VOL. 63 STUDIA POLITOLOGICZNE
DOI: 10.33896/SPolit.2022.63.6



*Marek Górka*[*]

# The Importance of Surveillance in the Context of Contemporary Threats: Based on the Experience of the Terrorist Attacks of 11 September 2001



***Keywords:*** *security policy, terrorism, counterterrorism, freedom, coronavirus*

***Abstract:*** *The main objective of security policy is to prevent threats, which means to fight certain phenomena at their very source. Governments of many countries threatened by a terrorist attack are still searching for an effective way to prevent attacks on intended terrorist targets and to uncover them in time. It is now recognised that monitoring telephone and internet communications is one of the most effective ways to combat terrorism.*

*In recent years, international security has become one of the most debated issues due to, among other things, the coronavirus pandemic and numerous terrorist attacks. An important factor in preventing these threats is how the state and its services function through the use of a variety of tools and techniques, thus creating new and unique ethical and legal problems. The force and impact of state policy measures are often excessive and disproportionate to the threats posed. In this case, civil rights and liberties are most often violated. Doubts that arise when analysing these two values also stimulate reflection on the question to what extent the state is the victim of threats and to what extent it itself is the aggressor.*

*Contemporary threats such as terrorism or the coronavirus pandemic are a major source of public fear that has far-reaching implications for public governance. The analysis carried out in this study examines the use of digital technologies for surveillance and control of the public by governments as a means to combat contemporary threats. The article describes both cases highlighting the importance of digital technology in maintaining security and cites evidence showing the threats that electronic surveillance poses to democratic norms.*

[*] ORCID ID: https://orcid.org/0000-0002-6964-1581. Research Fellow in the Humanistic Department of the Koszalin University of Technology. E-mail: marek_gorka@wp.pl

*In other words, digital control over society promotes security but also restricts civil rights and liberties. The article emphasizes the worrying tendency for governments to implement technology rapidly without sufficient concern for the consequences for socio-political life.*

## Introduction

Current debates on surveillance demonstrate the complexity of political solutions whose uncertainties and moral ambiguities make it difficult to achieve a normative consensus. In this context, numerous questions arise about how to analyse political controversies, their sources and their consequences on public discourse. The search for an answer to this question remains a challenge for researchers investigating security policy, among other things[1].

Research in the field of security policy has begun to focus on political disputes and disagreements around government control and its impact on changing practices in everyday life[2]. However, the practices of (de) legitimisation have, up to now, not been the subject of sufficient analysis.

In the 21st century, when international terrorism is widely recognised as a major threat, democratic governments seem increasingly determined to take tougher measures against it. However, a major challenge then arises, namely: on the one hand, what measures to take to combat terrorism effectively, and on the other, how to preserve fundamental human rights and individual freedoms. Creating an appropriate legal framework to support an effective battle against terrorism while respecting fundamental human rights and individual freedoms constitutes a difficult challenge for democratic states. The ways in which contemporary threats can fuel democratic decline or stimulate democratic resilience remain under-researched[3].

The rise and widespread acceptance of state surveillance after the 9/11 attacks has received much analysis in the literature on security policy. The control of political regimes exercised through secret services such as the NSA and CIA was largely uncontested or deemed uncontro-

---

1 Ch. S. Ochoa, F. Gadinger, T. Yildiz, *Surveillance under dispute: Conceptualising narrative legitimation politics*, «European Journal of International Security» 2021, No. 6/2, pp. 210–232.

2 M. Cayford, W. Pieters, *Effectiveness fettered by bureaucracy: why surveillance technology is not evaluated*, «Intelligence and National Security» 2020, Vol. 35/7, pp. 1026–1041.

3 A. Huq, *Terrorism and Democratic Recession*, «University of Chicago Law Review» 2018, No. 85, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2974006 (23.09.2021).

versial in the public discourse until these facts were revealed by WikiLeaks and Edward Snowden in 2013. Since then, the question still remains as to whether a more closed society that rejects or restricts such liberal democratic values be better able to defend itself against terrorism.

Today, the role and importance of surveillance for the functioning of democratic rights is a more frequently encountered topic of discussion. Therefore, one of the objectives of the analysis undertaken is to confront the following research question: What are the main directions of countering terrorist threats while trying to preserve the existing norms of a democratic state and society? And how can counter-terrorist actions based on surveillance tools affect the functioning of democratic states?[4]

The existing literature on political science has already extensively described the ways and tools of controlling society in times of crisis, especially in the context of terrorist threats[5]. The analysis conducted here aims to answer the question whether the use of advanced technologies in the field of intelligence and information gathering increases security and prevents the possibility of a terrorist attack in democratic societies, with the main focus placed on the United States. The aim of this paper is also to systematize existing research on the application of surveillance methods to deal with public threats, which at the same time pose a challenge to democratic governance. This paper also presents current research analyses relating to state control in the context of the COVID-19 pandemic[6], thus making it possible to outline future directions for research and reflection on digital control vis-à-vis civil liberties.

---

4 V. Stam, *The 9/11 Generation: Youth, Rights, and Solidarity in the War on Terror*, «Surveillance & Society» 2018, No. 16/1, pp. 137–139.

5 D. M. McLeod, D. V. Shah, *News Frames and National Security*, Cambridge University Press 2014; R. Levinson-Waldman, *NSA Surveillance in the War on Terror*, [in:] D. Gray, S. E. Henderson (eds.), *Cambridge Handbook of Surveillance Law*, Cambridge University Press 2017, pp. 7–43; L. Melgaço, J. Monaghan (eds.), *Protests in the Information Age: Social Movements, Digital Practices and Surveillance*, Routledge, London 2018; D. Kostakopoulou, *How to do Things with Security Post 9/11*, «Oxford Journal of Legal Studies» 2008, Vol. 28/2, pp. 317–342; S. Le´onard, *Border Controls as a Dimension of the European Union's Counter-Terrorism Policy: A Critical Assessment*, «Intelligence and National Security» 2015, Vol. 30/2–3, pp. 306–332; J. Monaghan, *Performing counter-terrorism: Police newsmaking and the dramaturgy of security*, «Crime Media Culture» 2020, pp. 1–19.

6 S. Ch. Greitens, Surveillance, *Security, and Liberal Democracy in the Post-COVID World*, «International Organization» 2020, Vol. 74/1, pp. 169–190; J. H. H. Weiler, *COVID, Europe, and the Self-Asphyxiation of Democracy*, [in:] M. Poiares Maduro, P. W. Kahn (eds.), *Democracy in Times of Pandemic*, Cambridge University Press 20202, pp. 141–152; P. Genschel, M. Jachtenfuchs, *Postfunctionalism reversed: solidarity and rebordering during the*

In undertaking the analysis of the actions applied by governments against the above-mentioned threats, the comparative and systemic methods are used. A research perspective chosen in this way allows for a better understanding of the dilemmas concerning security measures taken in order to minimize terrorist threats on the bases of the Polish and American legal systems. The case of the use of biometric data by institutions in the public space in order to reduce the COVID-19 pandemic is also considered. In this context, an attempt is made to indicate similarities in the use of tactics by the states in the face of contemporary threats, which are a continuation of the process of surveillance already known from the field of counterterrorist activities.

The main thesis of the article is that digital technologies have gained considerable attention at all political levels in various countries, despite their questionable, if not harmful, effects when implemented in response to contemporary threats. In many countries, digital technologies have become a key component of public safety procedures. Based on a description of their application to specific threats, the article explains how technology has been interpreted as a means of implementing security policy.

## Securitisation – as a starting point for security policy

One of the main theses of the article is that today the dimension of threats has increased on an unprecedented scale both in the domestic and international arena. Terrorist attacks have dramatically increased security concerns, a phenomenon which has further problematised security policy in many of its dimensions. In short, the 9/11 attack is seen as both a critical moment and a major accelerator of the securitisation of terrorism in Europe and the United States.

Political elites have conducted a series of deliberate, sustained campaigns to convince the public that terrorism is a pervasive threat to state security, one which requires the urgent implementation of extraordinary policy measures. Such securitisation discourse is deliberately intended to facilitate the transfer of threat issues from the realm of conventional politics to crisis politics, in which the identified problem can be addressed outside of the normal political procedure. In other words, political elites

*COVID-19 pandemic*, «Journal of European Public Policy» 2021, Vol. 28/3, pp. 350–369; T. Lee, H. Lee, *Tracing surveillance and auto-regulation in Singapore: 'smart' responses to COVID-19*, «Media International Australia» 2020, Vol. 177/1, pp. 47–60.

who operate in a liberal-democratic environment need to gain public approval in order to introduce emergency measures to counter a specific threat. Moreover, securitisation has enhanced the process of collective and political consolidation, generating greater loyalty to the government and patriotism through the definition of a common threat[7].

Until 11 September 2001, many countries, including the United States, defined terrorist acts as criminal offences. However, after this event terrorism began to be treated as an act of war or as a crusade. Thus, Prime Minister Tony Blair refers to al-Qaeda attacks in messianic terms, describing them as "This mass terrorism is the new evil in our world today. It is perpetrated by fanatics who are utterly indifferent to the sanctity of life and we, the democracies of this world, are going to have to come together and fight it together and eradicate this evil completely from our world"[8].

A similar tone is maintained by President George W. Bush who stated that the war on terror "will be a monumental struggle of good versus evil"[9] stressing that the former will undoubtedly prevail. As can easily be seen, all three definitions refer to the phenomenon in messianic terms and refer to the need for security usually manifested by individuals.

Americans generally supported the policies pursued by the George W. Bush administration with regard to the protection of the United States, including the subsequent decision to go to war in Afghanistan and Iraq as part of the 'Global War on Terrorism'[10] Bush also stated that this kind of war would include invisible measures, pointing to the kinds of measures needed to prevent and pre-empt terrorist threats, including warrantless wiretaps and bulk data collection[11]. Even after the failed identification of Weapons of Mass Destruction (WMD) in Iraq, Bush was re-elected as US President in 2004, meaning that his counter-

---

[7] Ch. Boswell, *Migration, security, and legitimacy: some reflections*, [in:] T. Gives, G. P. Freeman, D. L. Leal, (eds.), *Immigration Policy and Security: U.S., European, and Commonwealth Perspectives*, Routledge 2009, p. 94.

[8] *Tony Blair, Statement at the Trade Union Conference on the 9/11 Attacks*, 11 September 2001, http://www.americanrhetoric.com/speeches/tblair9-11-01.htm, (23.09.2021).

[9] A. J. Bacevich, E. H. Prodromou, *God is not Neutral. Religion and US Foreign Policy after 9/11*, «Orbis» 2004, No. 48/1, pp. 43–54.

[10] H. Criado, *What Makes Terrorism Salient? Terrorist Strategies, Political Competition, and Public Opinion*, «Terrorism and Political Violence» 2017, No. 29/2, p. 199.

[11] B. L. Nacos, Y. Bloch-Elkon, R. Y. Shapiro, *Prevention of Terrorism in Post-9/11 America: News Coverage, Public Perceptions, and the Politics of Homeland Security*, «Terrorism and Political Violence» 2007, No. 20/1, p. 2.

terrorism strategy, even with all its failures, was much better received than a possible subsequent terrorist attack.

This approach, using the concept of the War on Terror, has thus allowed for, among other things, an expansion of the scope of powers of state institutions and services, all of which is intended to effectively counter and deter potential attackers. The NSA data collection programmes that were introduced under George W. Bush continued under Barack Obama (when he took office in 2009), along with other controversial anti-terrorism programmes, such as the use of drones to kill suspected terrorists abroad, including US citizens[12].

Feelings of insecurity and fear thus became an element that creates public discourse. The sense of threat and instability subsequently served to legitimise a package of laws regulating various forms of counter-terrorism, while upsetting the balance between possible threats and civil rights.

## The limits of surveillance in the example of the Patriot act and the Freedom act

Still unchanged, twenty years after the 9/11 attacks, is the commitment of states to establish a democratic, adequate and effective legal framework to combat terrorism. This process should take place through the application of rules that do not harm fundamental human rights and that impose the least possible restrictions on civil liberties.

A watershed moment in the area of counter-terrorism regulation, and in some ways a source of inspiration for many countries, was the Patriot Act, passed immediately after the 2001 attacks in the United States without public debate. The Patriot Act of 2001 was based on the little-known Foreign Intelligence Surveillance Act of 1978 (FISA) aimed at overseeing applications for surveillance warrants against foreign spies in the United States by federal law enforcement and intelligence agencies. It concerned surveillance by intelligence agencies of non-US citizens. An expanded 2001 law already covered US citizens.

[12] M. Mazzetti, C. Savage, S. Shane, *How a U.S. citizen came to be in America's cross Hairs*, «New York Times» 9 March 2013, http://www.nytimes.com/2013/03/10/world/middleeast/anwar-al-awlaki-a-us-citizen-in-americas-cross-hairs.html?pagewanted=all&_r=0, (23.09.2021).

Under Section 215 of the USA Patriot Act, both law enforcement and intelligence agencies applied "new countermeasures" to the threat of terrorist attacks occurring within the United States[13]. In October 2001, the NSA, under the leadership of Michael Hayden, used its new capabilities to commence "warrantless wiretapping of international communications both to and from American citizens"[14].

The Act caused much controversy and allegations of violating the US Constitution. Analysts have noted that the Patriot Act violates many constitutional provisions, including the First Amendment to the Constitution[15]. This proclaims that: "Congress shall make no law respecting an establishment a religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances"[16]. The right of expression and association guaranteed by the First Amendment demonstrates the extreme difficulty of reconciling civil liberty with secret service surveillance of groups considered to be extremist and of expressions of views articulated both in public forums and in cyberspace[17].

The surveillance that enveloped American society also directly violated the Fourth Amendment, which states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"[18]. The Patriot Act provides for searches to be conducted without a warrant on the basis of probability and suspicion

---

13 R. W. Williams, *Terrorism, anti-terrorism and the normative boundaries of the US polity: The spatiality of politics after 11 September 2001*, «Space and Polity» 2003, No. 7/3, p. 285.

14 J. Bamford, *The Shadow Factor: The Ultra Scret NSA from 9/11 to the Eavesdropping on America*, Anchor Books 2008, p. 118.

15 S. B. Bhattacharya, *Of Democracies, Wars and Responses to War: A Comparative Perspective on War and Security in India and the United States*, «India Quarterly: A Journal of International Affairs» 2013, No. 69/3, pp. 211–227.

16 *The Constitution of the United States of America*, http://libr.sejm.gov.pl/tek01/txt/konst/usa.html, (23.09.2021).

17 The American Civil Liberties Union (ACLU), on the other hand, believes that the program is a massive breach of privacy, with no significant contribution to the fight against terrorism, available at *La «surveillance généralisée» de la NSA jugée illégale*, http://www.lefigaro.fr/secteur/high-tech/2015/05/07/32001-20150507ARTFIG00292-la-surveillance-generalisee-de-la-nsa-jugee-illegale.php, (23.09.2021).

18 *The Constitution of the United States of America…*

that a particular person has committed an offence. Another allegation concerned violations of the Fifth and Sixth Amendments, which related to the legal rights of defendants and the provision of testimony when facing criminal prosecution. In this case, the main allegation concerned the secret detention of people without charge or trial[19].

The main argument of critics of the Patriot Act was that it restricted individual liberty. Supporters, on the other hand, argued that it was difficult to strike the right balance between security and freedom in such a dangerous international reality[20]. The Patriot Act has come to play a symbolic role in the debate about whether the confidentiality of information stored in cyberspace can be sufficiently guaranteed. Moreover, laws governing electronic surveillance cannot be interpreted unilaterally, as is often the case. The Patriot Act is also a good example of an anti-terrorism law containing many domestic safeguards, such as cyber-surveillance, which helps to ensure security. In addition, the act has played a key role in breaking down barriers between different law enforcement agencies, making information sharing more efficient[21].

The Patriot Act thus not only concerns counter-terrorism, but also covers data collection. The NSA has collected and stored nearly two billion emails, phone calls and other information of an everyday character[22]. However, one may say little about how often the US government has actually used the powers described. This is partly due to the nature of clandestine programmes, which provide little information on whether the NSA's powers under the Patriot Act were useful in marginalising the phenomenon of terrorism[23].

After the United States' surveillance programme was publicly exposed by Edward Snowden, a protracted debate led to its rejection by the US Congress and the Obama administration. The Patriot Act was replaced by the Freedom Act of 2015 with a programme that placed new

---

19 M. Brzezinski, *Fortress America: On the front lines of Homeland Security: An inside look at the coming surveillance state*, Bantam 2004, p. 68; J. Marrs, *The terror conspiracy: Deception, 9/11 and the loss of Liberty*, Disinformation 2006, pp. 303–304.

20 D. L. Hudson, *Debate on Patriot Act and First Amendment continues*, «Bismarck Tribune» September 11, 2011, p. 6.

21 B. J. Goold, *Privacy, Identity and Security*, [in:] B. Goold & L. Lazarus (eds.), *Security and Human Rights*, Portland 2007, pp. 45–72.

22 G. A. Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, «Loyola Law Review» 2014, No. 59, pp. 863–867.

23 *Let a little sunshine in*, «The Economist» http://www.economist.com/blogs/democracyinamerica/2015/06/patriot-act-0, (23.09.2021).

restrictions on the bulk collection of telecommunications metadata by US intelligence agencies, including the National Security Agency. It also reinstated authorization requirements for the establishment of wiretaps on those suspected of terrorist activities.

However, this limited programme was abandoned in 2019 when it was found to be impossible to implement. The trajectory of the programme and the decision to terminate it was based on a cost-benefit analysis. As a bulk data collection programme, the so-called 'Section 215' programme presented the most advanced capabilities in terms of levels of intrusiveness, as it also collected data on individuals who were not in any way suspected of being linked to terrorism.

Both the Patriot Act and the Freedom Act were created in a unique situation, the former immediately after the terrorist attacks, as a reflection of public sentiment resulting from a sense of imminent danger, the latter as a result of unauthorised disclosures of the actions of the US government and its subordinate services.

## Surveillance technology and public security in the face of COVID-19

Maintaining a balance between security and the nature of democracy has been a topic of great debate in the twenty years that have passed since the attacks of 11 September 2001. Today's threats – such as terrorism – also force one to redefine the tools used in terms of the kind of privacy that societies need and are willing to sacrifice for their collective security[24].

As governments around the world race to contain a pandemic, many are deploying digital surveillance tools to exercise social control in order to determine, among other things, which people should be quarantined or allowed to enter public places. What the surveillance of society has demonstrated has become a turning point for the evolution of modern reality, in which everything is collected, recorded and processed. In the new surveillance carried out with the help of information technology, the mere logging in to online accounts, the use of ATM cards or the use of mobile phones entails the processing of huge amounts of data.

[24] D. E. Tromblay, *Botching Bio-Surveillance: The Department of Homeland Security and COVID-19 Pandemic*, «International Journal of Intelligence and CounterIntelligence» 2022, Vol. 35/1, pp. 164–167.

It is also worth noting that twenty years after 9/11, there has also been a change in the another dimension of the nature of surveillance. While the traditional view points to a distinction between the organisation conducting the surveillance and the object (person or group), in the new use of surveillance the vectors have been reversed and the dominant position can be gained by the individual, for example when ordinary citizens photograph government officials in situations of abuse of power. It is also worth noting that, thanks to new technologies, surveillance can be carried out from remote locations.

Modern surveillance is also carried out not only by visualisation, i.e. observation, but also by means of other data recorders, detecting one's movement, sounds, or even temperature. Technological advances in surveillance allow not only the collection of traditional data by administrative entities and related institutional settings, but also enable the collection of information using multiple sources, such as social networks and location systems[25].

The current fight against a global pandemic through the introduction of multiple digital surveillance measures that have been introduced in the interest of public health, with little international oversight[26] may permanently open up opportunities for more invasive forms of surveillance. This phenomenon is in some ways similar to the experience after the terrorist attacks of 11 September 2001, both in terms of state surveillance activities and the public perception of threat. In other words, there are certain similarities between terrorism and pandemics as it turns out that both threats are unpredictable and determine the daily lives of citizens and, therefore, the public space. Being in a crowd in both cases carries risks and implies danger. As both threats are also not fully known, they are difficult to control, a phenomenon which increases the sense of fear in society even more[27].

In terms of the technological response of many governments to the coronavirus outbreak, there has been a proposal to use apps to track the spread of the virus despite questions about the effectiveness of the

---

[25] L. Costa, *Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection*, Namur: Springer 2016, p. 175.

[26] N. Singer, C. Sang-hun, *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, «New York Times», https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillancetracking-privacy.html, (23.09.2021).

[27] S. Erlanger, *The Coronavirus Inflicts Its Own Kind of Terror*, «New York Times», https://www.nytimes.com/2020/04/06/world/europe/coronavirus-terrorismthreat-response.html, (23.09.2021).

technology, privacy safeguards and compatibility with democratic principles. Hence, in the reality of the 2020 pandemic, citizens in many countries, possessing a wealth of experience of counter-terrorism threats and expressing much greater sensitivity to freedom, have become more cautious or distrustful of a smartphone tracking app that would inform people if they came into contact with an infected person.

Terrorist threats have made surveillance, especially in highly digitally advanced countries such as the US, based on biometrics, which allows for the collection of data such as DNA, fingerprints, voice patterns, iris patterns, facial features, which are then digitally processed. Technological ventures in security policies, databases, digital passports and visas, the inclusion of biometrics in documents and computer records are gaining popularity. The Bush administration pioneered the launch of the Smart Borders programme, which was later copied by the European Union (the Smart Borders package was presented by the European Commission in February 2013, and further described in Regulation 2017/2226 – Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States[28]. The stated aim was to identify suspicious persons or cargo (e.g. terrorists and their weapons), while facilitating the rapid entry of legitimate goods and travellers.

Responding to the challenge of terrorism, the United States has attempted to strengthen its understanding of the cross-border movement of people through the use of technology in its border management policy. In this context, it is worth mentioning that the 'Automated Target System' programme was used by the US Department of Homeland Security as a border control measure. The project involved conducting research to select specific sensors that capture video images, audio recordings, cardiovascular signals or respiratory measurements. This led to measurements being taken to determine whether the physical, physiological or behavioural characteristics of an observed person could be an indicator and, at the same time, a harbinger of a real threat.

[28] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R2226, (23.09.2021).

In this context, surveillance means the act of identifying a person, i.e. establishing, for instance, that a passenger is the person they claim to be. This is usually a process of comparing the biometric data of an individual with multiple biometric templates stored in a database. Such a procedure can be used when authorities aim to identify criminals or potential criminals among passengers by comparison with a list of suspects. The Chinese government has recently started using technologies such as facial recognition and artificial intelligence to identify and track 1.4 billion people[29].

This use of biological traits in biometric systems has proved popular in the reality of the coronavirus pandemic, in which, according to the German Robert Koch Institute, almost 90% of COVID-19-infected individuals in China were diagnosed with fever by screening for it using a new camera that measures body temperature with a high degree of accuracy. This proved to be an effective tool for preventing virus transmission[30]. In summary, the benefits of biometric technology often cited by experts increase efficiency in both time and accuracy of subject profiling[31].

Biometric data is a unique identification instrument that, like traditional identity cards, can pose a risk of theft and thus can be one of the tools employed in terrorist attacks. On the other hand, the collection and transformation of a person's physical characteristics into digital data may become an element of violation of a citizen's integrity, including his or her privacy.

In 2020, due to the coronavirus pandemic in the United States, White House officials were in talks with Google, Facebook and other technology companies about the potential use of location data captured from mobile phones to attempt surveillance of the spread of the virus in society. The pandemic has also created fertile ground for greater use of technology services as a substitute for social contacts.

Moreover, companies with growing demand for their digital services pushed for deregulation or other government action that would benefit

---

[29] P. Mozur, *Inside China's dystopian dreams: A.I., shame and lots of camera*, «New York Times», https://www.nytimes.com/2018/07/08/business/china-surveillancetechnology.html, (23.09.2021).

[30] Ch. Burt, *Fever detection technology added to biometric hardware by Dermalog, Telpo, DFI, Hikvision and Kogniz*, «Biometric update», https://www.biometricupdate.com/202004/fever-detection-technology-addedto-biometric-hardware-by-dermalog-telpo-dfi-hikvision-and-kogniz (23.09.2021).

[31] M. O. Enerstvedt, *Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles*, Springer, 2017, p. 213.

them, arguing that this would improve the response to the pandemic. Just weeks before the virus swept the US, groups representing Google, Facebook and Twitter already wanted California's attorney general, Xavier Becerra, to wait until 2021 to enforce the state's new privacy rules. The law, known as the California Consumer Privacy Act, requires companies to give people access to a copy of the data collected on them, as well as the ability to delete it. Such companies have complained that the legislation places too many obligations on them[32].

It can be surmised that currently government agencies in many countries including the US, are introducing or considering a range of tracking and surveillance technologies designed to control the rapidly spreading coronavirus, while testing the limits of privacy. Raising concerns about ubiquitous control in a pandemic environment is reminiscent of public fears in the period just after the 9/11 attacks. Increasingly effective digital technology and a lack of government oversight have each time raised suspicions that policymakers are exploiting new means of social control.

In conclusion, the question of striking the right balance between privacy and security is of great importance for the degree of democracy to be enjoyed. The opposition of these two values displays a special presence in the public discourse usually in extreme moments, when the threat is felt directly by citizens, or when it goes unnoticed by public opinion and is pushed to the margins of life in society.

In states of emergency, such as the threat of a terrorist attack or a coronavirus pandemic, the governments of many countries reach for broader powers, claiming access to among other things, location data from telecommunications operators or from Google, which has access to more precise data belonging to Android and Google Maps users.

The challenge for policymakers is to strike a balance between deploying technology and keeping data secure in cyberspace, as with adapting digital tools to crisis situations. In this context, it is crucial that governments are transparent about the technology they use and provide adequate safeguards for consumers.

[32] M. Kołodziejczyk, *Technológia služiaca na zadržiavanie koronavírusu: potenciálne hrozby pre ochranu ľudských práv*, «Medzinárodné Vztahy» 2020, No. 18/2, pp. 156–181.

## Technology as an agent of security policy change

Today's public space can be characterised by the dynamic pace of change occurring in every dimension of life in which human beings function. Global economic and political conditions, the technological infrastructure, and socio-cultural development all contribute to revolutionary processes in the management of information systems in the areas of business, administration, the military, and every other political and social space. The economic, political, military, as well as cultural and social spheres of life are becoming increasingly globalised and interconnected, and are heavily dependent on automated systems to deliver traditional resources to citizens.

This global interaction of information, people, goods and services is based on communication in cyberspace. Thus, traditional state institutions such as public offices, political organisations, economic institutions, educational institutions, security services are increasingly vulnerable to changes in cyberspace. This fact leads to an increasing scale of threats, whose instrument is technological progress, which is a natural domain of human activity and from which it is impossible to escape. Deliberate human activity against public order, in the form of the activities of hackers, spies, terrorists or criminal organisations, is based on the use of global information resources. The aim of such individuals is to cause the greatest possible damage to the interests of the state for political, religious, economic or military reasons. It is important for the security of the state to have information. The search for trade secrets, financial secrets, technological secrets or other proprietary data is an essential condition for carrying out fraud, identity theft or other crimes. As the security of many states is fully dependent on information technology and their information infrastructure, research analysis in this area is crucial for one's protection in this new era of interconnectedness and global interdependence.

Modern society's dependence on cyberspace, technology and information in everyday life has increased at an astonishing rate. The turn of the 20th and 21st centuries has seen the availability and integrity of information systems become a common standard in many countries. The growing global economic dependence on cyberspace is undeniable. Careful reflection on state policy is therefore required, particularly in the use of technology in relation to information retrieval. Technology was intended to cure the state of all the problems plaguing the modern democratic system. The Internet has enabled cheap and easy access

to a virtually unlimited world of information. In a way, technology has become a kind of remedy for apathy, ignorance or citizen alienation. Although it is difficult to say unequivocally whether this goal has been achieved, the modern user possesses all the means at their disposal to be fully informed and involved in ongoing world events.

According to the researchers, the tension that most people experience is not related to the conflict between security and freedom, but to maintaining one's privacy while benefiting from the flow of information. Although they point out that broad access to information supports democratic decision-making, this is only a half-measure. Of much greater importance is the ability to organise online human communities to interpret and use information for public purposes. According to researchers, the active involvement of citizens in public life, through informed expression and discussion, has the potential to revitalise democracy[33].

Technology has the potential to foster social dialogue, provides opportunities for access to information and can be used for surveillance and control. Thus, the mediation of personal data can help to identify specific groups in society. It is worth noting in this context that the cost of acquiring information thanks to the technological revolution is much cheaper, making it easier to build databases on specific individuals.

When studying the functioning of contemporary democratic systems, it is impossible to ignore one of the most fundamental rights and values citizens possess, namely privacy. A number of research analyses dealing with the relationship between privacy and surveillance and security inevitably focus on the perspective of the citizen. Here, too, scholars formulate the question: is it possible to achieve security by giving up one's civil liberties?[34] Currently, all types of communication systems, can be seen as a risk to privacy due to the ability of security services to gather information[35].

Private companies and government agencies collect huge amounts of data on various aspects of citizens' health, finances and habits – much of it also used for commercial purposes. Many security organisations are constantly looking for ways to secure this type of information in order

[33] G. Lidén, *Technology and democracy: validity in measurements of e-democracy*, «Democratization» 2015, No. 22/4, pp. 698–713.

[34] M. Friedewald, J. P. Burgess, J. Cas, R. Bellanova, W. Peissl, *Surveillance, Privacy and Security Citizens' Perspectives*, Routledge 2016.

[35] R. Rios, J. Lopez, J. Cuellar, *Location Privacy in Wireless Sensor Networks*, CRC Press 2016.

to manage threat levels more effectively. However, it is worth asking the question – one which will certainly be repeated many times in the future – whether technology and counter-terrorism measures will protect the state and its citizens, or whether they will lead to an unintended ‚virtual' totalitarianism in which every individual will feel they are being observed? Are there risks worth taking to protect freedom? Or will the collective need to feel safe while the application of more surveillance derails freedom? These questions are nothing new and will certainly capture the attention of observers and researchers investigating security policy.

The advent of digital technology has provided intelligence agencies with access to vast amounts of data that were previously inaccessible without the use of secret means. Oversight of the use of digital technology is undoubtedly necessary to protect the security and interests of the state and its citizens. The latter must receive assurances from their governments that control is strictly enforced by their governments and not by external actors, such as other states or multinational companies[36]. Even in pluralistic democratic societies, the tendency to use technology that may provide less freedom under the guise of greater security may prove difficult to curb.

Despite this article's failure to sufficiently address the question of how to draw the line between security and freedom, a certain solution to this dilemma is to suppose that the focus should be on how data is used rather than how it is collected, since in today's digital world, information is virtually impossible to protect. Following this line of thought, it should be said that the problem is not the technology, but the authority whose duty it is to ensure the rights and freedoms of citizens.

Today, security measures involve complex technologies that provide an unprecedented amount of data which, when correctly analysed, become identifiable and, to a large extent, can also prevent terrorist attacks both at home and abroad. However, it is worth remembering that technology alone cannot provide security. Although it can be a means to an end, collecting data (no matter how much) does not guarantee that such intelligence strategies will make society safer.

---

[36] M. Cayford, W. Pieters, C. Hijzen, *Plots, murders, and money: oversight bodies evaluating the effectiveness of surveillance technology*, «Intelligence and National Security» 2019, Vol. 33/7, pp. 999–1021.

## Conclusions

Until recently, the prevailing view was that democracies are more vulnerable to terrorist attacks than authoritarian government and that "the more democratic a state is, the more incidents of terrorism it should experience"[37]. Proponents of this view offer two main explanations to support it. The first is that liberal democratic freedoms of association and movement, combined with legal restrictions on security forces, facilitate the organisation of terrorist groups and the planning and execution of attacks. The second explanation emphasises the mobilisation, publicity and susceptibility of democratically elected politicians to pander to public sentiment. Terrorists can most easily achieve "influence" in the most liberal democracies through the functioning of the mass media, which guarantees a wide audience for acts of violence, and a government that feels strong public pressure to avoid threats[38].

In the context of the above arguments, it is worth noting the existence of an opposing view in the literature, namely that a democracy run anti-terrorist operations because its liberal openness allows for peaceful and public expression of grievances and the redressing of injustices, which in turn makes legitimacy more difficult for violent and extremist groups[39].

Attempting to assess the post-9/11 political consequences twenty years on remains a complex matter. It is not clear whether democratic states are in the initial phase of this conflict with terrorists, somewhere in the middle, or whether they have found sufficient and effective means to marginalise the terrorist threat.

Freedom, which is one of the factors characterising democracy, rests largely on the pillar of protection of privacy. However, contemporary concerns about the threat of terrorism after 9/11 and the dynamic technological advances in security allowing for data collection may lead to the marginalisation of this right to privacy.

Society has come to deeply value privacy because it is understood that the right to privacy not only allows freedom but also protects human interactions ranging from the intimate to the more open, where people can do and say as they wish, otherwise they would not feel free while

[37] E. Chenoweth, *Terrorism and Democracy*, «Annual Review of Political Science» 2013, No. 16, p. 357.

[38] B. Hoffman, *Inside Terrorism*, New York: Columbia University Press 2017, p. 174.

[39] D. A. Christensen, J. Aars, *Does Democracy Decrease Fear of Terrorism?*, «Terrorism and Political Violence» 2019, No. 31/3, pp. 615–631.

feeling watched by the state and its security services. Since privacy lies at the heart of freedom, choice, self-expression, creativity and autonomy, it is the foundation of a democratic society.

On the other hand, it is difficult to deny the importance of a certain amount of surveillance, including increasingly technological surveillance, which makes society safe and functional. If everyone believed that no one controls the mechanisms of the state and society, it might well be that many citizens would refuse to carry out their basic daily duties towards the state, such as paying taxes or obeying traffic rules. Excessive anonymity could therefore lead to anarchy. Thus, the extent and type of citizen surveillance used is an extremely sensitive issue and represents one of the most important challenges for policymakers today. Controlling and understanding the processes involved in the use of technology seems particularly urgent in the age of artificial intelligence which is now upon us.

## Bibliography


Bacevich A. J., Prodromou E. H., *God is not Neutral. Religion and US Foreign Policy after 9/11*, «Orbis» 2004, No. 48/1.

Bamford J., *The shadow factor: The ultra secret NSA from 9/11 to the eavesdropping on America*, Anchor Books 2008.

Bhattacharya S. B., *Of Democracies, Wars and Responses to War: A Comparative Perspective on War and Security in India and the United States*, «India Quarterly: A Journal of International Affairs» 2013, No. 69/3.

Boswell Ch., *Migration, security, and legitimacy: some reflections* [in:] T. Gives, G. P. Freeman, D. L. Leal (eds.), *Immigration Policy and Security: U.S., European, and Commonwealth Perspectives*, Routledge 2009.

Brzezinski M., *Fortress America: On the front lines of Homeland Security: An inside look at the coming surveillance state*, Bantam 2004.

Burt Ch., *Fever detection technology added to biometric hardware by Dermalog, Telpo, DFI, Hikvision and Kogniz*, «Biometric update», https://www.biometricupdate.com/202004/fever-detection-technology-addedto-biometric-hardware-by-dermalog-telpo-dfi-hikvision-and-kogniz (23.09.2021).

Cayford M., Pieters W., *Effectiveness fettered by bureaucracy: why surveillance technology is not evaluated*, «Intelligence and National Security» 2020, Vol. 35/7.

Cayford M., Pieters W., Hijzen C., *Plots, murders, and money: oversight bodies evaluating the effectiveness of surveillance technology*, «Intelligence and National Security» 2019, Vol. 33/7.

Christensen D. A., Aars J., *Does Democracy Decrease Fear of Terrorism?*, «Terrorism and Political Violence» 2019, No. 31/3.

Costa L., *Virtuality and Capabilities in a World of Ambient Intelligence. New Challenges to Privacy and Data Protection*, Springer 2016.

Criado H., *What Makes Terrorism Salient? Terrorist Strategies, Political Competition, and Public Opinion*, «Terrorism and Political Violence» 2017, No. 29/2.

Erlanger S., *The Coronavirus Inflicts Its Own Kind of Terror*, «New York Times», https://www.nytimes.com/2020/04/06/world/europe/coronavirus-terrorismthreat-response.html (23.09.2021).

Genschel P., Jachtenfuchs M., *Postfunctionalism reversed: solidarity and rebordering during the COVID-19 pandemic*, «Journal of European Public Policy» 2021, Vol. 28/3.

Goold B. J., *Privacy, Identity and Security*, [in:] B. Goold & L. Lazarus (eds.), *Security and Human Rights*, Portland 2007.

Greitens S. Ch., *Surveillance, Security, and Liberal Democracy in the Post-COVID World*, «International Organization» 2020, Vol. 74/1.

Hoffman B., *Inside Terrorism*, Columbia University Press 2017.

Huq A., *Terrorism and Democratic Recession*, «University of Chicago Law Review» 2018, No. 85, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2974006 (23.09.2021).

Kołodziejczyk M., *Technológia služiaca na zadržiavanie koronavírusu: potenciálne hrozby pre ochranu ľudských práv*, «Medzinárodné Vztahy» 2020, No. 18/2.

Kostakopoulou D., *How to do Things with Security Post 9/11*, «Oxford Journal of Legal Studies» 2008, vol. 28/2.

Lee T., Lee H., *Tracing surveillance and auto-regulation in Singapore: 'smart' responses to COVID-19*, «Media International Australia» 2020, Vol. 177/1.

Le´onard S., *Border Controls as a Dimension of the European Union's Counter-Terrorism Policy: A Critical Assessment*, «Intelligence and National Security» 2015, Vol. 30/2–3.

Levinson-Waldman R., *NSA Surveillance in the War on Terror,* [in:] D. Gray, S. E. Henderson (eds.), *Cambridge Handbook of Surveillance Law*, Cambridge University Press 2017.

Lidén G., *Technology and democracy: validity in measurements of e-democracy*, «Democratization» 2015, No. 22/4.

Marrs J., *The terror conspiracy: Deception, 9/11 and the loss of Liberty*, Disinformation 2006.

McLeod D. M., Shah D. V., *News Frames and National Security*, Cambridge University Press 2014.

Monaghan J., *Performing counter-terrorism: Police newsmaking and the dramaturgy of security*, «Crime Media Culture» 2020.

Nacos B. L., Bloch-Elkon Y., Shapiro R. Y., *Prevention of Terrorism in Post-9/11 America: News Coverage, Public Perceptions, and the Politics of Homeland Security*, «Terrorism and Political Violence» 2007, No. 20/1.

Ochoa Ch. S., Gadinger F., Yildiz T., *Surveillance under dispute: Conceptualising narrative legitimation politics*, «European Journal of International Security» 2021, No. 6/2.

Rios R., Lopez J., Cuellar J., *Location Privacy in Wireless Sensor Networks*, CRC Press 2016.

Sinha G. A., *NSA Surveillance Since 9/11 and the Human Right to Privacy*, «Loyola Law Review» 2014, No. 9.

Stam V., *The 9/11 Generation: Youth, Rights, and Solidarity in the War on Terror*, «Surveillance & Society» 2018, No. 16/1.

Tromblay D. E., *Botching Bio-Surveillance: The Department of Homeland Security and COVID-19 Pandemic*, «International Journal of Intelligence and CounterIntelligence» 2022, No. 35/1.

Weiler J. H. H., *COVID, Europe, and the Self-Asphyxiation of Democracy*, [in:] M. Poiares Maduro, P. W. Kahn (eds.), *Democracy in Times of Pandemic*, Cambridge University Press 2020.

Williams R. W., *Terrorism, anti-terrorism and the normative boundaries of the US polity: The spatiality of politics after 11 September 2001*, «Space and Polity» 2003, No. 7/3.