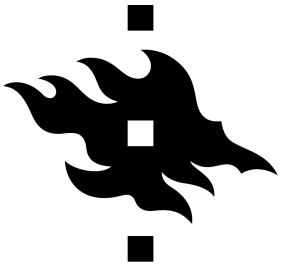

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Surveillance Society as a Threat to Liberal Democracy in the European Union

Heta Heikkilä, Noora Honkola, Milla Huunonen, Kati Makkonen & Emma Pesu

Faculty of Social Sciences, University of Helsinki
Master's Programme in Global Politics and Communication

Abstract

This study discusses surveillance society as a threat to liberal deliberative democracy in the context of the European Union (EU), using Hungary as a case example. The research examines the EU laws and programs regulating citizens' surveillance and reviews how their use has been legitimised. The study analyses the narrowing privacy of the citizens as a result of targeted surveillance and the dimension of digital society in relation to surveillance, taking into account the developments and new forms of surveillance that have emerged during the information age. The study shows that the regulation of surveillance at the EU level is in its infancy, and the Union's power to intervene in the surveillance of citizens is limited.

Key words: surveillance society, liberal democracy, European union, Hungary, algorithms, surveillance capitalism

1. Introduction

This study discusses surveillance society as a threat to liberal deliberative democracy in the context of the European Union, using Hungary as a case example. The concept of the surveillance society is perhaps best known from China's example, where the surveillance exercised by the state, the government and the Communist party is comprehensive. In this study, we delve into the EU laws and programs regulating citizen surveillance and examine how their use has been legitimised in the Union. In this context, securitisation refers to the legitimisation of control by paternalism which is justified by the protection of individuals. Our research analyses the narrowing privacy of citizens caused by citizen surveillance and the dimension of digital society concerning surveillance.

The theoretical background for the research paper is the discussion of liberal democracies that have become illiberal (e.g. Mounk, 2018). A similar development has occurred in Hungary, a European Union member state. In the conclusions, we summarise the threats to the rights and freedoms of individuals at the EU level that citizen surveillance proposes. We present solutions to protect the rights and freedoms of individuals in the European Union area. Accelerated polarisation in civil society, along with digitalisation, is negatively shaping liberal democracies. The development has led to the illiberalisation of EU member states such as Hungary.

In the first section, we elaborate more on the study's theoretical background: we discuss the tension between liberal and illiberal democracy and the development of illiberalisation. The concept of a surveillance society and the justification of surveillance will be explored in more detail in the second chapter. The third chapter examines the current EU-level regulation on supervision and, on the other hand, its limitations. In the fourth chapter, we delve deeper into algorithms and their effects on the democratic system. While the first half of this research paper will deal with surveillance primarily from a governmental perspective, the fifth chapter examines the commercial dimension of surveillance: surveillance capitalism, in more detail.

In the age of the information flood, surveillance capitalism plays a central role in individuals' consumption of social media and is strongly present in the use of time spent online. In this study, surveillance capitalism refers to the commercialisation of personal data for the pursuit of profit, as the means of surveillance capitalism today are diverse and essentially involve intense surveillance. In addition, we delve into how democracy can also be threatened by surveillance capitalism and why citizens are more receptive to surveillance for commercial

purposes. For example, eye-gaze technology can monitor consumer preferences when analysing reactions to advertisements or products in online stores. This is how surveillance capitalism can be used to target ads individually and hide control mechanisms in cookies.

Citizen surveillance has existed in various forms for the longest time. Still, digitalisation has changed the nature of surveillance to, first of all, commercial but also patronising and violating individual rights.

2. Theoretical background: Introduction to Liberal and Illiberal Democracy

Emma Pesu

In this section, we will examine the concepts of liberal and illiberal democracy in more detail. The development of Hungary from a liberal democracy to an illiberal democracy will also be briefly covered.

Liberal democracy has long been considered an ideal form of government. After the collapse of the Soviet Union, liberal democracy became the dominant form of government almost everywhere in the world. The victory of liberal democracy is explained mainly by the fact that there has been no viable alternative (Mounk, 2018, p. 3). Until recently, citizens of liberal democracies were highly satisfied with their government and other state institutions now, however, citizens are more dissatisfied with these entities than ever before (Mounk, 2018, p. 5). How did this situation come about, and why has the discussion turned to illiberal democracies and the post-truth era?

In the 2020s, we live in a time that experts and scientists did not expect to see (Mounk, 2018, p. 25). Examples of the post-truth era include the rise of Donald Trump as President of the United States, the Brexit vote in the UK, and the popularity of populist parties in countries such as Hungary and Poland. Yascha Mounk mentions that in the European context, illiberal populists have come to power in Poland, Hungary, and Turkey (2018, 9).

2.1. The concepts of “liberal” and “illiberal” democracy

The term "liberal" has been used to refer to many different things. In the context of liberal democracy, liberal refers to values such as freedom of speech, separation of powers, or protection of individual rights (Mounk, 2018, p. 26). Political scientist Robert Dahl defines democracy as a system with free, fair, and competitive elections, universal suffrage, broad protection of individual rights, and officials not elected by popular vote (Mounk, 2018, p. 26).

In Dahl's definition, the protection of liberal rights is a central part of democracy. According to Mounk, liberal democracy is a political system that is both liberal and democratic and also protects individual rights and transforms popular opinions into general policy lines (2018, 27). Tero Lundstedt defines liberal democracy as the power of representatives elected in fair and free multi-party elections, limited by the separation of powers, the principle of legality, and a constitution that protects individual freedoms (2022, 13).

However, democracies can also become illiberal when independent institutions decline or minority rights are restricted. The concept of illiberal democracy was first used by Fareed Zakaria in his 1997 article *The Rise of Illiberal Democracy*. Liberalism and democracy are built on technological, economic, and cultural conditions. However, these conditions have weakened (Mounk, 2018, pp. 27-28). The rise of illiberal democracies is seen to have begun with the 2008 financial crisis. The financial crisis weakened the Eastern European countries' belief in the previously unshakable liberal democracy (Lundstedt, 2022, p. 15).

According to Lundstedt, in illiberal democracies, a strong individual leader or ruling party controls the seemingly democratic system. Lundstedt lists the common features of illiberal democracies: concentration of power, restriction of citizens' freedoms, tightening of ethnic conflicts, and increased societal polarisation. In illiberal democracies, the separation of powers is abolished, and one of the branches of government is often raised above the others.
Typically, this branch of government is the government (2022, 14). A report by The Finnish Institute of International affairs (Mikkola et al., 2018, pp. 31-34) introduces four common features and characteristics of liberal democracies that can make them vulnerable to hybrid influence, including limited public power, pluralism, free flow of information, and open economy. We will examine hybrid influence in more detail in chapter three.

2.2. Background factors of the post-truth era

Western societies have undergone significant changes due to digitalisation. Traditional institutions have come under scrutiny, traditional media is no longer the gatekeeper it once was, and the political climate has become increasingly polarised (Vihma et al., 2018, p. 17). For a long time, new technology was expected to revitalise democracy and strengthen it. However, by the time of the 2016 US presidential election and the UK's Brexit vote, the true power of social media was revealed - social media began to be seen in a negative light as well (Vihma et al., 2018, p. 20). The amount of information and data has increased dramatically as internet

users have grown. There has also been talk of an "information overload" that has been said to contribute to a decline in people's attention span (Vihma et al., 2018, pp. 21-22).

The internet has caused the "death of traditional gatekeepers," as all internet users have access to vast sources of information (Vihma et al., 2018, p. 23). Today's social media platforms are characterised by the personalisation of platform content and the use of algorithms. The aim of algorithms and personalisation is to provide each platform user with increasingly individualised content. There are also many dangers associated with personalising content, such as the risk of forming “a bubble”. As a result of the bubble, like-minded people only share content they like with each other (Vihma et al., 2018, pp. 26-29). Increasingly sophisticated algorithms may therefore threaten this. Algorithms are also not immune to fake news. The algorithm does not recognise whether a news item is true or false, and thus a news item that arouses interest may quickly spread to a wide audience (Vihma et al., 2018, p. 31). These factors related to digitalisation are seen as the key background factors behind the post-truth era and the rise of illiberal democracies.

As Mounk (2018) also mentions, another key background factor of illiberal democracies has been political polarisation and the growth of populism. Polarisation can be seen as a precondition for the flourishing of post-truth phenomena. Political polarisation is currently driven by populist movements (Vihma et al., 2018, p. 44). In the United States, the background to polarisation can be seen as a political right-wing identity crisis, but in the European context in the 2000s, polarisation has been influenced by the problems faced by social democratic parties. In Europe, many populist movements have benefited from the problems of social democrats. European right-wing populists have often focused on immigration and the EU, while in the United States, populism has been fueled by dissatisfaction with the political system. Both of these factors have contributed to the rise of post-truth politics and the decline of liberal democracies (Vihma et al., 2018, p. 44). Chapter four will examine algorithms, bubbles, and polarisation in greater detail. Such developments provide excellent soil for the rise in support of populism. Nevertheless, what events have led to Hungary no longer being considered a liberal democracy?

2.3. The Development of Hungary into an Illiberal Democracy

Hungary's economy strengthened in the 1990s, and it appeared that the model of liberal democracy would be established in Hungary as well. However, problems began to arise when many Hungarians felt they did not receive a share of the country's economic growth.

Hungarians began to think that immigration threatened their national identity. In the 2010 parliamentary elections, most Hungarian voters cast their ballots for Viktor Orbán's right-wing Fidesz party. Upon coming to power, Orbán changed the election system to his advantage and appointed like-minded individuals to lead the state television channels, the justice system, and the election commission (Mounk, 2018, pp. 9-10). Therefore, Orbán has acted according to the development described by Lundstedt: Orbán originally came to power through fair elections, but once in power, he began to take steps to limit the boundaries of the constitution (2022, 14). As a result of these events, Hungary is no longer considered a liberal democracy but is thought to have become an illiberal democracy. According to Lundstedt, Orbán has been considered a promoter of certain illiberalism worldwide (2022, 15).

The European Union awoke relatively late to the events in Hungary. In 2011, Hungary received its first warnings from the European Parliament regarding the restriction of media freedom. The definition of the rule of law in the EU was also established in the same year. From 2013 onwards, there has been discussion in the EU about the type of sanctions that can be imposed on EU member states that violate the shared values of the union. The rule of law mechanism was launched for this purpose, but only in 2021 (Miklóssy, 2022, pp. 57-58). In the following chapters of this research, we delve deeper into the phenomena of the post-truth era in illiberal democracies. We focus on surveillance, hybrid influence, algorithms and the polarisation they create, and surveillance capitalism.

3. Introduction to a surveillance society. How is surveillance legitimised?

Kati Makkonen

Already in the 18th century, Enlightenment philosopher Jeremy Bentham outlined in his writings the idea of a new kind of prison, a panopticon, where prisoners would constantly be monitored without their knowledge. Bentham's thoughts' ultimate goal was a happy society, to which he saw the key was surveillance. Due to surveillance, those who acted correctly could be rewarded, and those who acted incorrectly could be penalised (Crimmins 2021). Often the information produced by surveillance has been identified as a tool of social control. However, technological development has brought new challenges to the supervision of more comprehensive applications, which have been used to solve security problems and commercial purposes (EDPS 2022). This section looks at how state-practised surveillance is carried out and justified and its consequences for democratic societies.

Technology is often seen as a tool to achieve something better and more efficiently. The ultimate responsibility for the consequences of its use is often left to the user. German philosopher Martin Heidegger has especially criticised in his writings the passing of the responsibility to the user because, according to him, it puts man in the role of an object instead of recognising technology's role in shaping social and political reality (Haque, 2015, p. 38). If technology is viewed from the perspective of its reality-shaping properties, it raises the question of its usability in public institutions. Are, for instance, supervision and control technologies designed in the private sector suitable for democratic institutions, and under what conditions should they be regulated? (Haque 2015, 43-44.)

The control carried out by the administration has been taken the furthest in China, where it is estimated that there are even half of the world's billion surveillance cameras. (The New York Times, 2022) Surveillance penetrates every aspect of life with applications that citizens use daily, online monitoring, and through surveillance cameras equipped with facial recognition technology. In China, citizens' support for surveillance, mainly with surveillance cameras, is quite significant and is seen as a stabilising factor for society. The concern about data misuse is not recognised similarly in western countries (Zheng 2020, 3). Since 2014, a social credit rating system has been used based on big data produced by the monitoring system, i.e., databases containing information collected from citizens. Based on this to the citizen, a social credit rating score is formed, divided into five areas: social connections, consumer behaviour, security, wealth, and obedience. For now, the credit rating system does not cover the whole society (Zheng 2020, 11). The most extensive of all is supervision in Western China in the province of Xinjiang, where control is specifically directed at the Muslim minority, Uyghurs.

A large part of contemporary societies is seen primarily as utilising information and fast information flow and valuing information societies. Surveillance societies, on the other hand, are defined as societies that work in part by collecting, recording, and analysing individuals' and communities' data on a large scale, even at the expense of their fundamental rights (Mathiesen, 2013, p. 36). Mass surveillance is defined as a method whose goal is to gather information on a large scale from a group of people without narrowing it down to a specific individual (Wirth et al., 2019, p. 1339). Control can also be targeted at particular individuals, for example, in criminal investigations. Scope of Control and goals often distinguish between democratic and authoritarian systems. (Bigo et al. 2013, 2) The most famous example of large-scale mass surveillance is global mass surveillance by the US security agency NSA, revealed

by Edward Snowden. Mass surveillance can be utilised for questionable purposes, such as discrimination and profiling, and as a manipulation tool, which has been the result, especially in China.

3.1. The many faces of control

In Western societies, a strong argument for more thorough supervision security has been raised. The security argument itself is not new and has been justified for ages considering, for example, the necessity of intelligence activities (Nokkala 2022, 6). During the Cold War, communist states, in particular, implemented the ideal of a natural police state - everyone monitored, and everyone was monitored. Even though the police states of the Cold War partially ceased from being, the value of information has, on the contrary, grown in today's information societies, and control increased (Nokkala, 2020, p. 6). Methods of acquiring knowledge in democratic societies define laws, which have changed even more widely in societies like Finland to allow monitoring. The security environment justified the intelligence laws enacted in 2019 to require broader rights for the authorities to guarantee national security.

The security threats the intelligence laws sought to address were terrorism, illegal intelligence activities, the proliferation of weapons of mass destruction and extremism, and organised crime-related projects (Ministry of the Interior 2022). The justifications reflect the 21st century in the beginning, with the war against terrorism declared by the United States, threatening speech became more familiar about terrorism as a critical factor unbalancing the stability of society (Maras, 2010).

In the security policy discourse, the state is seen as the primary guarantor of the security of society and citizens. This role justifies the right to, for example, what is included in the scope of privacy, to information or even broader prerogatives. However, it is appropriate to review the validity of the security argument. Could it be the pursuit of social control by securing certain aspects of society? Do we strive for security even through undemocratic means?

Threats are open to interpretation and, ultimately, social constructs exploited as an instrument of policy making. Threats that are particularly assessment-related are in the context of security because safety has so far not been able to be objectively measured (Limnell, 2009, p. 3). Threat pictures are used to achieve various political interests. Each state defines threat images from its national starting points. However, in western societies, it has been noticeable that security threats are defined relatively consistently, as threat assessments are primarily based on the estimates of the United States and NATO (Heinonen, 2011, p. 227). Accepted in spring

2022 in the European Union's security and defence policy guidance document, Strategic Compass described the EU as facing even more threats and challenges, among which others were raised, such as regional instability, information operations, and terrorism.

The concept of safety has expanded even further and, for example, environmental issues and, especially with the corona pandemic, health safety have been brought into the scope of safety. Securitisation is a process where something is formed into a threat image and named as part of the security circle. Securitisation often impacts how the defined threat is responded to and how resources are shared (Limnell 2009, 71). Terrorist attacks have decreased in Europe during the last few years (Council of European Union 2021). Despite this, terrorism is raised as a significant threat to social stability. Vague and surprising, terrorism can be seen as a simple justification by the authorities and the citizens' fear enormously appealing to emotion. Studies have shown that safety-based rhetoric works because citizens also justify self-monitoring for security based on that (Wirth, 2019, p. 1340). On the other hand, as the corona pandemic has shown, supervision can be helpful, for example, in tracing infection chains and monitoring quarantines.

It can be seen that the rhetoric in which the state of emergency is used to justify even broader powers to the authorities has become more common (Nokkala, 2022, p. 11). This development can reflect a view of the state's paternalistic obligations, according to which the citizens cannot understand what is best for them. This is why society should have even broader rights to make decisions for the individual. However, in democratic societies, state power is last in hand responsible, along with all its other activities, also responsible for the supervision it exercises and its justification to the people.

3.2. Hungary: Surveillance hotspots under review

In the first section, it was stated that the technological, economic, and cultural conditions have weakened, which is manifested especially in Hungary. After coming to power, Prime Minister Viktor Orbán tried to centralise power by changing the constitution. The use of the previously mentioned Pegasus monitoring program is just one example of Orbán's government's actions that undermine the fundamental rights of citizens. Pegasus monitoring revealed that worrying signals were again received about Hungary's rule of law situation. Instead of an official investigation being launched after the surveillance came to light, key ministers either denied the case or acknowledged it by stating that every state needs similar tools. The prime minister's

party, Fidesz, dismissed the revelation as the aim of the left-wing media to cause political trouble and mayhem (BIRN 2021). The increasing surveillance in Hungary can be seen as one of the administration's centrally managed efforts to reach even more robust control of the civil society.

Legislation projects have also been promoted under the guise of a state of emergency declared due to the corona pandemic. In the reform of the State of Emergency Act, instead of the previous six, three states of emergency were defined: state of war, emergency mode, and standby mode. Due to the corona pandemic, the standby mode was in effect for several years and continued after Russia invaded Ukraine. The state of emergency gives the government exceptional powers and enables it, if necessary, to rule with regulations and bypass the parliament (HS 2022). Orbán has tried to use security threats as a basis for a state of emergency and thus to centralise power for himself by the powers of a state of emergency.

Targeted online surveillance is not the only area Orbán's government has sought to gain control. Funding for national intelligence agencies has been increased by about fifty per cent, while inflation is high and the public finances are in deficit. The Hungarian national security service (SSNS) has recruited personnel for surveillance and supervisory tasks (BIRN 2022). The aim has been to address society's simmering dissatisfaction and respond to it by further tightening control. Investing in the surveillance apparatus is a worrying signal about the state of the democratic system. The following section looks in more detail into the regulation of supervision at the level of the European Union as well as to the deepening and increasing effects of surveillance on the ideals of liberal democracy in Hungary.

4. Cyber security strategy of the European Union and emerging hybrid threats - a case example of Hungary

Milla Huunonen

In this chapter, we will learn more about the regulation of citizen surveillance in the European Union, and the case study of Hungary will be introduced. In Hungary, the Pegasus surveillance system was used to monitor journalists and political opposition representatives.

The chapter outlines the EU-level preparation for hybrid and cyber threats coming from outside and inside the Union and considers the change in the role of traditional media as a “watchdog” of power.

4.1. The growing threat of hybrid influence at the borders of the European Union

Surveillance of citizens is a challenge of the information age for the European Union. According to the Data Protection Supervisor of the European Union, surveillance within the Union has increased alongside technological development in the public and private sectors. Citizen surveillance has become cost-effective, commercialised, and can be practised in many ways, such as through monitoring, following and profiling citizens. Every form of surveillance is a threat to one's privacy and threat to the protection of personal data (European Data Protection Supervisor, n.d.).

The general data protection regulation (GDPR) aims to protect citizens' privacy in the European Union. GDPR sets exact requirements for organisations and companies for the storage, collection and management of personal data. This regulation applies to organisations and companies operating in the European area and to organisations operating outside of the European area if the data processing is aimed at EU citizens. (Your Europe, n.d.) According to those who have researched surveillance in the European Union, surveillance programs that are typical in Europe cannot be analysed only in the light of data protection and national security, as the threat of surveillance proposed for collective freedom and democracy must be taken into account. (Bigo et al., 2013, 2)

The concept of information warfare refers to all kinds of activities "that aim to influence public opinion systematically, people's behaviour and decision-makers, and thereby society's ability to function." (Valtioneuvosto, 2019, p. 5) Information warfare is a form of hybrid influence and, therefore, one of modern warfare's tools. (Mikkola et al., 2018, 53) Disinformation is one concrete example of the versatile means of information warfare, as it is used to spread false information purposefully. During the coronavirus pandemic, a considerable amount of disinformation and misinformation related to the disease and the fight against the pandemic was circulated globally. As a result, the European Union issued a policy on combating disinformation and finding reliable sources. It should be essential to think about the intentionality of spreading disinformation and the actors behind it. (European Commission, n.d.) Preparations for combating hybrid influence, such as disinformation, began in the EU in 2016, as more and more hybrid threats against EU member states were outlined, and a common framework was created to respond to these threats. (European Commission, n.d)

The European Union's joint statement on the cyber security strategy outlines that democracy depends on functional and reliable digital tools and on connectivity. Cyber security

is needed in order to strengthen resilience in the Union area. In particular, the mass shift to remote work due to the coronavirus pandemic has affected democratic processes in a way that they are becoming more and more dependent on interconnected networks and information systems, which increases the threat of cyber attacks. Restrictions on global internet networks would threaten global and open cyberspace but also legal order, fundamental rights, freedom and democracy. (European Commission, 2020) China, which can be seen as the origin and the extreme example of citizen surveillance, restricts its citizens' access to Internet-based Western applications such as Facebook and other social media platforms. (Xu & Albert, 2017) With the increase in cyber and hybrid threats, the EU's challenge is to prepare for possible attacks and build resilience in the Union territory without interfering with the rights and freedoms of individuals to use the open space internet.

Cyberspace is increasingly used for ideological and political purposes, which increases polarisation in societies. Increasing polarisation at the international level weakens multilateral cooperation. The EU is prepared for hybrid threats that combine disinformation campaigns with strategic infrastructure, economic processes and democratic institutions with the aim of causing physical damage. Threats that can open illegal access to personal information, steal industrial or state secrets, sow mistrust and undermine social cohesion. These threats undermine international security and stability and the benefits that cyberspace could bring to economic, social and political development (European Commission, 2020).

In the cyber security strategy, the EU outlines ways to prepare for cyber threats in the cyber security strategy. These include building a cyber shield and super-secure communication infrastructure, securing extensive future mobile networks, such as 6G, increasing cyber security in the interface, tackling cyber crime, strengthening cyber defence and establishing a leadership position for the European Union in cyber-security-related to standards and structures, in cooperation with multilateral partners (European Commission, 2020).

It is noteworthy that the EU's cyber security strategy does not address preparing for and responding to internal threats. In the next paragraph, the emerging threats are discussed, and in the conclusion chapter, some solutions are presented.

4.2. Internal threats

Hungary has received a lot of criticism within the European Union for the country's shift towards authoritarianism. This development, seen in Hungary and also in Poland, weakens the unity of the European Union but also its prestige as a transnational actor in the international

rule-based system. The rule of law mechanism has been presented as a solution for the situation, which aroused much opposition in Hungary and Poland but was finally found to be in line with the values of the Union by the European Court of Justice. In addition, support packages related to the coronavirus have been denied from both countries as a sanction (World Justice Project, 2022, Zsiros and Gill et al.,2020).

This case study examines citizen surveillance in Hungary through the laws and programs regulating citizen surveillance in the European Union. The discussion illustrates the nature of surveillance as a threat to Western liberal democracy. The case example concerns the democracy-threatening forms of citizen surveillance by Hungarian Prime Minister Viktor Orban and the country's far-right government.

Pegasus is a spyware developed by the Israeli NSO Group, which The Guardian calls the most powerful spyware ever developed. Pegasus can monitor incoming or sent messages, go through pictures in the photo gallery or record phone calls. Pegasus uses the smartphone's microphone to listen and record speech and the camera to take pictures. With these functions, the spyware can find out the location of the individual, the places they have visited and the people they have spent time with. NSO Group markets the Pegasus program to the governments of different countries. The first version of Pegasus was discovered in 2016, and it has developed so much over time that installing it on smartphones no longer requires action from the owner of the phone. It is possible to run the program on phones through iOS and Android operating systems, for example, via the app store. When you download the WhatsApp application, you might as well download Pegasus to your phone (Pegg and Cutler, 2021).

As stated earlier, Viktor Orban and his government have been confirmed to have used the Pegasus program on lawyers, journalists, activists and people in business in the country. The use of this spyware on the country's citizens is worrisome, but what makes it especially worrisome is the spying on journalists (Birnbaum et al., 2021). The role of journalists and the media in liberal democracies is to act as a special “watchdog” of power, and restricting their activities is a real threat to the values, unity and liberal democracy of the European Union (Uimonen, 2009).

In societies that have changed due to digitalisation and after the Post-truth era, the role of traditional media as a “watchdog” of power has weakened. In liberal democracies, the media has traditionally been considered the fourth power of the state, alongside the rule of law, the parliament and the government. The duty of the media has been to monitor those in power, highlight grievances and thus promote the realisation of democracy. "Journalists have a clear

task in a democracy: they cherish freedom of speech and take care of its realisation" (Uimonen, 2009). In particular, social media and widespread free access to information are factors that can be seen to have weakened the role of traditional media as the fourth state power. Suppose the role of traditional media as a defender of freedom of speech has already weakened due to digitalisation. What does the monitoring of journalists with the Pegasus program do to freedom of speech in Hungary? The narrowing of freedom of speech is a real threat to liberal democracies and a big step towards authoritarianism.

In summary of the European Union's preparation for cyber security and hybrid threats, it can be said that there is an ambition to act as a pioneer, but there is a complete lack of concrete action to deal with threats within the Union. What kind of community of values and actors does the EU present itself in a multilateral rule-based system when several member states are shifting towards authoritarianism? What does it mean for liberal democracy and the security of the Union? What kind of cyber security pioneer can the EU act as when it is not prepared for threats within the Union?

5. Algorithmic surveillance

Noora Honkola

5.1. Algorithms as gatekeepers of information

The Internet and digitalisation have created a new era for information search and its processing. Information is constantly available easily and in abundance, which contributes to the conditions that receiving information does not require much reflection (Ikäheimo, 2017). This can lead to not considering or questioning information or its sources. In addition to availability, the search for information is guided by algorithms, based on which specific search results are directed to the searcher's view. Algorithms are not neutral actors since they reward content with visibility that improves the effectiveness of, for example, Google advertising (Ikäheimo, 2017). The information value is, therefore, not the factor based on which the algorithm directs certain search results to the searcher's screen. Instead, it uses the metadata stored in the databases, which is constantly modified based on the user's actions (Knuutila, Laaksonen, 2020, 397). A person and his worldview are nowadays to some extent, dependent on what the algorithm shows them, as a growing number of people seek information and read news from social media platforms, where the information they see is personally optimised (Knuutila, Laaksonen, 2020, 397).

According to Hannu-Pekka Ikäheimo (2017), the internet can strengthen human characteristics, such as seeking confirmation of one's beliefs and looking for like-minded company. Algorithms, in particular, enable the phenomenon of forming ´political bubbles´. This refers to a situation where the algorithm suggests content to the user that it thinks the user will like, in which case opposing opinions disappear from the news feed. Social media in particular, strengthens the bubble, as personalised content and advertisements are tailored to the user with the help of algorithms (Ikäheimo, 2017). The content we see is also strongly influenced by the publications of our friend network and reactions to the news feed. Often, however, algorithms suggest similar content that you have searched for or consumed before. In this case, it strengthens your already existing world of thought, and you may get the illusion that the world around you also agrees with you. If your views are never challenged, you are unlikely to change or modify your opinions either.

Naturally, this is where the problem lies for liberal democracy because when people form these political bubbles, open and fair public debate suffers. If a person encounters opposing opinions only rarely, it may also emphasise the confrontation between dissenters when these "echo chambers" meet each other. A person is also prone to believing fake news or half-truths without questioning and examining the contents critically.

5.2. Algorithms as political influencers?

Since algorithms have become a part of our everyday life, there has been a debate about whether algorithms aim at political influence. In recent years, election campaigns have shifted to social media to a significant extent (Knuutila, Laaksonen, 2020, 394). To some extent, it is possible for the administrators of social media platforms, such as Facebook, to influence the spread of certain types of content, such as fake news (Ikäheimo, 2017). Algorithms, however, do not identify fake news from the news stream but instead reward publications that get many reactions with visibility. Political topics arouse a lot of emotions, especially during elections, and desirous social media posts are often very successful on social media. Algorithms may therefore have significant power to influence the final results of elections. Several researchers suggest that especially right-wing populist political leaders have come to power by exploiting this new kind of emotional culture (Knuutila, Laaksonen, 2020, 394).

It has also been studied that, for example, Facebook can influence the emotional states of its users by adding positive or negative posts to the news feed (Ikäheimo, 2017). Those

exposed to positive input react by sharing positive things, while those exposed to negative input react in a negative way. This is also how social realities become polarised, i.e. set against each other. When algorithms determine visibility on internet platforms, they may intentionally or unintentionally enable extremist opinions, which accelerate polarisation (Ikäheimo, 2017). Algorithms seem to support commotion and the creation of intentional or unintentional harassment campaigns (Knuutila, Laaksonen, 2020, 394). Of course, it must be remembered that realities have differed and will continue to differ also by our own choices, not only based on algorithms. There is also evidence that even positive messages during the elections have gone viral and gained a lot of visibility on social media (Knuutila, Laaksonen, 2020, 395). However, it must be stated that algorithms speed up and make polarisation even more visible.
From the viewpoint of liberal democracy, the effect of the personalisation of algorithms on the spread of disinformation is indeed problematic. In the past, for example, fake news has been known to a more limited circle, but because of the internet and algorithms, they can now reach a wide audience quickly. The user is also not able to choose the content he consumes in the same way in a digital environment as, for example, choosing a print magazine from a store shelf.

5.3. Algorithms and journalism

Algorithms are now also a part of editorial work processes in EU countries (Grundström, Haapanen, Ilkka, 2019, 253). This was seen in Finland, for example, in the 2017 municipal elections, where Yleisradio's Voitto robot, Vaalikone Valtteri and Helsingin Sanomat's Latoja produced content about the election results. These news robots are a relatively new phenomenon in Finland, while content targeting has already become common even in newsrooms (Grundström, Haapanen, Ilkka, 2019, 253). Content targeting refers to, among other things, the view of a website that changes based on a person's page history, advertisements or story recommendations.

Algorithms used by news outlets can offer a challenge to liberal democracy, especially in countries like Hungary, where the independence and freedom of journalism and the media are threatened. After Prime Minister Viktor Orbán came to power, efforts have been made to systematically destroy the independence of the media, and the government's self-defined fake news may result in a prison sentence of several years (Heijari, 2020). Observing the world press freedom index, Hungary is ranked 85th in 2022 (Reporters Without Borders, 2022). The ethics and values of algorithms are largely determined by the purposes for which they are used.

In 2019, the Finnish Public Word Council (JSN) issued a statement under the name *Statement on labelling news automation and personalisation (Lausuma uutisautomatiikan ja personoinnin merkitsemisestä)*. The purpose of the statement was to define the use of algorithms as tools in journalistic work (Grundström, Haapanen, Ilkka, 2019, 253). In the statement, recommendations were also given regarding targeting and labelling of news automation, which has previously been very inconsistent both in Finland and elsewhere in the European Union. According to JSN, attention should be paid to the regulation of the use of algorithms because if its regulation is left only to the authorities or platform companies, this will endanger the freedom of the press (Grundström, Haapanen, Ilkka, 2019, 257). The statement also mentions that journalistic decision-making power should not be handed over to parties outside of newsrooms, referring to algorithm developers. However, it is impossible for the responsible editor to fully know the operating logic of the algorithms.

5.4. Who oversees algorithmic surveillance?

Who then understands and controls the operating logic of algorithms? No one is completely in control of them. In the past, algorithms were programmed to do a certain task according to a certain pattern. As the artificial intelligence algorithm progresses, algorithms often perform machine learning, where the algorithm constantly learns from the data it receives and modifies its actions based on it (Trémouille, 2020, p. 4). The programmer of the algorithm can therefore influence how the algorithm processes the data it collects, but not much on the end result because algorithms develop their operations independently.

It must also be remembered that algorithms and the data they process are closely guarded trade secrets of companies such as social media platforms (Trémouille, 2020, p. 12). Therefore, companies often do not open the operating logic of the algorithms they use. In a 2019 survey of the Finnish media, it was also found that the media inform their readers about the use of personalisation in very different ways (Grundström, Haapanen, Ilkka, 2019, 255). Therefore users don't necessarily understand that they are seeing personalised content or the operating logic of the algorithm that prunes the content. For democracy, this lack of transparency is problematic. Many decision-makers within the European Union have been concerned about this problem. For example, Angela Merkel expressed her concern in 2016 that algorithms distort our observations and demanded more visibility into the algorithms used by platforms (Ikäheimo, 2017).

Algorithms, therefore, do not have agency in themselves, but rather they carry out a task programmed into them (Trémouille, 2020, p. 2). For example, algorithms programmed according to the business logic of social media platforms favour user-interesting, discussion-provoking, sensational and emotional content (Knuutila, Laaksonen, 2020, 397). It is worth noting that machine learning algorithms are not completely regulated by anyone. Algorithms interact with users, in which case their operation should be observed as part of a wider totality (Knuutila, Laaksonen, 2020, 397). Beyond human factors and the built-in features of algorithms, they must be viewed more broadly as part of surveillance capitalism.

6. Surveillance capitalism and its dimensions to democracy *Heta Heikkilä*

Earlier in this research article, we have discussed surveillance mainly from the state actors' perspective. However, state actors are not the only practitioners of surveillance and this paragraph focuses on the commercial dimension of supervision and control. There is no coincidence after you have been browsing new shoes from the store's website, and a few moments later, you scroll your Facebook or Instagram feed and accidentally see shoe advertisements about the exactly same shoes you were looking at before. Now the shoes might be even discounted – even if the browsing was only 15 minutes ago. The example is definitely much uncomplicated, but still it is a good example of surveillance and the market economy's interconnection in the digital era. Although capitalism does not have a single universal definition, it usually refers to the economic system typical of Western democracies, in which the production is privately owned, and trade and competition are pursued in the free market. The term Laissez-faire is the principle of free commerce adopted by capitalism, according to which the state should intervene as little as possible in commerce. Trading is aimed at increasing capital and creating financial profit for its owners (Heywood, 2013, 131-138).

6.1. Surveillance capitalism: the economic system of the internet

With the digitalisation and development of technology, also capitalism becomes digitalised (Funch & Charler, 2019, 2-3). Thus a new global economic system has emerged, which can be called surveillance capitalism. The term surveillance capitalism refers to US researcher

Shoshana Zuboff's (2019) definition in the "The age of Surveillance Capitalism: the Fight for a Human Future at the Frontier of Power". In this book, she describes surveillance capitalism as a global economic system in which people's digital behaviour on the internet is a resource for platform companies. For example, large platform companies such as Meta (formerly Facebook) financially utilises the data of users' behaviour. Platforms sell the user's information and data for marketing purposes. It is clear that the logic of the capitalistic economic system works in the digitalised world as well. Digitalisation is therefore provided a completely new marketplace in the modern world, but the logic behind the algorithms is still very dark and non-transparent to the users. According to Zuboff, surveillance capitalism has become a threat for modern democracies, and the consequences of surveillance capitalism can be compared to the devastation industrialisations' causes to the nature in the 19th century, which we now, 200 years later suffer in the form of climate change. At the end of the day, surveillance capitalism's attempt is to predict people's behavior and to create data patterns of behaviour. It causes that the liberal democracy's main values, people free will and – is faltering. (Zuboff, 2015, 76)

6.2. Is surveillance capitalism a threat to democracy?

As mentioned previously, surveillance poses a threat, especially to liberal democrats' societies where individual freedom and privacy are important values. When the surveillance is performed for commercial purposes, usually the benefits of control come to big international corporations. On the other hand, while surveillance capitalism is often associated with market economy and trade in the private sector, it can approach also political goals. When combined with the economic gains, surveillance begins to affect also the political sphere. In this case, the surveillance capitalism starts to threaten democracy as well, not only the private sector.

The power of global platforms has already grown so large that it is hard to ignore when discussing positions of power and political dominance. One example of the influence of surveillance capitalism that can be considered here is the "Cambridge Analytica scandal", which showed the consequences of surveillance and mass data exploitation when a large audience was exploited for political purposes. In the scandal, it emerged that a data analytics company called Cambridge Analytica exploited up to more than 87 million Facebook users' (now Meta) data to analyse its user's political beliefs and personal traits. In addition, data was used to define users targeted by political marketing and how their activities could be affected (Hagar et al. 2020, 115). Later the scandal played a role in the background of at least the United States presidential

election in 2016 and on the Brexit voting in the United Kingdom. Despite the fact that it is hard to evaluate afterwards how the scandal was affecting the election, it has even been claimed that the election winner would not necessarily have been Donald Trump without the microtargeting of voters and analyses produced by Cambridge Analytica (E.g. The Guardian, 2019). In democratic elections, it is dangerous that the election result can be influenced discreetly or even insidiously and without transparency in the logic of algorithms and political advertisements. In addition, financial resources provide certain political actors more opportunities to purchase such services, similar to Cambridge Analytica, which drives inequality between political actors.

6.3. If you are not paying for the product, you are the product

Even if several global social media platforms have market value in the thousands of billions (Forbes, 2022), social media apps are usually free for its user without exceptions. How is this possible?

One of the main characteristics of surveillance capitalism is the commodification of people. In the context of digitalisation, that can mean that the data of users' activities are sorted, analysed and sold to other organisations through private interaction or a data marketplace where companies are exchanging data. Thus, user data becomes a factor and resource of production that has a significant role in the platform's operation. In addition, for many platforms, it is typical that users create the content by themselves on the platform (e.g. Meta, Instagram, Twitter, etc.). Väliverronen & Seppänen (2012) characterise this phenomenon as "User-generated content", where a media company typically does not produce the content itself on the platform but compiles the platform out of user-generated and company-generated content. In the system that follows the logic of surveillance capitalism the user becomes the object of control, whose behavioural data is collected, sorted, analysed and ultimately productised (Zuboff, 2015, 75). Therefore, this forms a two-sided market – firstly, services and products are sold for customers but secondly, media platforms and companies sell users as audiences for other companies (Väliverronen & Seppänen, 2012). Because the user data transforms into the fuel for platforms operations, it has aspired users spend as much time as possible on platforms. This logic makes users desirable commodities for platform companies.

Furthermore, the concentration of media companies' ownership can be seen as problematic. The term "Big Five" refers to the giant tech companies Google, Amazon, Apple, Meta and Microsoft. The commoditisation and takeover of data is, therefore, after all, in the hands of a small, multinational elite. Thus, the exploitation of data and capitalist activity in the

digitalised world is very concentrated only in a few places on established platforms. In addition, as mentioned earlier in this research article, the data gained from users is power. Concentration of power and knowledge to certain multinational groups, mainly for the groups of elites, is problematic when looked at from the point of view of the principles of democracy. Especially when the logic of surveillance capitalism is still very non-transparent and inconsistent for its' users.

It is essential to understand that it is not just the finances that these companies receive as a benefit. Users' data and clicks also provides these companies with an unprecedented amount of power, the kind that is not previously seen in history. The more accurate data platforms are able to collect about their users, the more accurately it will be able to predict their behaviour and modify it to the desired direction. Particularly precious information can be seen in the "Big Data", in which the company holds comprehensive and extensive mass data of its users. When efforts are made to control the exercise of power by state actors in democratic states through various institutions and legislative means, the oversight and control of platforms are quite obscure. According to Zuboff (2019), surveillance capitalist media companies already have so much power that they are already challenging the current Western liberal democratic system.

6.4. Who is the Watchdog of Capitalism?

Earlier in this research article, in chapter two, we discussed the legitimacy of surveillance from the state actors' view. We can state that the surveillance of citizens is often legitimised by the common state security. In particular, after the WTC attacks in 2001, one of the most common defensive arguments to supervise citizens is the threat of state terrorism. When it occurs in commercial purposes by the multinational platform giants, it is appropriate to consider critically how these platforms legitimise the supervision and what ethical problems arise.

Often when speaking of surveillance capitalist activities, it is highlighted that the absence of platform operating logic is not transparent and clear to users. It is demanding for the user to obtain information and understand what information about one can be exploited. The legislation of platforms is admittedly challenging because the ownerships of media platforms are usually multinational and private, and the laws are national.

Interesting are also users' experiences of surveillance. Often, attitudes towards national surveillance are seen as very negative and as a major threat to democracy, but data collected for economic purposes and its utilisation is seen rather as an essential part of the platform that must

be accepted if one wants to participate in social media. Afriat & Dvir-Gvirsman (2020) describe citizens' attitudes towards surveillance: "This is capitalism. It is not illegal". Their research results show that Facebook users relatively favourably accept surveillance conducted for economic reasons. Surveillance is viewed as a negotiable commodity - users are willing to give up their privacy in exchange for the free use of digital platforms (Afriat & Dvir-Gvirsman, 2020, 123). Thus, many users believe that surveillance is simply an acceptable part of digitalisation. It is possible that state surveillance is viewed more critically because privacy is seen as a constitutional right that is not subject to public interference without proper cause. In social media, privacy is seen by Afriat and Dvir-Grisman (2020, 120) more as a commodity, an exchange tool, and as compensation for their use of the application.

As mentioned earlier, when surveillance is utilised for political purposes, it must be understood as a broader societal and democracy-threatening problem. The capitalist nature of surveillance also makes its regulation challenging - the basic nature of capitalism includes as free markets as possible and minimal government intervention, so it can be considered how much surveillance performed by platforms can be limited without touching its operating logic in free markets. Thus, surveillance capitalism is a balancing act between individual rights, the capitalist market economy, and regulation.

7. Analysis and conclusion

In our research, we have delved into the consequences of citizen surveillance for liberal democracy penetrating different areas of society. It is important to recognise that the established model of liberal democracy is not immune to threats. We have already noticed this in a few European Union member states. Although many countries, including Hungary, have shifted towards an illiberal direction, it cannot be said that liberal democracy will never return to these countries. In some countries, it has already been noticed that the illiberal populist leaders were unable to implement the “true will of the people", and some populist movements have already failed in achieving their goals (Mounk, 2018, pp. 254–255). In order to prevent populist governments from ascending to power, some citizens must show that the populists do not represent the will of the whole population. However, a huge part of the population is still on the side of liberal democracy. For example, mass demonstrations have been able to stop populist reforms in Hungary. The opposition also plays a significant role in challenging populists (Mounk, 2018, pp. 186–187). According to Mounk, it is also crucial for preserving liberal

democracy that citizens believe in the possibility of economic development in the future. In addition, citizens must recognise the misinformation and disinformation they encounter, which is encountered by everyone daily in social media, for example (2018, 194). However, according to Mounk, in the end, the only reasonable possibility to protect liberal democracy is to keep populists out of power (2018, 189).

Based on our research, we see that increasing media education in schools, coordinated at the EU level, would be of primary importance. However, increasing media literacy would be important in all age groups. In order to prevent the development of illiberalisation, it would be important for younger people to learn to recognise misinformation and disinformation on social media. We consider the protection of liberal democracy fundamental in terms of preserving the unity of the EU. Our research has shown that although it is important to recognise individual responsibility, not all responsibility for the development of polarisation can be attributed to the individual.

This research has shown that the practice of citizen surveillance is a threat to liberal democracy, and the illiberalisation of democracy may increase the amount of citizen surveillance in society. This development can be seen in Hungary. The current environment of the information age, which is also called the new normal, leads to adding more and more areas of society under the scope of security. Due to their complexity, faceless information operations, viruses that threaten health, and terrorist movements are easy grounds for expanding the authorities' powers, even at the expense of citizens' basic rights. Until now, in democratic societies, the rule of law has protected both the rights of individuals and limited the powers of authorities. However, Hungary's example shows that the erosion of the ideals of liberal democracy and the violation of citizens' basic rights go hand in hand.

A development like Hungary's is a threat emerging from within the European Union, which should be better prepared for. This kind of development may also occur in other European countries in the future, where liberal democracy has not been deeply integrated into society's basic values and activities. This collectively undermines the security and position of the EU region in the global rule-based system. The powers of the European Union to intervene in citizen surveillance are limited, as the example of Hungary has shown. The Union's cyber security strategy should consider threats from within the Union and seek solutions to combat them.

As the research has revealed, the rise of populism has been partly accelerated by digitalisation and ever-developing social media platforms. In addition to administrators, these

platforms are run by algorithms, which no one completely regulates. It is also not possible to fully understand the operating logic of the machine learning algorithm, and the administrators of the social media platforms do not make the processes of the algorithms they use as transparent as the leaders of the EU countries have hoped. The threat formed by algorithms is their lack of regulation and lack of transparency. It will be interesting to see whether the EU will regulate the operation of algorithms or give its member states instructions for regulation within the framework of national borders. Countries like Hungary are especially worrying, where algorithms can, if harnessed incorrectly, threaten the country's democracy.

However, it is also necessary to remember the user's responsibility in what they agree to when using online services and which publications they react to and how. Above all, our research clearly shows the need for media literacy when an individual navigates in a new political and digital environment. A critical examination of the contents is essential for a citizen living in a surveillance society.

As shown in chapter 5, alongside state actors, surveillance is also carried out by numerous private commercial media companies such as Meta, Instagram and TikTok. In this case, the control is primarily justified by economic arguments, and these companies make their earnings largely by selling the data acquired through the means of control and, for example, by targeted marketing. However, in the light of research, the approach to surveillance capitalism is more sympathetic than, for example, to the control of a state actor because surveillance is seen as so-called in return for users getting the apps for free. It is seen as an acceptable form of control because few users see leaving social media as an option. However, the Cambridge Analytica scandal, for example, has shown that the means of surveillance capitalism can also be harnessed for political purposes, in which case democracy is also threatened. Although an individual may have an indifferent attitude towards surveillance, the scale of the problem expands enormously when surveillance is directed at a large mass and the data obtained from them is analysed. In addition, an important point made in the paragraph is that digital platforms hold a huge amount of data and information about citizens worldwide, which is power in itself.

Digitalisation has therefore brought individuals under a completely new kind of supervision and has raised many questions about who should supervise supervision and how supervision should be regulated. Often the responsibility has been shifted to the individual. As the research shows, it is challenging that the operation logic of the monitoring is not transparent, and the conditions are often buried deep in long data protection statements. It is also appropriate to consider whether the individual's knowledge level can be trusted enough to evaluate the

effects of supervision. In this research we have discussed various means of regulation and introduced various legislative means, such as the GDPR. However, regulation is challenging, for example because the entities exercising control are often multinational whereas the legislation is national.

References

Afriat, Hagar ; Dvir-Gvirsman, Shira ; Tsuriel, Keren ; Ivan, Lidor. (2020). *The Information Society 2020: "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal.* Routledge.

Antto Vihma, Jarno Hartikainen, Hannu-Pekka Ikäheimo ja Olli Seuri. (2018): *Totuuden jälkeen. Miten media selviää algoritmien ja paskapuheen aikana*. Teos.

Aittokoski, H (23.5.2022). Pääministeri Viktor Orbán määräsi Unkariin jälleen poikkeus tilan – tällä kertaa syynä sota Ukrainassa. Helsingin Sanomat.

URL:https://www.hs.fi/ulkomaat/art-2000008842298.html (referenced 6.11.2022)

Bigo, Didier, Carrera, Sergio, Hernanz, Julien Jeandesboz, Parkin, Joanna, Ragazzi,

Francesco ja Scherrer, Amandine. (2013): Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law. *CEPS Paper in Liberty and Security in Europe.*

Birnbaum, M; Petho, A & Chastand, J-B(19.7.2021). In Orban's Hungary, spyware was used to monitor journalists and others who might challenge the government. *Washington Post.*

Crimmins, J. E., "Jeremy Bentham", The Stanford Encyclopedia of Philosophy (Winter 2021

Edition), Edward N. Zalta (ed.),

<https://plato.stanford.edu/archives/win2021/entries/bentham/>. (Viitattu 5.11.2022)

The Guardian. (23.3.2018): *Leaked: Cambridge Analytica's blueprint for Trump victory*.

Refecenced 5.11.2022.

https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-fo r-trump-victory

European Commission. Fighting disinformation. n.d. Verkkosivu. Viitattu 21.10.2022 https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation_fi

European Commission. (16.12.2020) Joint communication to the European Parliament and the council. The EU's Cybersecurity Strategy for the Digital Decade.

https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European commission. Tehostetut käytännesäännöt disinformaation torjuntaan. n.d.

Verkkosivu. Referenced 21.10.2022

https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan/strengthened-eu-code-practice-disinformation_fi

European Union. European Data Protection Supervisor. n.d. Verkkosivu. Referenced

19.10.2022 https://edps.europa.eu/data-protection/our-work/subjects/surveillance_en

European Union. Your Europe. Yleinen tietosuoja-asetus. n.d. Verkkosivu. Referenced 19.10.2022.

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

European union (2022). Strategic Compass 2022. URL:

https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
European Council (2021). Infographic - Terrorism in the EU: facts and figures. URL: https://www.consilium.europa.eu/en/infographics/terrorism-eu-facts-figures/ (Referenced 6.11.2022)

Forbes: The Global 2000. (12.5.2022). Referenced 5.11.2022. https://www.forbes.com/lists/global2000/?sh=6bc8cc815ac0

Funch, Christian. Chandler, David. (2020). Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data. University of Westminster Press.

Haque, A. (2015) Surveillance, transparency, and democracy : public administration in the information age. Tuscaloosa: University Alabama Press.

Heywood, Andrew. (2013): Politics. 4th edition. Palgrave Foundations.

Kocsi, I. (23.7.2022). Pegasus: A Spy Story Turning into a Nightmare. Balkan Insight. Balkan Investigative Reporting Network. URL: https://balkaninsight.com/2021/07/23/pegasus-a-spy-story-turning-into-a-nightmare/ (Referenced 5.11.2022)

Limnell, J (2009). Suomen uhkakuvapolitiikka 2000-luvun alussa. Strategia. Strategian laitos.

Tohtoriopiskelijan väitöskirja. Maanpuolustuskorkeakoulu. https://www.doria.fi/handle/10024/74110

Lundstedt, Tero. (April/2022): Demokratiapuolustuskannalla – tilannekuva vuonna 2022. Teoksessa: Diktaattorin käsikirja. Eli miten liberaalia demokratiaa puolustetaan. Ajatuspaja Libera, Helsinki.

Maras, M. (2010) How to Catch a Terrorist: Is Mass Surveillance the Answer?, Journal of Applied Security Research, 5:1, 20-41.

Miklóssy, Katalin. (April/2022): Autoritaaristen järjestelmien haaste ja EU:n dilemma: Puola ja Unkari. Teoksessa: Diktaattorin käsikirja. Eli miten liberaalia demokratiaa puolustetaan. Ajatuspaja Libera, Helsinki

Mikkola, Harri, Aaltola, Mika, Wigell, Mikael, Juntunen, Tapio ja Vihma, Antto. (May/2018): Hybridivaikuttaminen ja demokratian resilienssi - ulkoisen häirinnän mahdollisuudet ja torjuntakyky liberaaleissa demokratioissa. FIIA Report, Helsinki.

Nokkala, J (2020). Vaarojen valvonta vai valvonnan vaara? : suomalaisten suhtautuminen valtiovallan valvontaoikeuksiin. Pro gradu -tutkielma. Sosiologia. Jyväskylän yliopisto.

Panyi, S. (13.10.2022). Boosting of spying capabilities stokes fear Hungary is building a surveillance state. Balkan Insight. Balkan Investigative Reporting Network. URL:

https://balkaninsight.com/2022/10/13/boosting-of-spying-capabilities-stokes-fear-hungary-isbuilding-a-surveillance-state/ (Referenced 5.11.2022)

Pegg, David ja Cutler, Sam. (18.7.2021) What is Pegasus spyware and how does it hack phones? *The Guardian.*

https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

Qian, I; Xiao, M; Mozur, P; Cardia, A. (21.6.2022) *Four Takeaways From a Times Investigation Into China's Expanding Surveillance State.* The New York Times.

.https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html (Referenced 5.11.2022)

Sisäministeriö (2022). Siviilitiedustelulainsäädännön valmistelu. URL: https://intermin.fi/tiedustelu (Referenced 6.11.2022)

Uimonen, Risto. (2009) Median mahti - kuinka journalistit käyttävät valtaa ja pakottavat maan mahtavia eroamaan. WSOY.

Valtioneuvoston kanslia. (2019) Informaatiovaikuttamiseen vastaaminen. Opas viestijöille.

Väliverronen, Esa. (2015) Seppänen, Janne. Mediayhteiskunta. Vastapaino.

Wirth, J. Maier, C. Laumer, S. (2019): Justification of Mass Surveillance: A Quantitative Study O'Hara, Kieron, 'Policy Question: When Is Surveillance Justified?', Four Internets: Data, Geopolitics, and the Governance of Cyberspace.

World Justice Project. (2022) European Unions Top Court Rules Against Hungary and Poland in Rule of Law Showdown https://worldjusticeproject.org/news/european-union%E2%80%99s-top-court-rules-against-hu ngary-and-poland-rule-law-showdown

Yascha Mounk. (2018): *The People vs. Democracy. Why Our Freedom Is in Danger & How to Save It*. Harvard University Press.

Xu, Beina ja Albert, Eleanor. (2017) Media Censorship in China. *Council on Foreign Relations.* https://www.cfr.org/backgrounder/media-censorship-china

Zheng, S; Xu, X; Cao, X (2020). What explains popular support for government monitoring in China?

Zsiros, Sandor & Gill, Joanna. (2020) Hungary and Poland block EU's COVID-19 recovery package over new rule of law package. *Euronews.*

https://www.euronews.com/my-europe/2020/11/16/hungary-and-poland-threaten-coronavirusrecovery-package

Zuboff, Shoshana. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Public Affairs.*

Zuboff, Shoshana. (2015). Journal of Information technology: *"Big Other: Surveillance*

Capitalism and the Prospects of an Information Civilization." SAGE Publications London.