

Izabela Stańczuk¹

**Constitutional Right of the Individual to Informational
Autonomy in the Light of the Powers of the Police
to Collect and Process Personal Data**

Keywords: informational autonomy, human rights, privacy, Police, Constitution of the Republic of Poland

Słowa kluczowe: autonomia informacyjna, prawa człowieka, prywatność, Policja, Konstytucja RP

Abstract

The article attempts to confront the individual's constitutional right to informational autonomy and the powers of the Police in the framework of which the service may collect and process personal data. Bearing in mind the paramount role of the Constitution of the Republic of Poland and its special importance for the sphere of rights and freedoms, the key regulations devoted to the right to privacy and the possibility of limiting informational autonomy were referred to. Treating the constitutional content as fundamental in the relationship between the individual and the state authorities, they were referred to the powers of the Police based on which the service may legally interfere in the information sphere of the individual. It was also stressed that the multiplicity of powers and the expansion of their catalog make it necessary to pay more attention to applying the proportionality mechanism.

¹ ORCID ID: 0000-0003-2446-8428, M.A., Department of Cybersecurity Law and New Technologies Law, Law Institute, War Studies University in Warsaw. E-mail: i.stanczuk@akademia.mil.pl.

Streszczenie**Konstytucyjne prawo jednostki do autonomii informacyjnej w świetle uprawnień Policji do gromadzenia i przetwarzania danych osobowych**

W artykule podejmuje się próbę skonfrontowania konstytucyjnego prawa jednostki do autonomii informacyjnej oraz uprawnień Policji w ramach których służba ta może gromadzić i przetwarzać dane osobowe. Pamiętając o nadrzędnej roli Konstytucji RP i jej szczególnym znaczeniu dla sfery praw i wolności, przywołano kluczowe regulacje poświęcone prawu do prywatności oraz możliwości ograniczenia autonomii informacyjnej. Traktując treści konstytucyjne jako fundamentalne w relacji jednostki z organami państwa, odniesiono je do uprawnień Policji na podstawie których, służba ta może legalnie ingerować w sferę informacyjną jednostki. Podkreślono również, iż wielość uprawnień oraz poszerzanie ich katalogu sprawia, że coraz więcej uwagi należy poświęcić zastosowaniu mechanizmu proporcjonalności.

✱

I. Introduction

For its functioning, the contemporary state needs not only, as it results from a classic definition of a state – population, territory, power, international recognition, and capacity to conduct international relations – but one more, even essential element should be added – information. A basic type of information collected and processed by the competent authorities is information about individuals. The specific powers in the field area of its collection and processing are granted by the law provisions to the services responsible for public safety and order, but, as should be kept in mind, these powers are not absolute. The right to maintain information about oneself is now all the more important since, in virtually every field area of social life, disclosure of this information is required of us. As a weaker party in the proceedings with the state authorities, the individual should be granted special protection. The conducted researches have been, to a significant extent, based on an analysis of the applicable law provisions, which sets out the rights and obligations both on the part of the individual and the Police authority and concern the

information sphere. An essential doubt that arises against the background of the assumed problematics of the research is the question: How, in the light of current legal regulations, is the individual's right to informational autonomy shaped, and what is the relationship between this right and the Police's powers to collect and process personal data? The paper also attempts to answer questions such as: What is the scope of the right to informational autonomy of the individual, and what are the legal grounds for its limitation? What powers do the Police have over the collection and processing of personal data? What ICT solutions does the Police use to obtain, collect and process personal data? The article assumes that the legal guarantees of the right to informational autonomy in the context of broad police powers to collect and process personal data are not reflected in the individual's actual possibilities of exercising this right. The multitude of legal solutions with the simultaneous extension of the powers of this service makes the relationship between the powers of these two groups of subjects (citizens and the Police) very complex and puts the citizens in a much weaker position. Considering that the Police, as a service responsible for security and public order, obtains various information and data about individuals in many areas of the functioning of the state and society, its activities in this respect should be subjected to special scrutiny. The main method used in the paper was the dogmatic-legal method. Analysis and synthesis were also used as one of the most commonly used theoretical research methods in the social sciences.

II. Right of the Individual to Informational Autonomy

Information autonomy as a right vested in the individual is directly linked to the right to privacy. An individual can dispose of their data by themselves while being free from coercion or otherwise controlled. Warren and Brandeis have rightly described the right to privacy as the right to be 'left alone'².

The understanding of the term of 'informational autonomy' was presented in the judgment of the Constitutional Tribunal of June 17, 2008, according

² K. Szymielewicz, A. Walkowiak, *The informational autonomy in the context of the Internet services: on the importance of a consent to data processing and the risks associated with profiling*, "Monitor Prawniczy" 2014, No. 9, supplement, p. 1029.

to which the principle of the informational autonomy should be understood as the right to decide for oneself whether or not to disclose information concerning oneself to others, as well as the right to exercise control over such information if other entities hold it. However, this entitlement does not and cannot be absolute. The aforementioned refers in particular to the citizen-public authority relationship³.

The Polish legislator does not directly use the concept of ‘informational autonomy’, but refers to it in Art. 51 of the Polish Constitution⁴. As J. Kurek and J. Taczkowska-Olszewska point out: ‘In this manner, the Constitution of the Republic of Poland implements the essential elements of the right to protection of private life: respect for informational autonomy of the individual, and thus the obligation itself to make data available is limited to the situations strictly defined by the statutory law; limitation of the arbitrariness of the legislator – the statutory law cannot form a scope of the obligation freely, while the Constitution of the Republic of Poland operates in this case with limitations of two types (as to its form – the obligation to make data available must be introduced by the statutory law, and as to matter – the obligation is justified only to the extent that it is necessary for a democratic rule of law)⁵. Both Art. 47 and Art. 51 of Polish Constitution are aimed at protecting the personal data of the individual against its unauthorized processing. Carrying out such activities by the public authorities, even if they are performed under the law, will be tantamount to the introduction of certain limitations within the sphere of human rights and freedoms, to which the legislator has referred in Art. 31 sec. 3 of Polish Constitution imposing the requirement to establish them only by way of the statutory law. While bearing in mind that Art. 51 sec. 2 of Polish Constitution fails to specify a catalog of values that could be quoted by the public authorities to justify the limitations applied, it should be considered that the catalog provided for in Art. 31 sec. 3 of Polish Constitution will be proper here. The conceptualization of the catalog of information that can be acquired, collected, and made available by the public author-

³ Judgment of the Constitutional Tribunal of June 17, 2008, File ref. No. K 8/04, OTK ZU (Case law of the Constitutional Tribunal. Official Collection) 2008, No. 5A, item 81.

⁴ Constitution of the Republic of Poland of April 2, 1997 (Dz.U.No. 78, item 483 as amended).

⁵ J. Kurek, J. Taczkowska-Olszewska, *Personal data protection as a performance of responsibilities in the field area of the state security*, Warsaw 2020.

ities as ‘necessary in a democratic state ruled by law’ due to the broad generality of its wording seems to empower the state authorities to take a broad spectrum of actions. A doctrinal interpretation is also interesting, but it is not binding. As B. Banaszak presumes: ‘Generally speaking, it seems that the necessary information can be stipulated as that which enables the individual to function on a normal basis in a state-organized society. While considering this problem, from the point of view of the public authorities, any information is necessary without which they will not be able to take (or complete) action within the limits of the powers vested in them’⁶. This issue is also raised by the Constitutional Tribunal in its case law, taking the position that due to a content of Art. 51 sec. 2, the Constitution of the Republic of Poland protects the Polish citizens by introducing a ban in respect of the public authorities (legislative, executive, judicial) on stepping into informational autonomy of the individual in a manner unnecessary from the viewpoint of the standards of a democratic state ruled by law. Therefore, neither considerations of purposefulness nor convenience of the authorities justify a breach of informational autonomy (...)⁷.

Article 51 of Polish Constitution fails to bear all aspects of the individual’s information autonomy, to which, for example, refers Art. 53 sec. 7, which is also an example of *lex specialis*. The provision grants an individual the right to maintain their own world view, religious beliefs, or beliefs in the internal sphere and not to disclose them, while at the same time imposing on the public authorities a ban on requesting this type of information. In turn, in Art. 61 sec. 3 of Polish Constitution, the Polish legislator provided for the need to protect the individual and individual’s informational autonomy, making it possible to limit the right to public information having due regard to protecting the freedoms and rights of other persons⁸.

The limitation of the right to informational autonomy and privacy should take place while taking into account the proportionality mechanism. It makes it possible to define the permissible limits of interference in the situation re-

⁶ B. Banaszak, *Constitution of the Republic of Poland. Comment*, Warsaw 2012, par. 6.

⁷ Judgment of the Constitutional Tribunal of November 20, 2002, File ref. 26, K 41/02, Case-law of the Constitutional Tribunal. Series A (OTK-A) 2002, No. 6, item 83.

⁸ M. Wild, *Comment to Art. 51 of the Constitution of the Republic of Poland*, [in:] *Constitution of the Republic of Poland. Volume 1. Comment to Art. 1–86*, eds. M. Safjan, L. Bosek, Warsaw 2016, par. 6.

lated to a conflict of values, especially when its subject matter constitutes the rights and freedoms derived from the Polish Constitution. A frequent subject matter of the said conflict is the one between the right to individual privacy and values of particular importance to the state institutions, such as security and safety, a fight against crime, and transparency of the public authorities. Settlement of this type of dispute may develop significant difficulties because we are dealing with values that are formally equivalent to each other. The limitation of one of the rights or one of the constitutional freedoms in favor of another one will always lead to a question of the grounds and justification for such action. Since the Constitution itself fails to hierarchize these rights, the only solution seems to reference the constitutional axiology⁹.

Significant changes in the protection and processing of personal data, both on the part of the controller that processes the data and the individual whose data is being processed, have been introduced by the provisions of the General Regulation on Personal Data Protection (hereinafter referred to as the GDPR¹⁰). Given the individual and the right of the latter to maintain information about themselves, the content of Art. 15 (right of access by the data subject), Art. 16 (right to rectification), Art. 17 (right to erasure, the so-called “right to be forgotten”), Art. 18 (right to restriction of processing) or the right to object, expressed in Art. 21, is of particular importance. An important right is also the right to lodge a complaint with the supervisory authority, which is the President of the Office for the Protection of Personal Data, in the case where the processing of personal data is considered to be in breach of the provisions of the GDPR.

III. Powers of the Police to Process Information About the Data Subjects

The Police is a service operating within the domain of public safety and order. Nevertheless, it will be impossible to carry out its responsibilities without

⁹ M. Safjan, *Challenges for the rule of law*, Warsaw 2007.

¹⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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), OJ EU L119/1.

obtaining appropriate information about individuals and social groups. The catalog of this information is broad and includes both information obtained in an unclassified and classified manner. The Act on the Police¹¹ in Clause 3 determines what rights its officers are vested in concerning their service. According to Art. 14 sec. 4, for a performance of the statutory responsibilities, the Police may use data of the data subject, including in the form of an electronic record, obtained by other authorities, services, and state institutions as a result of performing operational and surveillance activities and process it within the meaning of the Act of December 14, 2018 on the protection of personal data processed in relation to the prevention of and fighting against crime¹², without the knowledge and consent of the data subject¹³. More detailed regulations are provided for in Art. 20, which gives to the police officers authority to, inter alia, process information, including personal data, to the extent necessary to carry out the statutory responsibilities or exercise powers in respect of the conduct of administrative proceedings, a performance of administrative and order activities and other activities which the police officers are authorized to carry out under the Acts¹⁴. The Act on the protection of personal data processed for the prevention of and fighting against crime is undoubtedly the key legal act that has filled a gap in the sphere of legislation dedicated to the legal regulation of the collection, processing, and protection of information about the data subjects by this service.

What is particularly important from the point of view of the individual's informational autonomy is the introduction in Art. 13, section 1 of the statutory limitation on the use and processing of personal data. This right is granted solely to carry out the responsibilities imposed on the Police and only to the extent that it is necessary to exercise the right or fulfill the obligation resulting from the law provision¹⁵. The controller decides each time on a scope of personal data that should be considered necessary. The method and purpose

¹¹ Act of April 6, 1990 on the Police (Dz.U.No. 30, item 179 as amended).

¹² Hereinafter referred to as the Act on protection of personal data processed in relation to the prevention of and fighting against crime.

¹³ Ibidem.

¹⁴ Art. 20 of the Act of April 6, on the Police.

¹⁵ *Comment to Art. 14, [in:] Act on the Police. Comment*, eds. K. Chałubińska-Jentkiewicz, J. Kurek, Warsaw 2020.

of its processing results directly from Directive (EU) 2016/680 of the European Parliament and of the Council, in which recital 26 stipulates that the purposes of their processing should be explicit, justified, and specified at the time of their collection. Moreover, personal data should be adequate and relevant for the processing. In particular, it should be ensured that the collected personal data are not excessive and that the storage period is no longer than necessary to achieve its processing. Personal data should only be processed where the purpose of the processing cannot reasonably be achieved by other means. In order to prevent the data from being stored for longer than is necessary, the controller should set a date for their erasure or periodic review¹⁶. At the same time, the Polish legislator in Art. 14 of the Act on the protection of personal data processed for the prevention of and fighting against intensified the protection granted about the categories of sensitive data, indicating its closed catalog including 11 types of data. This type of measure consisting in the enumerative indication of sensitive data causes that no other type of data, even if it may result in a breach of individual's informational autonomy, fails to constitute a subject matter of the protection provided for data included in the catalog.

Nevertheless, it does not mean that other provisions of the statutory laws cannot protect it. Given its strict connection to human rights and freedoms, sensitive data are subject to a general ban on processing. The legislator indicates the grounds when this ban may be canceled, but its catalog cannot be construed without any limitation. Therefore, it should be assumed that solely the exceptions contained in the Act substantiate the processing of sensitive data by the Police, and any action not falling within one of them will constitute a breach of the ban introduced in Art. 14¹⁷.

Article 16 of the Act on the protection of personal data processed to prevent and fight against crime makes profiling of the data subjects impermissi-

¹⁶ Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ EU 2016, L 119/89.

¹⁷ *Comment to Art. 14, [in:] Comment to the Act on protection of personal data processed in relation to the prevention of and fighting against crime*, eds. A. Grzelak, Warsaw 2019, par. 1, 11.

ble. The legislator prohibits the final settlement of the cases of individual data subjects (also within the scope of sensitive data) solely based on the result of the automated processing of personal data, including as an effect of profiling¹⁸. The ban set out in Art. 16 is not absolute, which means that the legislator has provided for some exceptional situations in which a decision concerning a specific person may be taken in an automated manner. The permissibility of this type of activity must result from and be based on the law provision to which the controller is subject. This law provision must provide for adequate safeguards for the rights and freedoms of the data subjects¹⁹.

IV. Datasets

The use of modern technology not only contributes to improving citizens' quality of life, but in the context of public institutions, it allows to increase their efficiency and streamline their work. The adoption of the e-government concept understood as transferring information and providing public services using ICT (Information and Communications Technology) has changed the way state bodies function and has enabled the development of cooperation and faster data exchange²⁰.

The main ICT system of the Police, constituting a centralized set of data sets, maintained at the General Police Headquarters, is the National Police Information System (hereinafter referred to as the NPIS). The data sets that constitute the System are the sets: Person, Fact, Entity, Subject, Victims, and registers of offenses. The basic legal provisions based on which the processing of personal data takes place include mainly Art. 20 of the Act on the Police and the provisions of the Act of September 16, 2011 on the exchange of information with law enforcement agencies of the European Union Member States, third countries, European Union agencies, and international organiza-

¹⁸ *Comment to Art. 15*, [in:] P. Liwzic, T. Ochocki, Ł. Pocięcha, *Act on the protection of personal data processed in connection with preventing and fighting against crime. Comment*, Warsaw 2019, par. 1, 2, 4.

¹⁹ *Ibidem*, par. 5.

²⁰ N. Lubik-Reczek, I. Kapsa, M. Musiał-Karg, *Electronic citizen participation in Poland. Declarations and opinions of Poles on e-government and e-voting*, Poznań 2020, p. 41.

tions²¹. The powers of the Police also include the processing of personal data provided to the Police Commander in Chief by the Police, the Internal Security Agency, and the Border Guard on the principles, in the manner and under a procedure specified in the provisions of Art. 10 of the Act on anti-terrorism activities and the provisions of the Regulation of the Prime Minister on the collection of data of persons who are not citizens of the Republic of Poland. The powers of the Police also cover the processing of information on the results of deoxyribonucleic acid (DNA) analysis and maintenance of the DNA database and dactyloscopy²² data sets, regulated by different regulations.

The use of the NPIS information and communication systems by the Police enables to get access to and the processing of information, including personal data in many data sets, e.g., the Police Register of Mass Events, the System of Recording Accidents and Collisions, the “Weapons” Register, the record of drivers who breach the road traffic regulations. Moreover, the NPIS information and communication systems enable to process by the remote transmission of information, including personal data, from the following data sets of other entities or public authorities: the Central Database of Persons Deprived of Liberty, the central record of drivers, the central record of vehicles, the official national register of economic entities, the Polish Resident Identification Number (PESEL) and register of residents, the Register of Identity Cards, the central record of issued and invalidated passports, the Schengen Information System (SIS), the Visa Information System (VIS), the Integrated Record System administered by the Border Guard, databases of the International Criminal Police Organisation – Interpol²³.

A specific category of information is criminal information processed by the Police to detect and prosecute offenders and prevent and fight against crime under the Act of July 6, 2001 on criminal information processing²⁴.

According to G. Rydlewski, intelligent technologies are changing the environment in which we live and will shape the future of countries and individu-

²¹ Dz.U. 2018, item 484 and Dz.U. 2019, item 125.

²² Ordinance No. 28 of the Police Commander in Chief of August 11, 2020 on dactyloscopy data sets, OJ of the GPH of 2020, item 44.

²³ §4 of Ordinance No. 70 of the Commander in Chief of December 2, 2019 on the National Police Information System (Dz.U. item 114).

²⁴ Dz.U.No. 110, item 1189.

als. Referring to the words of Z. Brzezinski, the author notes that the combination of technological revolution and technocratic approach poses a real threat to society. Its manifestation is the use of technology by the elites for their own purposes, including controlling society²⁵. With this vision in mind, the Police, as a service with broad powers to collect and process personal data, may become a tool in the hands of those in power, and its actions may undermine the constitutionally guaranteed sphere of information autonomy.

V. Conclusions

The individual's right to informational autonomy is undoubtedly a specific right that all public authorities should respect. Its importance is all the greater as the reality in which the individual functions is referred to as the information society. Information about the individual, including their personal data, is a valuable asset, and its acquisition constitutes a subject matter of the activities of the state authorities in a broad sense. Thus, we are dealing with a highly conflicting area in which the individual's rights clash with the state's. In a democratic state ruled by law, which operates while observing the principle of legalism, it is clear that public authorities can only do what the law expressly allows them to do. Considering the reform of 2018 and related to the new regulations on the protection of personal data in Poland, it should be emphasized that exercising the right to informational autonomy is not easy. It is not due to a lack of the appropriate legal guarantees, but rather to a large number of the EU and national, general, and specific provisions, the knowledge and appropriate use of which often exceed the abilities of the average individual. A confirmation of this assumption constitutes, for example, the decisions taken as a part of the proceedings by the President of the PDPO, which failed to consider the complainants' requests.

²⁵ G. Rydlewski, *Governance in the age of information, digitization and artificial intelligence*, Warsaw 2021, pp. 20–21.

Literature

- Act on the Police. Comment*, eds. K. Chałubińska-Jentkiewicz, J. Kurek, Warsaw 2020.
- Banaszak B., *Constitution of the Republic of Poland. Comment*, Warsaw 2012.
- Comment to the Act on the protection of personal data processed in connection with preventing and fighting against crime*, ed. A. Grzelak, Warsaw 2019.
- General Regulation on Personal Data Protection. Comment*, ed. M. Sakowska-Baryła, Warsaw 2018.
- Kurek J., Taczowska-Olszewska J., *Personal data protection as a performance of responsibilities in the field area of the state security*, Warsaw 2020.
- Liwszic P., Ochocki T., Pocięcha Ł., *Act on the protection of personal data processed in connection with preventing and fighting against crime Comment*, Warsaw 2019.
- Lubik-Reczek N., Kapsa I., Musiał-Karg M., *Electronic citizen participation in Poland. Declarations and opinions of Poles on e-government and e-voting*, Poznań 2020.
- 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. Comment*, ed. P. Litwiński, Warsaw 2018.
- Rydlewski G., *Governance in the age of information, digitization and artificial intelligence*, Warsaw 2021.
- Safjan M., *Challenges for the rule of law*, Warsaw 2007.
- Szymielewicz K., Walkowiak A., *Informational autonomy in the context of the on-line services: on a meaning of a consent to the processing of personal data and risks related to profiling*, "Monitor Prawniczy" 2014, No. 9, supplement.
- Wild M., *Comment to Art. 51 of the Constitution of the Republic of Poland*, [in:] *Constitution of the Republic of Poland. Volume 1. Comment to Art. 1–86*, eds. M. Safjan, L. Bosek, Warsaw 2016.