Przegląd Europejski – European Studies Quarterly, **ISSN: 1641-2478**
vol. 2024, no. 4

DOI: https://doi.org/10.31338/1641-2478pe.4.24.4

The right to privacy in a world of modern technology

Sylweriusz M. Królak, *Civil Rights Foundation (Warsaw, Poland)*
E-mail: s.krolak@wp.pl
https://orcid.org/0000-0001-7615-9745

Abstract
The nature and scale of interference with the right to privacy, which is carried out by public authorities in Poland, or by other entities with their consent, may take a systemic character. The use of modern surveillance tools and changes in legislation lead to the intensification of such practices. Such actions are contrary to the legal acquis and values, on which the European system of protection of human rights and the European Union are based. Against the background of legislative activities conducted in Poland and the European Union, the author has attempted to outline the threats to the right to privacy that arise in connection with the use of new technologies, whereby the described phenomena are presented from a vertical and horizontal perspective. Within the framework of the work, the result of which is described in the publication, a study of the relevant provisions of Polish law (in force and projected) and the instruments of the EU and the Council of Europe was carried out. For this purpose, the legal-dogmatic method and qualitative comparative studies were used. In addition, the legal-empirical research technique was used, including indirect observation and analysis of source documents.
Keywords: human rights, right to privacy, protection of privacy, personal data, Council of Europe, European Union, Poland

Prawo do prywatności w świecie nowoczesnych technologii

Streszczenie
Charakter i skala ingerencji w prawo do prywatności, które są dokonywane przez władze publiczne w Polsce, lub za ich przyzwoleniem przez inne podmioty, może przybrać charakter systemowy. Stosowanie nowoczesnych narzędzi inwigilacji oraz konsekwentne zmiany ustawodawstwa sprzyjają intensyfikacji takich praktyk. Tego rodzaju działania są sprzeczne z dorobkiem prawnym oraz wartościami, na których osadza się europejski system ochrony praw człowieka oraz Unia Europej-

ska. Na tle działań prawodawczych prowadzonych w Polsce i Unii Europejskiej, autor podjął próbę zarysowania zagrożeń dla prawa do prywatności, jakie powstają w związku z wykorzystaniem nowych technologii, przy czym opisywane zjawiska ujęto w perspektywie wertykalnej i horyzontalnej. W ramach prac, których wynik opisano w publikacji, przeprowadzono badanie odnośnych przepisów prawa polskiego (obowiązujących i projektowanych) oraz instrumentów Unii Europejskiej i Rady Europy. W tym celu zastosowano metodę prawno-dogmatyczną oraz komparatystykę jakościową. Ponadto, wykorzystano technikę badań prawno-empirycznych, obejmującą obserwację pośrednią oraz analizę dokumentów źródłowych.
Słowa kluczowe: prawa człowieka, prawo do prywatności, ochrona prywatności, dane osobowe, Rada Europy, Unia Europejska, Polska

The difficult experience of recent years have revealed a new dimension of the challenges and threats facing civil society and each of us as participants in it. In fact, there is no area of our well-being that is not currently subject, to a greater or lesser extent, to a process of accelerated erosion. This is accompanied by axiological disputes and attempts to redefine many of the achievements of civilisation and social institutions (for more details, see: Królak 2022: p. 173–176). All too often, this leads in practice to a retreat from the ideas of Freedom – Equality – Solidarity (Fraternity), as these values, to varying degrees, are constrained by the force of objective events or subjective intentions behind the actions of the authorities of individual states and entities constituting sufficiently powerful interest groups. A noticeable effect of the changes is the deteriorating situation in Europe in the sphere of public services, e.g. in health care, social security or housing (see: Bryx et al. 2021), which undermines the material guarantees of human rights of a socio-economic nature, thus threatening equality and social solidarity. Even if the negative phenomena in the sphere of socio-economic rights could be considered transient and a consequence of events such as the COVID-19 pandemic or the situation in Ukraine (although there would be many arguments against such a thesis and point to their long-term, systemic nature), the erosion of political and civil rights cannot be justified by *ad hoc* causes. While „equality" and „solidarity" are not openly attacked, but rather subjected to constant, stealth attacks, undermining their meaning and significance in social practice, the idea of „freedom" and its concrete manifestations, protected by the provisions of the *European Convention on Human Rights* (hereinafter also: ECHR, see: Convention…1950) and the *Charter of Fundamental Rights* (hereinafter also: Charter, see: Charter of Fundamental Rights 2007), have in recent years been, and sometimes still are, openly contested by the authorities of some states that are not only members of the Council of Europe (CoE), but – like e.g. Poland and Hungary – also members of the European Union (EU).[1]

[1] Since this publication refers to both EU law and the ECHR, it is important to note here the specificity of the legal situation with regard to the binding of the EU and its Member States to the ECHR. The EU recognises the Council of Europe as a pan-European reference source in the field of human rights. This fact opens the possibility for multifaceted interaction between the CoE and the EU in various areas of human rights protection. The EU's accession to the *European Conven-*

The scope of this article does not allow for even a very brief presentation of the problem of restriction of the sphere of human freedom by the state or supranational corporations, therefore the subject of further discussion is only one of the important and, as it seems, current aspects of this phenomenon connected with threats to the right to privacy arising from the application of new technologies used against a citizen, at the same time relating these considerations to the legislative activities undertaken in the European Union and in Poland.

Historically, at the beginning of the 21st century, European societies, while not losing sight of the need to control the actions of their own, generally democratically elected governments, were more concerned about the actions of multinational companies operating simultaneously in several jurisdictions and thus beyond effective control. Later, however, this situation was to change under the influence of the authoritarian populisms that were gaining influence over the exercise of power in successive Member States of the European Union and the Council of Europe. This dualism necessitates a dual perspective, both in terms of research and legislation. In principle, the human rights norms of the ECHR, including the right to privacy (Article 8), are an obligation of the Member States and are vertically implemented, as they define the relationship between the state and the citizen. However, as our personal data (or, more broadly, information about us) has also become a valuable and massive commodity on the international market, it is impossible to avoid legislative intervention horizontally, i.e. in the relationship between individuals, especially when there are significant inequalities between them. This concept is not new, as it underpins all of European competition and consumer protection law, as well as international data protection instruments. However, the gap in the horizontal application of data protection rules, at least for EU countries, was only filled with the adoption of Article 8 of the *Charter of Fundamental Rights of the European Union*.[2] Until then, only the application of Article 8 ECHR was possible. It now seems clear that the addressee of the order (injunction) in Article 8(2) of the Charter is not only EU Member State, but also another entity, if it processes data of persons residing on the territory of those states.[3]

---

tion on Human Rights became possible in the light of the provisions of the Lisbon Treaty and, in the opinion of many researchers, would definitely contribute to ensuring coherence in the field of human rights in Europe (see: Buchowska 2014; Półtorak 2014; Karski 2008; Krzemińska 2005; Mik 2011; Kellerbauer et al. 2019: p. 2255).

[2] *Article 8 - Protection of personal data:* "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

[3] As an aside, it should be noted that the regional European system for the protection of human rights is a multicentric system. Institutionally, there are three organisations operating in its framework: The Council of Europe, the European Union, and the Organisation for Security and Cooperation in Europe, each with its own acquis. Some researchers draw attention to the essence of the relationship between the Charter and the Convention, for example: "Although the fundamental rights protected under the ECHR are part of Union law as its general principles, and the Charter itself prescribes an equal interpretation of the rights arising simultaneously from the CFR and the ECHR, the Convention, until the Union accedes to it, does not constitute an act

A consequence of the above is, *inter alia*, a certain difference in meaning between the concepts of 'human rights' and 'fundamental rights', however, for the purposes of this publication the former concept will be used.

The eminent human rights expert Wiktor Osiatyński points out that unlike many other moral rights or rights granted by law, human rights are claimed by the state. Human rights regulate the relationship between the individual and the state, its organs and functionaries exercising power at various levels. Human rights can fulfil three functions. The first is the protection of the individual's freedom against its violation by the state, the second is the need for the state to create opportunities for the realisation of the individual's rights, and the third is the protection by the state of the individual's rights and freedoms against their violation by others (Osiatyński 2012: p. 2–3). In the light of these observations, the horizontal aspect is primarily linked to the ability of the individual to claim the safeguarding of his or her rights against infringements by third parties at the latter level. At the same time, this will be linked to the possibility of claiming not only against the state, but above all against the third party committing the violation of our rights.

Horizontal perspective

Already in May 2018, i.e. with the entry into force of the modern and groundbreaking rules contained in Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (hereinafter also: GDPR; see: Regulation (EU) 2016/679), it became clear that further legislation would be necessary with regard to all electronic communication channels and the data and metadata obtained through them. This is particularly true of the growing phenomenon of tracking the activities of Internet users and processing all kinds of information about them. This has taken advantage of a false sense of freedom and the belief of individuals that they will remain anonymous without incurring significant costs. Meanwhile, new forms of activity, including the use of social media and instant messaging (even encrypted ones), make it possible, thanks to ever-improving technologies, for service providers to make unlimited commercial use of the knowledge they have acquired about us. Public authorities, in turn, are gaining control of or extensive access to the information collected by service providers, often against our will. Thus, on the one hand, citizens fall victim to the expropriation of their data by technology companies with the intention of monetising it, and on the other hand, part of the data acquired is subject to a forced form of "leasing" or even nationalisation by the state with a view to its further use in the process of exercising power (state control over the individual). The two processes now appear to be inseparable, but the legal regime governing the relationship between the individual and the technology company and the individual and the public authority is different.

formally binding on the legal order of the Union." (Czapliński 2021: p. 343; own author's translation from Polish to English).

In this situation, the European Union, with its limited competence under the Treaties to effectively regulate the internal security sphere of the Member States, must at least intervene in the relationship between the service provider and the consumer (personal data subject). Even if the changes introduced so far are still modest compared to the existing needs, they continue to give rise to controversies expressed by the protagonists of technology companies, especially the so-called GAFAM[4] (also known as Big Tech).

Legal solutions aimed at protecting the privacy of citizens are criticised on the grounds that they threaten the freedom of the market, restrict competition, deprive companies of the opportunity to reach potential customers and have a disastrous impact on the economy. Any restrictions, even modest ones, where there were hardly any before, must be irritating, all the more so when the strengthening of citizens' rights is accompanied by a fall in company profits. At the same time, it must be weighed against the fact that free access for the big players to potentially „everything" about us poses specific risks – not only in terms of protecting the information we would like to keep to ourselves. After all, a lot of things are happening outside our awareness, and therefore outside our ability to influence the course of events, and are penetrating ever deeper into the personal and domestic spheres of each individual. How often do we move away from email or mobile phones in the hope that alternative electronic communication solutions will allow us to avoid surveillance or simply protect our privacy. However, it is just as easy to obtain data on any user, simply by having access to the technology to do so.

This is not the end of the story, however, as we face further challenges from a phenomenon such as the Internet of Things (IoT).[5] Our home appliances, which are connected to the Internet and communicate with the outside world without our participation, also provide knowledge about us and our habits. This knowledge can be used to our advantage, making our lives easier and helping to create an intelligent environment full of energy-saving and eco-friendly solutions. But it can also be "misused", used against our intentions, or even against the noble intentions of the creators of certain technologies. There is a great deal to be awared about our daily activities, tastes and needs by harnessing the knowledge provided by electronic devices and household appliances. This alone, when collected and processed, becomes potentially dangerous in itself, giving third parties access to sensitive knowledge about a specific user, potentially every citizen.

---

4 Nikos Smyrnaios proposed an expansion of this term in 2016. According to him, GAFAM (*Google, Amazon, Facebook, Apple, Microsoft*) appears to take control of the internet by concentrating market and financial power, applying patent and copyright laws, using the principles of capitalism. He further stated that Asia's largest corporations *Samsung*, *Alibaba* and *Tencent* could or should be included in the concept. He also noted that four key phenomena allowed GAFAM (Big Tech) to emerge: media and technological convergence, globalisation, economic deregulation, and financialisation (Smyrnaios 2016: p. 61–83).

5 For more details – see: Greser 2022.

Vertical perspective

The so-called 'Pegasus affair', which involved the revelation of the clandestine use of spyware in Poland and Hungary (Decision (EU) 2022/480), Switzerland, Latvia and Croatia[6] as a tool for offensive action in foreign anti-terrorist and intelligence operations, has provided a powerful and highly topical impetus for reflection on the philosophy that should guide legislative activity in the area of privacy, and in particular the protection of personal data. However, this important context does not limit the scope of the necessary debate. Firstly, because the use of *Pegasus* by the Republic of Poland for internal purposes is not only a violation of the principles of the protection of privacy (Art. 8(1) ECHR; Art. 7 and 8 of the Charter), but also a violation of the rule of law and the legality principle (Art. 2 and 7 of the Constitution of the Republic of Poland, see: Konstytucja RP 1997), the prohibition of abuse of rights (Art. 17 ECHR and Art. 54 of the Charter) and a violation of the principle of proportionality (Art. 8(2) ECHR and Art. 52 par. 1 of the Charter), the principle of freedom of expression, including the right to receive and impart information and ideas without interference by public authorities (Article 11 of the Charter), the violation of the right to an effective remedy and to a fair trial (Art. 6 ECHR and Article 47 of the Charter) and of the right to an effective remedy (Article 13 ECHR) and, through the monitoring of the opposition during the election campaign, also of the principle of free elections (Article 3 of Protocol No. 1 ECHR) and of freedom of political activity (Article 11 ECHR).

Secondly, the use of *Pegasus* has become a blatant, but not the only, example of the use of modern technology by the state to gain as much knowledge as possible about citizens through the collection and processing of personal data, the amount and scope of which, in the conditions of a democratic society, is disproportionate to the purpose declared by the public authority. In this context, the Polish authorities, contrary to public opinion, consistently engage in other activities that serve a questionable purpose from the perspective of human rights protection, namely the collection of sensitive data about fellow citizens. Examples include the collection of data in the Medical Information System (see: Skindzier 2022; *Tak będzie działał rejestr ciąż* 2022), which is disproportionate in relation to legitimate needs, or the draft law amending the Electoral Code to create, *inter alia*, a central register of voters (see: Sejm RP 2023a).

It must be worrying that the aforementioned way of building relations between the state and citizens, as currently intended by the authorities, may soon become a permanent action, carried out on the basis of the law and within its limits. There is much to suggest that, in the wake of the Pegasus affair, an attempt is being made to create a „get out of jail free" card, guaranteeing impunity for all those involved in surveillance. This would have

---

[6] "According to a report by *Citizen Lab*, an organisation under the umbrella of the University of Toronto in Canada, there are five *Pegasus* software operators in Europe that conduct activities focused, experts say, on targets located in Poland, Switzerland, Latvia, Hungary and Croatia. According to the report, listening activities against targets located on the territory of the Republic of Poland are carried out by an operator codenamed 'ORZELBIALY'." (*Oprogramowanie szpiegowskie Pegasus…* 2018, own author's translation from Polish to English).

been the case if the government's draft law on electronic communications (see: Sejm RP 2023b), which would have given the special services additional powers to collect information on citizens, had been passed (see: Kunert, Jaźwiński 2023). Among other things, the draft law would have given the secret services access to instant messengers, IP addresses, login locations and the content of e-mails, while requiring not only telecommunications companies but also providers of e-mail and other Internet services to send data on users to the services (Jaroszewski 2023). In the public discussion that followed the announcement of the government's draft, it was argued that judicial control over the work of the secret services would become illusory in this respect.[7] The judiciary pointed to the following as potential areas of abuse by the services: the possibility of exercising operational control beyond the material scope of the authorisation granted by the court; retrospective data collection; manipulation of authorisations that do not reveal a person's identity; incomplete (selective) material presented by the services in the context of an application for authorisation for operational control (Ivanova 2022).

Such a legislative approach, however, clearly contradicts the spirit and the letter of the Polish Constitution, the ECHR, but also the Charter of Fundamental Rights and, consequently, the legislation of the European Union. This is the case despite the fact that EU legislation is not free from its own errors and despite the fact that EU legal acts are characterised by a considerable degree of pragmatism. As a result, the legal instruments adopted by the EU over the years have not been free of solutions that primarily serve public security, sometimes even to the detriment of the protection of individual rights. However, even the „notorious" Directive 2006/24/EC on the retention of data in ICT systems (see: Directive 2006/24/EC), which was annulled by the Court of Justice of the European Union (CJEU) (see: Judgment 2014: par. 37 *in fine*), did not pose such a threat to the protection of human rights as the Polish draft law on electronic communications. Under Directive 2006/24/EC, EU Member States had to store information on all citizens' telecommunications data (telephone and internet connections) for at least six months, but no longer than twenty-four months, in order to make it available to police authorities upon request. Police and security authorities had the right to request access to information such as IP addresses and the time of use of every email, phone call and text message sent or received. There was no provision in the Directive for judicial control of access to the data, but on the other hand the data stored did not include the content of conversations and correspondence, and was therefore limited to so-called metadata, unlike the Polish draft law on electronic communications (Judgment 2014: par. 37 *in fine*).

In addition to the lack of effective judicial control over access to data, one of the main reasons for the CJEU's decision of 8 April 2014 in cases C-293/12 and C-594/12 (Judgment 2014) was that the Directive violates the fundamental rights to respect for private life and the protection of personal data in a particularly serious way. Moreover, the fact that data

[7] Prof. Łętowska, analysing the hearing against Poland at the European Court of Human Rights, alarmed: "In view of the passivity of the courts deciding on surveillance, judicial control of the activities of the police and intelligence services is reduced to a legitimising fiction" (Łętowska 2022, own author's translation from Polish to English).

is stored and then used without the subscriber or registered user being informed is likely to give rise to the feeling that their private life is under constant surveillance (Judgment 2014). At the same time, he pointed out that, in adopting the Data Retention Directive, the EU legislature had overstepped the limits set by the principle of proportionality. Although the retention of data provided for by the directive may be regarded as appropriate for the attainment of the objective pursued by the directive, the extensive and particularly serious interference with the fundamental rights in question provided for by the directive is not sufficiently limited to ensure that the interference is actually carried out within the limits of strict necessity (Judgment 2014: par. 51–52). The Directive covers all natural persons, all means of electronic communication and all traffic data, without any differentiation, limitation or exception in the light of the objective of combating serious crime. It does not lay down any objective criterion to ensure that the competent national authorities have access to the data and may use them only for the purpose of the prevention, detection or prosecution of criminal offences which, having regard to the extent and gravity of the interference with fundamental rights in question, can be considered sufficiently serious to justify such interference. The Directive does not lay down objective criteria for determining the duration of data retention in order to ensure that it is limited to what is strictly necessary. The Court also found that the Directive did not provide sufficient safeguards to ensure effective protection of the data against the risk of misuse and against any unlawful access to and use of the data (Judgment 2014: par. 56–69).

The content of the Digital Rights Ireland judgment appears to be particularly important and topical for the assessment of the Polish legislator's legislative measures. Despite the fact that on 21.04.2023 the governmental draft – the *Electronic Communications Act*, which was the subject of Project No. 2861, was withdrawn from parliamentary consideration, this does not mean that the Government of the Republic of Poland has abandoned solutions that are detrimental to human rights. According to representatives of the authorities, the future draft will not contain any provisions on television at all, but will still contain provisions on telecommunications and electronic communications[8]. In the light of the above, however, there can be no doubt that both the *Pegasus* case and the legislative initiative in this matter testify to a significant axiological shift on the part of the Polish authorities away from the values on which the European system of human rights protection and the European Union itself was founded[9].

---

[8] Minister Lewandowski informs: "There will not be a section on television at all. The draft will only include those issues that were in it before the Council of Ministers was proceeding with it. Issues concerning telecommunications, electronic communications. The elements added at the Council of Ministers at the request of the Minister of Culture and National Heritage will be missing" (*Nie będzie Lex Pilot…* 2023, own author's translation from Polish to English).

[9] By acting in breach of the Treaty on European Union (TEU), and in particular Articles 2, 6 and 21 of the Treaty. According to Article 2 TEU: "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail." Article 21(1) TEU, on the other hand, indicates that the principles, on which the Union has been founded, developed and enlarged, "and which it seeks to advance

Conclusions

It is clear that, in a period of rapid civilisational change and technological development, legal regulations have not kept pace with the needs of life, even everyday life, let alone the needs arising from professional practice. To make matters worse, contemporary legislation in the European states is struggling with two strong, sometimes contradictory trends, which in itself does not make it easier to find quick solutions to new challenges.

The first trend in legislation stems from the constant development and refinement of freedoms and human rights on European soil, among which the freedom and protection of the confidentiality of communications, the right to protection of private life or, more generally, the right to respect for the dignity of every human being is gaining particular importance in the context of the development of the Internet and digital technologies. This trend is reflected in the increasingly effective legal instruments for the protection of personal data on European soil.

The second, competing trend in legislation is dictated by the desire to implement a demand that is as strong in public perception as personal freedoms and the right to privacy, namely the demand for security, understood both as a personal right of the individual and, more broadly, as collective security.

While the first trend seeks to tame the 'element' and make technological solutions and practices applied to citizens by state bodies or corporations friendly to the individual, the second trend of legislation emphasises collective rights and does not so much limit as seek to exploit the emerging technological possibilities, harnessing them in the service of the state and sometimes even creating opportunities for their abuse or use in the economic interests of large players, especially those operating on a global scale. Strong ideological support for this second mode of regulation is provided by society's desire for security, which is particularly topical in the face of threats from terrorism, hostile activities by neighbouring states or organised transnational crime. Drastic breaches of public security in Europe tend to push the boundaries of social tolerance in a direction that favours all-encompassing state control. On the other hand, a well-publicised case of gross abuse of civil rights leads to a temporary intensification of pro-freedom sentiments.

Against this background, it is becoming increasingly clear that the great project that the European Union has been pursuing since the beginning of the 21st century, defined as Europe – Area of Freedom, Security and Justice, is an axiological and legislative attempt to reconcile fire with water. The problem is not so much the abstract nature of the demand for freedom *versus* the equally abstract demand for security. After all, most of us are able to translate them, if only intuitively, into the language of the everyday practice we want in our lives. The real problem we have, however, is in drawing the mutual

in the wider world: democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the United Nations Charter and international law" (TEU: art. 21, par. 1).

boundaries between these categories. As a result, we are much worse off when it comes to determining how much freedom and how much security we want for ourselves personally. When such a dilemma becomes part of the public debate about the relationship between the individual, society and the state, the matter becomes even more difficult. The caveat, however, is that some actions on the part of states are intensely excessive and cannot be justified by a conflict of values (liberty *versus* security) or by acting in a state of overriding necessity, because they exceed all frameworks of action necessary in a democratic society and are dramatically disproportionate to the stated purpose they purport to serve (Jaskiernia 2020: p. 631).

Unsurprisingly, these issues are constantly being debated by representatives of the interests of individual governments, social groups or political parties. There are also other, increasingly powerful pressure groups in the arena. Let us not forget that the modern world is a relatively single, globalised market, and our rights and freedoms, which seem to us invaluable and, as such, inalienable, come at a considerable price to some less sentimental players. As a result, fair legislation is too often sacrificed on the altar of political or economic calculations.

Law, democracy and the market share certain characteristics. One such feature is volatility over time, the dynamism that results from a state of constant social and civic play. Consequently, in a democratic society, some will do only as much and as little as others allow them to do. To this end, democratic institutions, including civil society and its members, cannot, by their very nature, remain passive observers of events, waiting for the outcome of national and European procedures (legislative, electoral, referendum, judicial, etc.), but should be active participants in them. The alternative could be the omnipotence of the State, illegally restricting the sphere of our privacy or arbitrarily violating our civil liberties, which necessarily constitutes a denial of the rule of law. In such a reality, therefore, it would no longer be possible to speak of a democratic state under the rule of law, which embodies the principles of social justice (Konstytucja RP: Art 2).

Sylweriusz M. Królak – PhD., university lecturer and lawyer, a member of the Civil Rights Foundation and the College of the Supreme Audit Office. Former Deputy Minister of Justice (2001–2005) and former member of the State Tribunal (2005–2015). He specialises in European law, economic and constitutional law, combating unfair competition, health protection law, EU pharmaceutical market regulations, arbitration proceedings and the European Civil Procedure. He is also an expert in the field of human rights protection, protection of personal data, privacy, modern technology law, management of legal security of enterprises. He is the author of the monograph: *Komisarz Praw Człowieka Rady Europy jako podmiot oddziałujący na ochronę praw człowieka w państwach członkowskich* (Toruń, 2022) and other publications in the field of human rights, European law, and the judicial system in Poland.

Sylweriusz M. Królak – doktor nauk prawnych, wykładowca akademicki oraz adwokat, członek Fundacji Praw Obywatelskich oraz Kolegium Najwyższej Izby Kontroli. Były wiceminister sprawiedliwości

(2001–2005) oraz były członek Trybunału Stanu (2005–2015). Specjalizuje się w prawie europejskim, gospodarczym i konstytucyjnym, zwalczaniu nieuczciwej konkurencji, prawie ochrony zdrowia, unijnych regulacjach rynku farmaceutycznego, postępowaniu arbitrażowym oraz europejskiej procedurze w sprawach cywilnych. Jest również ekspertem w zakresie ochrony praw człowieka, ochrony danych osobowych, prywatności, prawa nowoczesnych technologii, zarządzania bezpieczeństwem prawnym przedsiębiorstw. Autor monografii *Komisarz Praw Człowieka Rady Europy jako podmiot oddziałujący na ochronę praw człowieka w państwach członkowskich* (Toruń, 2022) oraz innych publikacji z zakresu praw człowieka, prawa europejskiego oraz ustroju sądownictwa w Polsce.

References:

BRYX Marek, SOBIERAJ Janusz, METELSKI Dominik, RUDZKA Izabela (2021), *Buying vs. Renting a Home in View of Young Adults in Poland*, "Land", vol. 10, issue 11. DOI: 10.3390/land10111183

BUCHOWSKA Natalia (2014), *Starania Unii Europejskiej o przystąpienie do Konwencji o ochronie praw człowieka i podstawowych wolności,* „Przegląd Zachodni", no. 4 (353).

CHARTER OF FUNDAMENTAL RIGHTS (2007) of the European Union, OJ C 303, 14.12.2007

CONVENTION for the Protection of Human Rights and Fundamental Freedoms (1950), Rome, 4 November 1950, subsequently amended by Protocols No. 3, 5 and 8 and supplemented by Protocol No. 2, Dz. U. 1993 Nr 61, poz. 284.

CZAPLIŃSKI Władysław (2021), *Znaczenie orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej w procesie rozwoju prawa europejskiego*, Warszawa.

DIRECTIVE 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.04.2006.

DECISION (EU) 2022/480 of the European Parliament of 10 March 2022 on setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee, OJ L 98, 25.03.2022.

GRESER Jarosław (2022), *Wybrane problemy funkcjonowania Internetu Rzeczy w relacji do praw człowieka,* w: B. Gronowska, P. Sadowski (red.), *25-lecie wejścia w życie Europejskiej Konwencji Praw Człowieka w Polsce*, Toruń.

IVANOVA Ewa (2022), *Afera Pegasusa. Ujawniamy, jak w praktyce wygląda kontrola sądu nad operacjami służb*, "Gazeta Wyborcza", https://wyborcza.pl/7,75398,27996593,sedziowie-kontrola-sadu-nad-sluzbami-to-fikcja.html (13.01.2022).

JAROSZEWSKI Damian (2023), *Rząd przeszuka smartfony Polaków. Sądy ostrzegają*,"Telepolis", https://www.telepolis.pl/tech/wydarzenia/inwigilacja-obywateli-nowa-ustawa-sady (24.01.2023).

JASKIERNIA Jerzy (2020), *Funkcje Konstytucji RP w dobie integracji europejskiej i radykalnych przemian politycznych*, Toruń.

JUDGMENT of the Court (2014), 8 April 2014, in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI identifier: ECLI:EU:C:2014:238

KARSKI Karol (2008), *Przystąpienie Unii Europejskiej do Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności,* w: Irena Głuszyńska, Kazimierz Lankosz (red.), *Rada Europy – 60 lat na rzecz jedności europejskiej,* Bielsko-Biała.

KUNERT Jan, JAŹWIŃSKI Piotr (2023), *Służby inwigilują obywateli pod kontrolą sądów? Nie, to kontrola iluzoryczna*, "Konkret24", https://konkret24.tvn24.pl/polska/inwigilacja-sluzby-inwigiluja-obywateli-pod-kontrola-sadow-nie-to-kontrola-iluzoryczna-6638879 (22.01.2023).

KONSTYTUCJA RZECZYPOSPOLITEJ POLSKIEJ (1997) z 2 kwietnia 1997 r., Dz.U. 1997 nr 78 poz. 483 ze zm., https://www.sejm.gov.pl/prawo/konst/polski/kon1.htm (11.10.2024).

KRÓLAK Sylweriusz M. (2022), *Komisarz Praw Człowieka Rady Europy jako podmiot oddziałujący na ochronę praw człowieka w państwach członkowskich*, Toruń.

KRZEMIŃSKA Joanna (2005), *Luksemburg kontra Strasburg? Przystąpienie Unii Europejskiej do Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności,* „Radca Prawny", no. 1.

KELLERBAUER Manuel, KLAMERT Marcus, TOMKIN Jonathan (2019) (eds.), *The EU Treaties and the Charter of Fundamental Rights: a commentary*, Oxford. DOI: 10.1093/oso/9780198794561.001.0001

ŁĘTOWSKA Ewa (2022), *Wobec bierności sądów decydujących o inwigilacji sądowa kontrola działań policji i służb wywiadowczych zostaje sprowadzona do legitymizującej fikcji*, https://archiwumosiatynskiego.pl/wpis-w-debacie/letowska-o-inwigilacji-m-in-pegasusem-sadowa-kontrola-to-fikcja-sluzby-moga-robic-co-chca/ (02.10.2022).

MIK Cezary (2011), *Przystąpienie Unii Europejskiej do Europejskiej konwencji praw człowieka,* w: C. Mik, M. Balcerzak, T. Jasudowicz, J. Kapelańska-Pręgowska (red.), *Europejska konwencja praw człowieka i jej system kontrolny - perspektywa systemowa i orzecznicza*, Toruń.

NIE BĘDZIE LEX PILOT. Rząd wycofuje się z przepisów ws. telewizji (2023), „Rzeczpospolita", https://www.rp.pl/prawo-dla-ciebie/art38348631-nie-bedzie-lex-pilot-rzad-wycofuje-sie-z-przepisow-ws-telewizji (19.04.2023).

OPROGRAMOWANIE SZPIEGOWSKIE PEGASUS wykryte w 45 krajach, w tym w Polsce (2018), https://cyberdefence24.pl/polityka-i-prawo/oprogramowanie-szpiegowskie-pegasus-wykryte-w-45-krajach-w-tym-w-polsce (27.01.2023).

OSIATYŃSKI Wiktor (2012), *Wprowadzenie do praw człowieka*, Helsińska Fundacja Praw Człowieka, https://www.ce.uw.edu.pl/wp-content/uploads/2018/10/3.-prawa-czlowieka-wiktor-osiatynski_wprowadzeniedopojeciaprawczlowieka.pdf (03.10.2018).

PÓŁTORAK Nina (2014), *Przystąpienie do Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z perspektywy Unii Europejskiej,* w: *Obywatel w Radzie Europy i Unii Europejskiej,* Warszawa.

REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.05.2016.

SKINDZIER Oliwia (2022), *Rejestr ciąż — co oznacza w praktyce?* https://www.money.pl/gospodarka/rejestr-ciaz-co-oznacza-w-praktyce-6776882271259200a.html (26.08.2022).

SMYRNAIOS Nikos (2016), *L'effet GAFAM: stratégies et logiques de l'oligopole de l'internet,* "Communication et Langages", vol. 2016/2, no. 188. DOI: 10.4074/S0336150016012047

SEJM RP (2023a), Rządowy projekt ustawy o zmianie ustawy - Kodeks wyborczy, Druk Sejmowy nr 265, https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?nr=2651 (26.01.2023).

SEJM RP (2023b), Rządowy projekt ustawy - Prawo komunikacji elektronicznej, Druk Sejmowy nr 2861, https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?id=66C7F7C637867159C12589170035C136 (21.04.2023).

TAK BĘDZIE DZIAŁAŁ REJESTR CIĄŻ. Węcławik: Te dane od dawna są widoczne w dokumentacji medycznej (2022), „Dziennik Gazeta Prawna", https://serwisy.gazetaprawna.pl/zdrowie/artykuly/8452766,rejestr-ciaz-dane-jak-to-dziala.html (13.06.2022).

Received: 02.10.2023. Accepted: 05.12.2024.