Przegląd Prawa Konstytucyjnego
-----ISSN 2082-1212-----
DOI 10.15804/ppk.2021.06.38
-----2021, No. 6 (64)-----

Katarzyna Chałubińska-Jentkiewicz[1]

On-line Anonymity Versus Access to Private Data as the Constitutional Right

Keywords: Private data, data protection, human rights, anonymity, freedom of speech, public interest
Słowa kluczowe: dane osobiste, ochrona danych, prawa człowieka, anonimowość, wolność słowa, interes publiczny

Abstract

Cyberspace seems to be ubiquitous. It coexists with the real world and it constitutes its coded zero-one reflection. However, it deprives us of privacy, our constitutional right. Even more, the modern technology allows our fingerprint to be traced forever. Problems with maintaining online privacy in the face of the phenomenon of identity theft for criminal purposes, or the use of our data for property purposes in the broadly understood internet marketing.

Streszczenie

Anonimowość on-line a dostęp do danych prywatnych jako prawo konstytucyjne

Cyberprzestrzeń wydaje się wszechobecna, bowiem współistnieje ze światem rzeczywistym i stanowi jego zakodowane zero-jedynkowe odbicie. Pozbawia nas jednak prywat-

[1] ORCID ID: 0000-0003-0188-5704, Assoc. Prof., Department of Cybersecurity Law and New Technologies Law, Law Institute, War Studies University in Warsaw. E-mail: k.jentkiewicz@akademia.mil.pl.

ności, naszego konstytucyjnego prawa. Co więcej, nowoczesna technologia umożliwia śledzenie naszego śladu w sieci na zawsze. Kluczowym problemem staje się zachowanie prywatności w sieci, prawa konstytucyjnie chronionego, w obliczu zjawisk kradzieży tożsamości w celach przestępczych, czy wykorzystywanie naszych danych do celów majątkowych w szeroko rozumianym marketingu internetowym.

*

Anonymity on the web is as durable as a footprint in the sand scooped by a tidal wave – it can stay in place, but it won't be what it was before the sea swallowed it. Even more, the modern technology allows our fingerprint to be traced forever. Many people think that when sitting in front of their computer in the comfort of their own home, with a cat on their lap and logging into the system they are still managing to maintain their privacy. Problems with maintaining online privacy in the face of the phenomenon of identity theft for criminal purposes, or the use of our data for property purposes in the broadly understood internet marketing is one side of these considerations.

According to the Polish language dictionary – PWN – anonymity means: not revealing one's surname or unknown by surname, one whose author or perpetrator is unknown, involving unknown or indistinguishable people[2]. Technically speaking, every computer which gains access to the network has its unique identifier – Internet Protocol address. Of course, it is possible to camouflage the IP address using appropriate encryption software or a network using the so-called onion routing (TOR). This term defines multidimensional data encryption and sending them through proxy servers called network nodes. This term defines multidimensional data encryption and sending them through proxy servers called network nodes. Anonymity on the web is also not explicitly guaranteed in the Polish legislation. At the same time, the IP number is not the basis for recognizing its holder as the perpetrator of the act. Of course, the user can assert his rights, if these are violated. He has the right to do so under constitutional provisions, however, the Polish legislator

[2] http://sjp.pwn.pl/szukaj/anonimowo%C5%9B%C4%87.html (5.05.2021).

has imposed a legal obligation on telecommunications undertakings in the collection of data on the network users.

It should also be noted that these data can only be made available on the basis of a reasoned request, i.e. through court proceedings for which they are relevant. Such access must, as a rule, take place on the basis of an order or request from the party concerned. The process of collecting and storing telecommunications data, commonly known as data retention, raises a lot of controversy, as it is inevitably associated with the concept of anonymity on the web. Data retention can be defined as a process in which a telecommunications service provider is obliged by law to store information about connections made by the user. These data must be, by law, made available, as needed, to the authorized bodies to detect and fight cybercrime.

The above-mentioned regulations are provisions on various aspects and ways of entering the privacy of an individual by the executive authority, in the scope of its constitutionally regulated freedom of communication and protection related to the private sphere, exercising its powers through investigative operations. These activities are inherently non-public (also towards the person who is interested), carried out in conditions that give the police a wide margin of discretion, with limited guarantees for the rights of the person subjected to these activities, as well as limited external control, including judicial control. The transparency of the operational activities would render them ineffective.

The modern state, obliged to ensure security (which is also a constitutional obligation), faces a difficult task due to the threat of terrorism and crime (including organized crime). Technical facilities affecting the speed of communication and movement can be used to protect the security of the state but they can also be taken advantage by criminals. Police operational activities, regulated in the ordinary legislation, carried out in closed-security conditions, remain in natural, irremovable conflict with some of the individual's fundamental rights. This applies in particular to the individual's right to privacy, constitutional freedom of communication and related protection of the secret of communication, protection of the autonomy of information (which in Poland is determined by Art. 49 and 51 of the Polish Constitution[3]), as well as

[3] Dz.U.No. 78, item 483 as amended.

with the constitutional guarantee of the legal protection of individual rights. This conflict is widespread and is known in all democratic states of law. Thus, taking into consideration the practice of international bodies, where – with Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms in the background – a universal standard has been developed to assess the proportionality between the interference of the authorities and the rights of an individual.

The experience of modern democratic states indicates that the executive authority responsible for public security and order, including its subordinate entities conducting investigative operations, has at its disposal the means which, in the name of defending public order, may lead to the destruction of democratic institutions and violate human and civil rights and freedoms. Therefore, constant control and monitoring of these activities is necessary to prevent this from happening. Legal instruments defining the degree and boundaries of such interference seem necessary here. Public security, as the good which, in principle, justifies the legislator's limitation of the exercise of civil freedoms, requires keeping the proportionality of permissible intrusion in the name of protecting security and an efficient system of monitoring whether this proportionality is maintained in practice[4].

Otherwise, the measures of protecting this security, in the form of legally permissible operational activities, pose a threat to these freedoms themselves. This may be the case when, firstly, the restrictions imposed will be arbitrary, disproportionate to possible threats and, secondly, when they are excluded (whether legally or de facto) from the control exercised by democratic institutions. The Constitutional Tribunal in the judgment of December 15, 2004[5] indicates that Art. 31 sec. 3 of the Polish Constitution is a precise definition of admissible restrictions on exercising the freedoms and rights of the individual. They include the following:

– statutory form of restrictions,

[4] See: L. Garlicki, *Przesłanki ograniczenia konstytucyjnych praw i wolności (na tle orzecznictwa Trybunału Konstytucyjnego),"*Państwo i Prawo" 2001, No. 10, pp. 22–23; K. Opałek, *Prawo podmiotowe. Studium z teorii prawa,* Warsaw 1957, p. 167; K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP,* Cracow 1999, p. 202.

[5] Judgment of the Constitutional Tribunal of December 15, 2004, K 2/04, OTK-A 2004, No. 11, item 117.

- existence of the necessity of restrictions in the absence of other measures effectively serving this purpose,
- functional relationship of the restriction with the implementation of the values indicated in the exhaustive manner in Art. 31 sec. 3 of the Polish Constitution (state security, public order, environment protection, public health and morality, freedom and rights of other persons),
- prohibition of violation of the essence of a given freedom or law.

Therefore, the conflict between the need for legal and legitimate existence of the operational activity and a threat to the constitutional freedoms and rights of the individual requires above all the right balance in the legal protection of both disputed areas.

In democratic countries, even where the restrictions on the constitutional freedoms of the individual are introduced due to the need to fight crime and terrorism, universal legislation regulating operational and investigative activities has constitutional references. Article 31 sec. 3 of the Polish Constitution formulates the general principle of maintaining the proportionality of any restrictions on constitutional freedoms/rights in the event that they would experience any (regardless of their subject matter) restrictions in the ordinary legislation. This principle applies both to the situation when the Constitution itself provides for the creation of exceptions by the legal acts, and to the situation when the ordinary legislator, by regulating other matter, collides with the constitutional freedoms/rights of the individual (including those which were formulated rigorously at the constitutional level, as it is for example the case in Art. 47 or Art. 51 sec. 4 of the Constitution, i.e. when the Constitution of the Republic of Poland does not provide for the ordinary act to co-shape the scope of this constitutional right or freedom). Going beyond the proportionality of the restriction will be decisive for determining whether the intervention of the ordinary legislator occurred in an excessive and therefore unconstitutional manner.

The operational activities of the police, infringing privacy as such, require a differentiated evaluation as to the proportionality of the intervention, depending on how specific and protected by the Polish Constitution the aspect of privacy is. Its scope covers several issues related to the security of data processing, ensuring confidentiality of communication, security of personal data processing and provision of the advertising services, identifying internet activities and

protecting databases related to the location (traffic) data. They must be removed or made anonymous when they are no longer needed for the purpose of message transmission or billing, unless the subscriber has agreed to use them otherwise. The user whose data is stored must be previously informed about the purposes of processing. The obligation to delete traffic or animation data when it is no longer needed for message transmission purposes does not interfere with the procedures such as capturing IP numbers in the domain name system of unauthorized use of electronic communications systems.

Data retention is intended, in particular, to detect crimes against defense, state security, public order and safety, as well as, fiscal offenses. According to I. Lipowicz[6], provisions granting access to telecommunications data to the services do not meet the criterion of specificity required by Art. 49 of the Polish Constitution. The author holds an opinion that "this loophole means that these services may in any case established only by them, and not in the situation specified in the Act, reach out for the data subject to secrecy". Provisions of the Code of Criminal Procedure[7] allow to seize electronic devices or other data carriers for inspection while searching a room. However, they do not provide for specific measures listed in Art. 19 clause 3 lit. b, c, d of convention on cybercrime[8], by means of which procedural authorities can search and retain data by copying and blocking them.

According to W. Grzeszczak[9], the IT data can be secured in a way that the Convention on Cybercrime specifies in Art. 19, regarding the search and seizure of the stored IT data, namely by: a) a seizure of the IT system or part thereof or a carrier used to store the IT data, b) making and saving copies of the IT data, c) maintaining all the relevant stored IT data (blocking), d) making the IT data inaccessible or deleting them from a given IT system.

In turn, M. Górtowski[10] points to the issue of identifying data of a person using an IP address. The author emphasizes that the internet providers

[6] I. Lipowicz, *Między wolnością a bezpieczeństwem*, "Rzeczpospolita", 15 March 2011, addition to newspaper "Prawo co dnia".

[7] Dz.U. 2021, item 534.

[8] Dz.U. 2015, item 728.

[9] Por. W. Grzeszczyk, *Zmiany prawa karnego wprowadzone ustawą z dnia 18 marca 2004 r.,* "Prokuratura i Prawo" 2004, No. 7–8, p. 77.

[10] M. Górtowski, *Poczta elektroniczna w postępowaniu karnym,* "Prokuratura i Prawo" 2004, No. 7–8, p. 201, thesis No. 2.

often use a technique that allows dynamic allocation of an IP address. It can be described as the process when a given user does not have a permanently assigned IP address but, at the moment of starting a computer connected to the network, the user identifies himself/herself by means of a user name and password assigned to him/her in the server of the internet provider and, after a successful verification, receives a random, temporarily not used by anyone else, IP address from the pool offered to him/her by his/her internet service provider. This way of assigning IP addresses means that the disclosed IP address of the sender of the electronic message may no longer point to the perpetrator, but to another person who drew this address at random.

The problem of data retention was raised in the judgment of the Constitutional Tribunal of July 30, 2014, file reference number K 23/11[11]. This judgment directly concerns two key features of online anonymity. The first issue is collecting data about the user, the scope and the method of their acquisition i.e. retention, and the second is the type of data collected and their destruction if they do not correspond to the profile of the case under investigation. In addition, the it was found necessary to inform the network user about the conducted audit post factum, i.e. after the completion of the audit. The Tribunal drew attention to the importance of the Internet and other modern forms of communication of individuals, but explained that the protection of constitutional freedoms and rights in connection with the use of the Internet and other electronic methods of remote communication does not differ from the protection of traditional forms of communication or other activity. Consequently, the scope of constitutionally protected privacy (Art. 47 of the Polish Constitution) and the secrecy of communication (Art. 49 of the Polish Constitution), as well as the requirements that must be met by the regulations governing secret acquisition of information about individuals, has become the subject of the necessary interpretation. Privacy is a constitutionally protected freedom with all its consequences. First of all, this means the freedom of individuals to act in the framework of freedom as long as the Act does not define its limits. Only an explicit statutory regulation may impose restrictions in the scope of on undertaking certain behaviours within the framework of a specific freedom. However, not every regulation is admissi-

[11] Judgment of the Constitutional Tribunal of July 30, 2014, K 23/11 (Dz.U. item. 1055).

ble in the light of constitutional norms, principles and values. Constitutional protection resulting from Art. 47, Art. 49 and Art. 51 sec. 1 of the Polish Constitution covers all methods of transmitting messages, in all forms of communication, regardless of their physical medium (e.g. personal and telephone conversations, written correspondence, fax, text and multimedia messages, electronic mail, transmission of messages via web portals). According to the Constitutional Tribunal, it does not matter whether the exchange of information concerns strictly private life or professional, including business activity. There is no sphere of personal life from which constitutional protection would be excluded or intrinsically limited. The judgment refers directly to the provisions contained in the Telecommunications Act[12], acts concerning secret services, police regarding the possibility of obtaining data on the subject with regards to which the services are conducting operational activities aimed at determining commitment of crime. Until now, the Act has not provided for the need to inform the controlled entity about the control process he/she was subjected to. The Constitutional Tribunal has established several key points here: one cannot freely create laws that interfere with the constitutionally protected freedoms and rights, the concept of the "operational control" is too vague when it comes to restrictions about the way data is obtained and what data can be obtained, provisions should be made to guarantee independent control over the disclosure of data from retention, immediate and certified (by a committee and protocol) destruction of data subject to prohibitions of using them as evidence should be guaranteed.

According to the new reading of Art. 19 sec. 12 of the Police Act[13], a telecommunications entrepreneur, postal operator and service provider providing electronic services are obliged to provide, at their own expense, technical and organizational conditions enabling the Police to conduct an operational control.

The Police Commander-in-Chief, the CBŚP Commander and the Voivodship Police Commander keep records of requests for obtaining telecommunications, postal and internet data containing information identifying the organizational unit of the Police and the Police officer obtaining this data, their

[12] Dz.U. 2021, item 576.

[13] Dz.U. 2021, item 1882; see: Art. 20 c, 20ca, 20cb *Ustawa o policji. Komentarz*, eds. K. Chałubińska-Jentkiewicz, J. Kurek; Warsaw 2021, pp. 291–305.

type, purpose and time in which they have been obtained. Registers are kept in an electronic form, subject to the provisions on the protection of classified information. The Police Commander-in-Chief, the CBŚP Commander or the voivodship Police commander forward the data relevant to criminal proceedings to a prosecutor competent with regards to the area or the subject matter. The prosecutor decides on the scope and method of using the provided data. The data that is irrelevant to the criminal proceedings is subject to an immediate destruction carried out in the presence of a committee and based on a protocol. Thus, pursuant to Art. 20ca sec. 1 of the Act on the Police, the District Court competent for the headquarters of the Police authority to which the data was made available, controls obtaining telecommunications, postal or internet data by the Police.

Subject to the provisions on the protection of classified information, the Police authority shall submit to the regional court a biannual report including: number of cases of obtaining, in the reported period, telecommunications, postal or internet data and their type and legal qualifications of acts in connection with which telecommunications, postal or internet data were applied for, or information on obtaining data to save human life or health or to support search or rescue operations. The regional court informs the Police authority about the result of the inspection within 30 days of its completion. Obtaining data is excluded from control pursuant to Art. 20cb sec. 1 of the Act on the Police. Thus, pursuant to Art. 20cb sec. 1 of the Act on the Police to prevent or detect crimes or to save human life or health or to support search or rescue operations, the Police may obtain data: electronic list of subscribers, users or network termination points, referred to in Art. 161 of the Act of July 16, 2004 – the Act on Telecommunications – telecommunications confidentiality clause; in the case of a user other than a natural person, the network termination number and the registered office or place of business, a company name or name and organizational form of that user; in the case of a fixed public telecommunications network – also the name of the city and street where the network termination point is located, made available to the user and he/she may process them without the knowledge and consent of the person they concern.

Thus, pursuant to Art. 159 sec. 1 of the Act on Telecommunications, the secret of communication includes: the user's data, the content of individu-

al messages, transmission data, which means the data processed for the purpose of transmitting messages in telecommunications networks or calculating charges for telecommunications services, including location data, which means all the data processed in the telecommunications network indicating geographic location of the device of the end user publicly available telecommunications services, location data, which means location data that goes beyond the data necessary for the transmission of a message or issuing an invoice, data on attempts to establish a connection between specific ends of the telecommunications network). Therefore, the data of the user being a natural person and subject to protection are: surname and given names, parents' names, place and date of birth, address of permanent residence, Personal Identification Number (PESEL). These are also the data contained in the documents confirming the possibility of performing an obligation (e.g. an employment or remuneration certificate) towards a provider of publicly available telecommunications services, resulting from a contract for the provision of telecommunications services (most often these are the obligations of payment for the provided services). The content of individual messages under protection covers the subject of the message between it sender and recipient. This applies to any information exchanged or transmitted between users through publicly available telecommunications services. Such services include prepaid service provided in the mobile phone network (the so-called prepaid service) or a land-line telephone subscription. It should be emphasized here that in pursuance with Art. 43 of the Act of June 10, 2016 on anti-terrorist activities[14] in Art. 60b of the Telecommunications Act, information obligations were introduced.

The judgment of the Constitutional Tribunal concerns a very sensitive matter which is privacy and fight against crime conducted by secret services. The discrepancy between what services can do to fight crime and how they do it, has always been the cause of controversy. On the one hand, the legislator has equipped secret services with a number of tools for the carrying out of tasks in the field of crime detection[15]. On the other hand, the Constitutional Tribunal stated that the conferred powers are contrary to the Polish Constitu-

[14] Dz.U. item 904.

[15] See M. Bożek, *Aspekty normatywne systemu bezpieczeństwa państwa w sytuacjach nadzwyczajnych zagrożeń o charakterze polityczno-militarnym,* Lublin 2004, p. 67.

tion. One should remember that secret services and other police units act as if automatically operating within the borders and on the basis of the law. They act according to the laws and restrictive clauses created especially for them. This conflict, as a subject for consideration, raised by the Constitutional Tribunal, apart from the legal aspect, touches also upon a very delicate sphere of ethics of action. The ethics and public morality itself, just as well as the public interest in the face of changes in the conditions of functioning of a human – a network user, digital service provider, as well as cyber victims of criminal activities in the network, constitute a topic for consideration preceding any strategies or new legal regulations regarding the sphere of a cyberspace.

Literature

Bożek M., *Aspekty normatywne systemu bezpieczeństwa państwa w sytuacjach nadzwyczajnych zagrożeń o charakterze polityczno-militarnym,* Lublin 2004.

Chałubińska-Jentkiewicz K., *Cyberodpowiedzilaność,* Toruń 2019.

Garlicki L, *Przesłanki ograniczenia konstytucyjnych praw i wolności (na tle orzecznictwa Trybunału Konstytucyjnego)*"Państwo i Prawo" 2001, No. 10.

Górtowski M., *Poczta elektroniczna w postępowaniu karnym*, "Prokuratura i Prawo" 2004, No. 7–8.

Grzeszczyk W., *Zmiany prawa karnego wprowadzone ustawą z dnia 18 marca 2004 r.*, "Prokuratura i Prawo" 2004, No. 7–8.

Lipowicz I., *Między wolnością a bezpieczeństwem,* "Rzeczpospolita", 15 March 2011.

Opałek K., *Prawo podmiotowe. Studium z teorii prawa,* Warsaw 1957.

Ustawa o policji. Komentarz, eds. K. Chałubińska-Jentkiewicz, J. Kurek, Warsaw 2021.

Wojtyczek K., *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Cracow 1999.