Personal Data Serving the Purpose of Ensuring State Security. Cyberspace Challenges. The European Context

JUSTYNA KUREK

Abstract Information of a personal character constitutes a special category of data used by the state and its bodies in the performance of public tasks. Difficulties in identifying risks and challenges are connected, inter alia, with the fact that the material scope of the definition of personal data is not a standing concept. It cannot be determined in advance whether a given category of information will be of a personal character or not. These risks are further aggravated when Big Data tools are used, which facilitate the effective analysis of huge volumes of data, linking information with different sources of origin, and the indirect identification of data subjects. In addition to the problems resulting from the nature of personal data, there is a further complicated problem resulting from the hybrid nature of legal regulations. This is due to the fact that some processes involving personal data processing are within the Community regime of personal data protection, while some others, as activities implemented as national security tasks, are excluded completely from the European regime. The purpose of this article is to identify the threats and problems in these conditions and the related implications for state security.

Keywords: • personal data • state security • cyberspace • Big Data • PESEL

CORRESPONDENCE ADDRESS: Justyna Kurek, Ph.D., dr. habil., Associate Professor, War Studies University in Warsaw, Faculty of National Security, State Security Institute, Political Security Department, Aleja Generala Antoniego Chrusciela "Montera" 103, 00-910 Warszawa, Poland, e-mail: j.kurek@akademia.mil.pl, ORCID: 0000-0002-8754-5243.

https://doi.org/10.4335/2022.2.8 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 Introductory remarks

Information of a personal character constitutes a special category of data used by the state and its bodies in the performance of public tasks. They often constitute the building blocks of public services. Without this type of data, it would be impossible to conduct public or economic activities (Karpiuk 2015:13). Difficulties in identifying threats and challenges in this area are related to the fact that the material scope of the definition of personal data is not a standing concept. It is significantly affected by the development of information techniques and technologies. As noted in literature, based on the reference to the criterion of "technological progress", it can be simultaneously stated that the scope of the term "personal data" may change over time, because the information that we are currently unable to link to a specific person, in the perspective of progressive civilisation and technological development, may be qualified in this manner in the future (Fisher, Górski, Nerka, Sakowska-Baryła, Wygoda, 2018:71-72). Thus, depending on the technical and technological identification possibilities, personal data can be, among other things, photographs, videos, biometric data, facial features or fingerprints. The danger for the state and its undisturbed functioning is further implied by the fact that the concept of personal data is extremely capacious. It cannot be determined in advance whether a given category of information will be of a personal character or not. These risks are further aggravated when Big data tools are used, which facilitate the effective analysis of huge volumes of data, the linking of information with different sources of origin and the indirect identification of data subjects. In addition to the problems resulting from the nature of personal data, there is a further complicated problem resulting from the hybrid nature of legal regulations. This is due to the fact that some processes involving personal data processing are within the Community regime of personal data protection, while some others, as activities implemented as national security tasks, are excluded completely from the European regime. The purpose of this article is to identify the threats and problems for personal data processing and the related implications for security.

2 The concept of personal data

Pursuant to Article 4(1) of the GDPR, personal data mean any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The definition adopted in the GDPR is horizontal in nature and applies in whole to the protection of personal data under European Union law. The source literature notes the fact that any information, regardless of the manner and form in which it is expressed, and no matter if it is widely understood, can be regarded as personal data. The legal nature of any such information should be assessed individually for each of its holders (Sibiga, 2003:33). It is not possible to exclude in advance any category of information from the scope of personal data.

Under the GDPR, there is no doubt that the term "personal data" should be construed as individual information about personal and factual relations of a specified or specifiable natural person. The concept of personal data does not cover information of an anonymous character, which makes it impossible to identify natural persons beyond reasonable doubt; as well as entities other than natural persons. On the one hand, the attribution of the quality of personal data to a given piece of information will, therefore, depend on external factors and the technological possibilities to identify that person. It is not essential that the data subject is known to the data processor. The legislation only requires that it should be specified (Däubler, Hjort, Schubert, Wolmerath 2010: § 3 BDSG *[Federal Data Protection Act]*). Identification, on the other hand, means that a person can be distinguished within a group from other group members. This, however, does not have to mean that the person is identified by their first and last name. It is sufficient to indicate circumstances which make it possible to identify this person uniquely (Drozd, 2008:24). It is also assumed that a person is identifiable, if – although not yet identified – such identification is possible. The source literature notes the fact that any information, regardless of the manner and form in which it is expressed, and no matter if it is widely understood, can be regarded as personal data. The legal nature of any such information should be assessed individually for each of its holders (Sibiga, 2003: 33). Therefore, from the point of view of implementing public tasks in the area of security, all information with identifiable potential must be subjected to special protection.

3 The impact of Big Data analytics on state security with regard to personal data

Big Data processes have caused a revolution in the analysis and processing of personal data, increasing the potential for their use. Technological developments mean that the character of personal data can be attributed to broad categories of information. The new analytical potential, apart from the broader benefits, also implies obligations, in particular towards personal data subjects. Since it is difficult to exclude *a priori* the personal character of various pieces of information, the protection of personal data should be extended to various categories of information held by the data subject in case this information, through the way it is linked to other information, acquires a personal character. The potential of Big Data further increases the analytical possibilities. The value of data can be increased not only through new processes of acquisition and analysis, but thanks to linking certain data with data from other sources. Often, the mere synthesis of unclassified data from, for example, public registers and social networks, owing to the use of analytical tools with strong data structuring capabilities, typical of Big Data analytics, can be threatening from the point of view of state security.

4 The hybrid nature of personal data regulations – the European context

One of the most interesting challenges for the state in the era of big data analytics is the issue of personal data protection and the use of personal information under the conditions of mass processing. From the point of view of state security, ensuring the protection of personal data is additionally connected with the necessity to function in a complex legal regime, which is created by intermingling national and EU regulations. The framework for the protection of personal data, established in the Treaty, plays a key role in structuring a personal data protection system. Pursuant to Article 72, in connection with Article 73, of the Treaty on the Functioning of the European Union, the legislative competence of the European Union shall be excluded in the case of activities which lie outside the scope of the Union law, in particular those relating to national security. This distinction is of particular importance in the area of personal data protection. Indeed, EU law on the protection of personal data is excluded for the regulatory areas which are not subject to European Union law (Article 16(2) of the TFEU). The regulatory framework adopted at a European Union level in the area of personal data protection consists of three instruments: (1) the General Data Protection Regulation (GDPR), (2) Directive (EU) 2016/680 (known as the Police Directive), and (3) Regulation (EU) 2018/1725 concerning the processing of personal data by EU bodies. The exclusion, under the GDPR and Directive 2016/680/EU, of the processing of personal data in the course of activities that fall outside the scope of Union law, including in particular activities within the scope of national security and the activities of entities carrying out tasks in the area of national security, leads, in effect, to a kind of regulatory regime of a hybrid nature – since some processes involving personal data processing are covered by Union law and some others are up to the arbitrary decision of the national legislator. The indicated regulatory context and the attempt at providing a systemic inclusion of the legal framework for personal data protection prompt a proposal for the adoption of the paradigm of a hybrid legal regulation (Kurek, 2021:18-19). A hybrid legal environment has already been *per se* a source of risk for security. This is because neither the Treaty provisions, nor the data protection provisions, define what national security is.

5 Personal data in land and mortgage registers from the perspective of state security

Data from land and mortgage registers may serve as an example. Such registers, apart from information relating strictly to real property, also contain information about owners as well as data on the financing of the property in the form of credit and mortgages encumbering the property. Although safeguards against unauthorised access are introduced in the explicit version of the interface, they are not of an absolute nature. The "anti-bot" mechanism does not require any intellectual effort, but only the ticking of the appropriate box. Also, limiting the search options to one criterion – the number of the land and mortgage register – does not protect the system. The designation of court districts is pre-definable, the numbers of registers are not assigned on a random basis, and the

control number is a combination of ten variations. Hence, this data can be obtained by suitably programmed robots and placed in a relationally structured database. By linking these data with information from social networks, it is possible to accurately determine the family circles of the property owner. Additionally, social networks contain photos and information about users' "check-ins". Unauthorised access to such information alone poses a threat not only to the privacy of data subjects, but also to the security of persons and property (Kurek 2021:136 ff).

6 The delivery of personal data from the PESEL database to Polish Post – a case study

From the point of view of state security, an extremely interesting case study arises from a project that was not implemented, which assumed the use of the PESEL database by Polish Post (Poczta Polska) for the purposes of organising the presidential elections by post. The objective of the following analysis is not to assess the correctness of the organisation of the presidential elections or lack thereof, but only to examine whether adequate precautions were taken with regards to personal data, and to indicate the risks which could arise for state security from any possible irregularities in data security.

PESEL (Universal Electronic System for Registration of the Population) is one of the basic registers in Poland. It contains information about Polish citizens and foreigners who have a PESEL number. This database operates on the basis of the provisions of the Act of 24 September 2010 on the Population Register. Thus, the PESEL register contains information making it possible to determine the status of a natural person. The provisions of the Act on the Population Register also define who may enter data into the PESEL database. However, they do not regulate the scope of entities with access to the system. According to information provided on the website of the Ministry of Digitalisation, the data can be accessed via secure connections by enumerated entities, including but not limited to election authorities, such as: public administration authorities, courts, state and local government organisational units.

Therefore, the public PESEL register contains contact details essential from the point of view of the potential organisation of postal voting, but under the law only those regarding a permanent place of registered residence or a voluntarily declared place of temporary residence. A list of electors is drawn up based on data from the PESEL register, but in accordance with adopted legal regulations, the list is verified on the basis of voluntarily declared places of residence by persons wishing to be added to the list of electors.

Under the anti-crisis shield, permission was granted (under the provisions of the Act of 16 April 2020 on Specific Support Instruments in connection with the Spread of the SARS-CoV-2 Virus) to provide the postal operator with the data from the PESEL register for the purposes of organising the elections. Pursuant to Article 99 of the afore-said Act, the designated operator, after submitting a request in electronic form, shall receive data

from the PESEL register or from other listings or registers being at the disposal of a public administration body, if the data are needed to perform tasks related to the organisation of the election of the President of the Republic of Poland or in order to perform other duties imposed by government administration bodies. On 22 April, Polish Post received data from the PESEL system exported on a DVD. The data were delivered on an encrypted carrier by convoy. Therefore, the delivery was contrary to statutory disposition, where it is indicated that access shall be provided in electronic form. Pursuant to Article 78^2 § 1 of the Civil Code, for the observance of the written form of an act in law, it is sufficient to make a declaration of intent and append a qualified electronic signature thereto. Delivery by convoy together with a password, which is sent through a different channel, does not meet the requirements of a qualified electronic signature. The explanations in no way indicate that the disc was secured with a qualified electronic signature. The fact of providing the password via other channels confirms the assumption that the data was secured outside the key public infrastructure. This situation seems completely incomprehensible in the light of the explanations of the Ministry of Digitalisation to the Ombudsman, according to which, at the time of delivery of the data Polish Post, by virtue of the Decision of the Minister of Internal Affairs of 8 September 2014 No. DSO-WUI-6173-24.2/14, had access to the PESEL register by means of devices for remote transmission of data for the performance of statutory tasks (https://www.rpo.gov.pl/sites/default/files/Odpowied%C5%BA%20MC%20%20dane%20przekazane%20Poczcie%2C%204.05.pdf). It is not entirely clear why the access already held could not be used.

The transmission of exported data to the disc implies the assumption that personal data from the PESEL register were, or were supposed to be, processed outside a secure environment. It is worth pointing out that other entities using the PESEL database may use it only at isolated workstations within a secure dedicated network. The condition is such that workstations are not allowed to have access to the internet.

Generating and storing data on a data carrier was, therefore, unnecessary and only posed a risk for personal information. According to the explanations of the Minister of Digitisation, the reason for data delivery on a disc in a structured form resulted from the fact that the interface of the system used by the designated operator did not enable the mass downloading of data and the preparation for sending election packages. From an IT point of view, it may have been sufficient for the data controller to change user rights and access levels.

In accordance with the declaration of the Minister of Digitisation, the delivered disc contained only indispensable data – that is the data of living Polish citizens who had reached legal age by 10 May 2020 and whose country of residence was Poland. The provided data included: PESEL numbers, first name(s), surnames and, depending on what data the person had registered in the PESEL register, their current address of permanent residence, and if there was no such address, the last address of permanent residence and

an address of temporary residence. Additional information provided gave notice of whether a person had currently registered a temporary trip outside the country (without specifying the country of departure).

From the point of view of the legal regulations on the protection of personal data, in particular in the light of Article 14 of the GDPR, the delivery could be considered admissible if it followed from the law that the data were provided for the purpose of the implementation of a task regulated by an act. The provision of Article 99, in the absence of an act on postal elections, does not seem sufficient in view of the disposition of Article 14 of the GDPR. The second element, which is important from the point of view of the legal regulations on the protection of personal data, is carrying out, at the stage of drafting a legal act, the proper analysis of the impact of the processing of personal data. The grounds for the governmental draft act (Parliamentary Paper no. 330) do not refer at all to the provision of data from the PESEL database. Significantly, as regards personal data and the impact of the regulation on personal data, the grounds refer only to the context of obtaining data on the financial situations of entrepreneurs applying for support in the light of Article 10a of the said Act, indicating that the principles regarding the protection of personal data shall not apply to the regulation (http://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=330). Neither the delivery of the PESEL database nor Article 99 are grounded. In this situation, it cannot be stated that any analysis of the impact of the regulation on personal data protection was made at the stage of drafting the legal act.

Thus, in the light of the disposition of Article 25 of the GDPR, neither the Ministry of Digitisation, nor Polish Post could abstain from carrying out an analysis of the impact of the processing of personal data under a risk-based approach. Also, due to the lack of an analysis, in the light of Article 14 of the GDPR, there were no grounds for abandoning the obligation to provide information to data subjects. The analysis would have demonstrated the existence of risks at multiple levels, not only to data subjects but also to state security.

The risk for security had already emerged at the stage of exporting the data to a DVD carrier and encrypting it. Securing the delivery with a qualified electronic signature within the meaning of Regulation 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market relies on a key public infrastructure using asymmetric encryption. This guarantees that any subsequent changes to the electronic data or interference is immediately noticeable by the recipient of the delivery. In the conditions of password-protected data delivery, there is no such effect.

Secondly, the delivery of data outside a secure IT environment exposes it to additional risks of a physical nature. A hostile takeover of a convoy could result in the structured data of both Poles and foreigners registered in the PESEL database being out of control

and could be used contrary to its purpose. On the other hand, multiplication of the database would be beyond any control.

The creation of a parallel database could make it possible to generate dummy identity documents and steal the identity of millions of people. Information such as first names, last names, PESEL numbers and permanent addresses are data used for authentication in the case of many services, including public services. The extraction of such data makes it possible, with the additional extraction of data from publicly available sources, to steal identities. They could be used to extort credit via the internet, to obtain fast loans where identification is simplified, and to conclude telecommunications contracts on behalf of the data subject, and this could lead to many other activities destabilising economic circulation and national security.

Even if the delivery and convoy itself do not cause problems, the provision of data outside a secure remote transmission also means that data retrieval is not controlled. According to the procedures applicable to the PESEL database, entities authorised to access the database may use the information only for the purpose of performing their duties. Access is obtained by means of remote transmission, through devices allowing the identification of the person obtaining data in the system and the scope, date and purpose of obtaining it. These entities must have technical and organisational safeguards making it impossible to use such data not in accordance with the purpose for which they were obtained (Czaplicki, 2015:144). With regard to standard queries to the PESEL database, each query by an authorised entity involves the identification of the entity through secure devices. The acquisition of data by an employee of a certain institution, which was not authorised by public tasks, was also easy to determine. This procedure gave a sense of control over the system. This made it possible in the past to control and detect unusual traffic in two bailiff offices, where 350,000 records were retrieved from the PESEL database inconsistently with the scope of tasks (https://www.money.pl/gospodarka/wiadomosci/artykul/pesel-dane-komornik-wyciek,237,0,2393581.html).

The delivery of data outside of a remote transmission is an exception and, unfortunately, it does not secure them against unauthorised access. Data from the DVD, in the possession of Polish Post, may be used beyond access control and entered into the system outside of a secure environment, thus generating numerous risks for state security, including the security of the Polish legal system and economic circulation.

The process of providing the data generated a risk not only for the security of the persons whose data are included in the public register, but also for the security of the state. The way in which the personal data were to be used in the elections should also raise serious doubts. Direct delivery of election packages to boxes at permanent addresses could not ensure data security nor the security of the election process itself. There is certainly a very large group of people who do not live at their permanent addresses. These people add

themselves to the list of electors in their place of residence. In addition, the obligation to inform authorities about changing a place of residence for more than three months is often not respected. Therefore, the proposed voting model assumed no control over who actually casts a vote, which, from the point of view of political security, undermines the credibility of potential results. It would result in a lack of democratic legitimacy for the body so established. A permanent address may be inhabited by completely different people than those who are registered there. Furthermore, Polish Post had no possibility to identify the declarations, which were to be submitted together with the votes, stating that they were cast by themselves. It does not have access to specimen signatures.

It is also worth paying attention to the physical risk of putting documents containing personal data into postboxes. Postboxes in blocks of flats and on housing estates do not have any special protection. They are often an element of public space. Therefore, the possibility of getting into them is very easy.

Looking at the risks indicated above, it should be stated that neither Polish Post, nor the provisions of the Act that created the framework for the delivery of information in any systemic way, guaranteed that any personal data protection standards were maintained. On the contrary, they generated serious risks for personal data. In addition, the legal regulations did not contain any mechanisms for the erasure of data no longer necessary for the purpose for which they were obtained. Despite the fact that the general election by postal ballot has not taken place, there is no documentation whatsoever confirming the erasure of data, the destruction of carriers, or data anonymisation. Under these circumstances, the Minister of Digitalisation should not have provided data to the postal operator from the beginning of the process, as this process did not guarantee any level of security for personal data.

7 Conclusions

Information of a personal character constitutes a special category of data used by the state and its bodies in the performance of their tasks in the area of security. Much of this information will correspond to a flexible definition of personal data. As indicated by the considerations made hereinabove, the scope of the term “personal data” may change over time, because the information that we are currently unable to link to a specific person, in the perspective of the progressive development of civilisation and technology may be qualified in this manner in the future (Fisher, Górski, Nerka, Sakowska-Baryła, Wygoda, 2018:72). Entities performing tasks in the area of security also take part in the processing of information of a personal character. For these entities, the challenges are double. Thus, the challenge faced by entities performing tasks in the area of security is to protect essential national values, at the same time maintaining the protection of citizens’ privacy and dignity. Thus, a particular challenge is to ensure a balance between the effective counteraction of threats to state security and the protection of citizens’ privacy. The problem of state security in connection with the processing of personal data is

accompanied by the problem of the hybrid nature of legal regulations. From the point of view of state security, ensuring personal data protection is additionally connected with the necessity to function in a complex legal regime, which is created by intermingling national and EU regulations. The indicated regulatory context and the attempt at a systemic inclusion of a legal framework for personal data protection prompts a proposal for the adoption of the paradigm of a hybrid legal regulation (Kurek, 2021:18-19), which *per se* constitutes a source of risk for state security resulting, for example, from the lack of a precise definition of the term "national security".

References:

Czaplicki, P. (2015) Identyfikacja tożsamości użytkowników publicznych baz danych, In: Szpor, G. (ed.) *Internet. Publiczne bazy danych i Big Data* (Warsaw: C.H. Beck), pp. 137-147.

Däubler, W., Hjort, J.P., Schubert, M. & Wolmerath, M. (2010) *Arbeitsrecht, Komentarz* (Baden-Baden: C.H. Beck).

Drozd, A. (2008) Pojęcie danych osobowych, In: Fajgielski, P. (ed.) *Ochrona danych osobowych z perspektywy dziesięciolecia* (Lublin: Wydawnictwo Katolickiego Uniwersytetu Lubelskiego), pp. 1-202.

Fisher, B., Górski, M., Nerka, A., Sakowska-Baryła, M. & Wygoda, K. (2018), In: Sakowska-Baryła, M. (ed.) *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz* (Warszawa: C.H. Beck), pp. 1-652.

Karpiuk, M. & Chałubińska-Jentkiewicz, K. (2015) *Prawo bezpieczeństwa informacyjnego* (Warszawa: Wydawnictwo Akademii Obrony Narodowej).

Kurek, J. (2021) *Bezpieczeństwo państwa w warunkach hybridowej regulacji danych osobowych w dobie analizy Big data. Aspekty prawne, organizacyjne i systemowe* (Warszawa: Wydawnictwo Akademii Sztuki Wojennej), pp. 1-319.

Sibiga, G. (2003) *Postępowanie w sprawie ochrony danych osobowych* (Warszawa: Dom Wydawniczy ABC), pp. 1-228.