phone calls and VoIP apps, stealing data from Signal, WhatsApp and Telegram, and even hiding applications or preventing them from starting after the device is restarted" (Anon, 2023).

The above examples clearly show that mass surveillance technologies are increasingly sophisticated and dangerous, and countries around the world are increasingly turning to private companies to ensure the procurement of the latest technological solutions.

3. CONCLUSION

On the basis of what has been said, it can be concluded that the development of modern technologies carries with it a great danger of abuses of various kinds, where one of the most dangerous forms is certainly the practice of mass, indiscriminate surveillance. The affair surrounding Edward Snowden showed all the extent of the misuse of modern technologies for the purpose of mass surveillance. The available data show the existence of a large number of different examples of mass surveillance around the world, with the state and its organs in the foreground. If the practice of the European Court of Human Rights is analyzed, it can be seen that international institutions understand the concept of privacy very broadly, which is an expression of special concern for the preservation of this right.

In this regard, a large number of court decisions that have been made in recent years are very significant, because based on them specific principles have been set when assessing the legality of limiting the right to privacy. This, first of all, refers to the conditions under which state

security authorities can undertake acts of mass surveillance of citizens. Second, acts of mass surveillance must be carried out extremely selectively and proportionally, which implies that the guaranteed human rights of citizens are violated to the least extent possible. Therefore, if it is shown that the goal of surveillance could be achieved by less restrictive methods, in terms of limiting human rights, then the activity of state authorities will not be legal. Finally, a particularly difficult problem is and will be the control of mass surveillance activities (primarily intelligence services) and the protection of the right to privacy. There are numerous discussions on this issue in the world, and independent supervisory bodies have been formed in many countries in order to protect the right to privacy.

In fact, surveillance in itself should not be a problem if it is carried out in accordance with the regulations and based on the approval of the competent authorities. The research showed that it is not only the states that carry out direct mass surveillance with the help of technologies that they have developed themselves, but it is increasingly done through other entities that are not under direct or indirect state influence.

Private companies have proven to be very inventive in the mass surveillance technology market, and revenues from this activity are growing year after year. Also, there is a noticeable growth in the number of these companies around the world, which shows how lucrative mass surveillance has become. Research has shown that private companies participate to a large extent in mass surveillance, either on their own or if they are left to do so by a special decision of public authorities. Therefore, private companies represent a convenient "screen" for activities that the state would not want to be publicly disclosed, given that all state activities (especially those in the field of security) are under the watchful eye of the public.

The presented examples show all the dangers of modern technologies, developed by private companies. Unfortunately, these are only examples that have reached the public. A major problem is the insufficient amount of data regarding the relationship between states and private companies regarding the development of mass surveillance technologies. This cooperation is often shrouded in secrecy, which is regularly justified by the need to preserve national security, while the information about it is marked with the appropriate level of secrecy.

Due to all of the above, the adoption of new or improvement of existing legal regulations, which will protect the right to privacy and other guaranteed rights of citizens in a more efficient way, is of key importance in the future. Practice shows that it is very difficult, due to conflicting interests between states, great resistance to civilian control of intelligence services, insufficiently developed mechanisms for controlling the work of private companies in the field of developing technologies for mass surveillance.

REFERENCES

Anon. (2013). Mass surveillance industry, Available from https://en.wikipedia.org/wiki/Mass_surveillance_industry Accessed: 2023-June-16

Anon. (2022). Markets and Markets, Available from <https://www.marketsandmarkets.com/PressReleases/global-video-surveillance-market.asp> Accessed: 2023-June-16

Anon. (2022). Zurnal, Available from <https://zurnal.me/sto-sve-mogu-pegaz-i-predator/> Accessed: 2023-June-16

Anon. (2023). Informacija. Available from <https://www.informacija.rs/Mobilni-telefoni/Predator-je-komercijalni-spijunki-softver-i-mnogo-je-opasniji-nego-sto-se-mislilo.html> Accessed: 2023-June-20

Anon., (n.d). Mass Surveillance, Available from <https://privacyinternational.org/learn/mass-surveillance> Accessed: 2023-June-15

Domazet, S. Dinic, S. (2022). International Legal Aspects of Mass Surveillance and Implications on Privacy, *Culture of Polis*, 19(1), pp. 79-97, ISSN (online) 2812-9466

Domazet, S. Lubura, M. Susak-Lozanovska, I. Ilik, N. (2021). Chinese Social Credit System: New Challenges for the Right to Privacy?, *Journal of Liberty and International Affairs*, 7(3), p. 138, ISSN 1857-9760

Feldstein, S. Kot, B. (2023). Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses Available from: <https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229> Accessed 2023-June-16

United Nations General Assembly (2015). The right to privacy in the digital age: resolution, s.l.: United Nations.

Valentino-DeVries, J., Angwin, J. & Stecklow, S (2011). Document Trove Exposes Surveillance Methods, Available from <https://www.wsj.com/articles/SB10001424052970203611404577044192607407780> Accessed: 2023-June-16