PROTECTION OF PERSONAL DATA IN PUBLIC INSTITUTIONS – SELECTED ISSUES

OCHRONA DANYCH OSOBOWYCH W INSTYTUCJACH PUBLICZNYCH – WYBRANE ZAGADNIENIA

Abstract: This article contains considerations regarding the protection of personal data included in the provisions of Polish law and international regulations. It raises the issue of the right to collect information about citizens by public authorities. It contains an interpretation of the judgments of the European Court of Human Rights in Strasbourg and, in particular, the Act of 29 August 1997 on the protection of personal data. It also contains statistical data on proceedings initiated and committed crimes related to obstructing public authorities
Introduction

The scope of personal data protection has been regulated by the Act of 29 August 1997 on the protection of personal data. Community law in this field is governed by the Council of Europe Convention 108 on the protection of individuals with regard to the automatic processing of personal data of 1981, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of persons with regard to processing personal data and the free movement of such data, as well as Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. In addition, the Inspector General for Personal Data Protection – IGPDP also has an important role in the protection of personal data. Detailed regulations are also included in the provisions of the Civil Code (in particular Articles 23 and 24).

1. Sources of personal data protection

In recent years, the use of very extensive personal data protection by separate countries has become particularly critical\(^2\). This problem has been noticed by the UN Human Rights Committee and the Council of Europe. The risks it generates for the rights of the individual are well known both at the level of national law and under international regulations, especially in the Council of Europe Convention of 1981 on the Protection of Individuals with regard to Automatic Processing of Personal Data\(^3\).

This Convention, although not ratified by Poland, creates an important reference point for standards set by the European Convention on Human Rights\(^4\), which our country is a party to. Procedures are in place to restrict the creation of datasets, their use and sharing in the public authorities system, as well as sharing of existing datasets and correcting their irregularities. Strasbourg jurisprudence has long dealt with these issues and, as in many other areas, has evolved from a tolerant approach to the official gathering of personal data to a more restrictive one. States have been obliged to limit interference in the privacy of citizens\(^5\) to actually “necessary” situations\(^6\).

Certain types of registering, so the creation of appropriate datasets, do not raise major controversies, however, special problems have arisen in relation to datasets compiled by special services and by the police. The Tribunal has no doubt that “special services find legitimate grounds for existence in a democratic society”, however, it also emphasises that “their competence to secretly follow citizens is tolerable only to the extent strictly necessary to protect democratic institutions\(^7\). Therefore, there is a justification, especially when it comes to state security, for issuing laws authorizing the special services to “collect and store classified information about citizens, as well as their use, e.g. when assessing the qualifications of people applying for employment in positions related to national security\(^8\). It may be connected with the passing of such information to other public authorities, and the interested party may not be notified of the fact of collecting information about them or about the scope of their passing. The lack of such notification ensures the efficiency of the

\(^7\) Ibidem, § 88.
procedure being followed\textsuperscript{9}. Public authorities have a “wide margin of appreciation” on these issues\textsuperscript{10}.

The Tribunal recognizes that “the existence of a system of secret information gathering in order to protect national security creates a risk of undermining a democratic state of law\textsuperscript{11}. This prompts the ECHR to increasingly formulate requirements and guarantees necessary for the implementation of Article 8 of ECHR. Interference into the sphere protected by Article 8 is not only gathering data person. Therefore, it cannot be said that undertaking a political activity hides a voluntary resignation from protection\textsuperscript{12}.

In Poland, the protection of personal data results from Articles 47 and 51 of the Constitution of the Republic of Poland and the Act of 29 August 1997 on the protection of personal data\textsuperscript{13}.

The works on the preparation of the current law on the protection of personal data lasted 6 years. The creation of legal norms in the field of personal data protection should be treated as a manifestation of the jurisdiction of the areas that until recently have been “free” from public-legal interference\textsuperscript{14}. This state of affairs carries with it interpretative doubts and difficulties\textsuperscript{15}, but also encourages the observation of the manner of applying similar laws in other countries, especially those belonging to the European Union.

The discussed Act was intended to be given a comprehensive character on several levels. The Act regulates, though perhaps too fragmentary, the issues of freedom of information, or third parties’ interest in accessing and using information. In this area, it looks for ways to reconcile conflicting interests to some extent. What is important the Act does not introduce any explicit provisions regarding the trading of personal data (databases).

An important role is given to the data administrators by the Act by imposing on them:

a) extensive informational obligations in relation to those whose personal data are collected and processed (Articles 24-25, Articles 32-33, 54 of Personal Data Protection Act);

b) the obligation to care for the legality and reliability of personal data processing (Article 26, Articles 49-50 of Personal Data Protection Act);

c) the obligation to maintain confidentiality of personal data (Articles 37-39, Article 51 of Personal Data Protection Act);

d) the obligation to secure personal datasets (Article 36 and next, Article 52 of Personal Data Protection Act.);


\textsuperscript{10} Judgment of the ECtHR in the case of Segerstedt-Wiberg, § 104.

\textsuperscript{11} Judgment of the ECtHR of 22 September 1993 in the case of Klass, Sign. 27/1992/372/446, § 49.

\textsuperscript{12} Judgment of the ECtHR of May 4, 2000 in the Rotaru case, Application No. 28341/95, § 43.


\textsuperscript{14} G. Szpor, Publicznoprawna ochrona danych osobowych, PUG 1999, No. 12, p. 10.

\textsuperscript{15} On the one hand resulting in misunderstanding or even disregarding of the act, on the other hand, it is over-zealous in its implementation and application.
e) the obligation to register the dataset (Article 40 and next, Article 53 of Personal Data Protection Act).

The Act in the scope operation concerns both:

a) all methods of data processing in “traditional” and automated manner
b) data processing in the public and private sectors\textsuperscript{16}.

The complex and comprehensive nature of the Act combines norms that belong to different areas of law. This applies mainly to administrative and criminal law, while personal data are protected by all public and legal means\textsuperscript{17}. It should also be noted that the Act adopted a registration model in the field of personal data processing. In this model the processing is not dependent on obtaining permission from the authority, while the data administrator is required to submit a data file to the Inspector General for Personal Data Protection.

The processing of personal data must be carried out in accordance not only with the Personal Data Protection Act, but also with all applicable legal norms. At the same time, personal data protection issues are part of a much wider problem, mainly related to “sharing” of their content. The legislator, taking into account the practice of doctrine and judicature, perhaps anticipating the direction of technological changes towards the popularisation of electronic communication, specified in the title of the Act the phrase “protection” of personal data, and not “processing” of personal data. He emphasized in Article 7 point 2 of the Personal Data Protection Act that data processing is an operation occurring on personal data mainly in information systems\textsuperscript{18}. Personal data can be processed in datasets and outside of this set (Article 2 sections 1 and 2 of Personal Data Protection Act). However, “sharing” is the result of the processing of personal data and has not been defined in separate regulations.

2. Consequences of violation of provisions on the protection of personal data in public institutions

The number of initiated proceedings and committed crimes concerning the destruction, damage, deletion, changing of a record, thwarting or hindering the reading of information to public authorities (Articles 268 and 268a of the Penal Code) in 1999-2014 has systematically increased (see Figure 1). The number of initiated proceedings in 1999 was 49, and in 2014 already 572. In 2009 the number of initiated proceedings increased up to 1115. In 1999 it was 59 and in 2014 as many as 743. The increase in efficiency in punishing criminals committing such acts was possible due to the significant development of information technology systems enabling better detection and prosecution of people committing crimes against information protection.

\textsuperscript{16} B. Fischer, \textit{Administrator danych osobowych po przystąpieniu Polski do Unii Europejskiej. Uwagi de lege lata}, „Radca Prawny” 2005, No. 5, p. 94.

\textsuperscript{17} Ibidem, p. 96.

Figure 1. The number of initiated proceedings and crimes committed concerning the destruction, damage, deletion, changing of the record, thwarting or hindering the reading of information to public authorities (Articles 268 and 268a. of the Penal Code)

The number of crimes committed and proceedings initiated in the scope of data destruction pursuant to Article 269 of Penal Code in the years 1999-2014 was on the level of a few, a dozen or so a year (see Figure 2). At the same time, no data destruction crimes were detected in 2004, 2007 and 2010.

Figure 2. Number of crimes committed and proceedings initiated in the field of data destruction (Article 269 of the Penal Code)
Rysunek 2. Liczba popełnionych przestępstw i wszczętych postępowań w zakresie niszczenia danych (art. 269 k.k.)

In the field of computer sabotage, the number of crimes committed and proceedings commenced on the basis of Article 269a of the Penal Code have been steadily growing since 2005 (see Figure 3). In 2005, only one offense was committed and only one proceeding was initiated. In the years 2006-2008 this number amounted to a dozen or so, and since 2010 it fluctuated in the range of 20-50, while in 2009, as many as 243 committed sabotage crimes were found. Such a state of affairs was mainly related to the entry into force of the amendment to Article 269a of the Penal Code to which there were also qualified offenses consisting in obstructing access to IT data causing disruptions in the work of a computer system or a teleinformatic network.

Figure 3. The number of committed crimes and proceedings in the field of computer sabotage (Article 269a of the Penal Code)

Rysunek 3. Liczba popełnionych przestępstw i wszczętych postępowań w zakresie sabotage komputerowego (art. 269a k.k.)

Also the number of crimes committed and proceedings initiated in the field of computer software production for unlawful acquisition of information (Article 269b of the Penal Code) has been steadily increasing since 2005 (see Figure 4). In 2005 six offenses of this nature were recorded and 6 provisions were issued regarding the initiation of proceedings. By contrast, in 2014 43 infringements of Article 269b of the Penal Code were recorded and 47 proceedings were initiated. In 2010 a record number of crimes in the production of computer software used for unlawful acquisition of information were found. This number amounted to 71 and was higher than the total sum of crimes committed in 2005-2009. After 2010 the number of crimes committed has never reached such a high level. This was due to the amendment of Article 269b of the Penal Code, it was indicated that it also refers to the situation included in Article 267 § 3 of the Penal Code, i.e. when unlawful information is obtained through eavesdropping, visual or other devices.

Figure 4. The number of crimes committed and proceedings initiated in the field of computer software production for unlawful acquisition of information (Article 269b of the Penal Code)

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of detected crimes</th>
<th>Number of initiated proceedings</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>2006</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>2007</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>2008</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>2009</td>
<td>18</td>
<td>23</td>
</tr>
<tr>
<td>2010</td>
<td>29</td>
<td>38</td>
</tr>
<tr>
<td>2011</td>
<td>27</td>
<td>38</td>
</tr>
<tr>
<td>2012</td>
<td>21</td>
<td>28</td>
</tr>
<tr>
<td>2013</td>
<td>28</td>
<td>42</td>
</tr>
<tr>
<td>2014</td>
<td>43</td>
<td>47</td>
</tr>
</tbody>
</table>

In the years 2002-2011 the number of people convicted by valid sentences for crimes concerning the destruction, damage, deletion, changing of a record, foisting or obstructing the reading of information to public authorities on the basis of Articles 268 and 268a of the Penal Code was growing and only after 2011 it started to decline (see Figure 5). At the same time, the percentage of people convicted for violating the norms of Articles 268 and 268a of the Penal Code in the first instance, and then acquitted systematically decreased from 19% in 2002 to 4% in the years 2013-2014.

Figure 5. The number and percentage of people convicted for crimes concerning the destruction, damage, deletion, changing of the record, thwarting or obstructing the reading of information to public authorities (Articles 268 and 268a of the Penal Code)

While until 2008 the largest number of people convicted for violation of Article 268 § 1 of the Penal Code (see Figure 16), then since 2009 the most frequent entities have been convicted for violation of Article 268a § 1 of the Penal Code. Thus, there is a clear increase in the number of crimes consisting of destroying, damaging, removing, changing or hindering access to IT data (including personal data) to public authorities.
Figure 6. The number of people convicted for violation of the law in the scope of destruction, damage, deletion, changing the record, thwarting or hindering the reading of information to public authorities (Articles 268 and 268a of the Penal Code)

Rysunek 6. Liczba osób skazanych za naruszenie prawa w zakresie niszczenia, uszkadzania, usuwania, zmieniania zapisu, udaremniania lub utrudniania zapoznania się z informacjami organom władzy publicznej (art. 268 k.k. i 268a k.k.)

Source: own elaboration based on: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ [access: 18.05.2017]
The number of people convicted for the destruction of data pursuant to Article 269 of the Penal Code during the period under consideration remained very low, however, after 2011 no person was convicted on this basis (see Figure 7). In 2002-2003, 2006 and 2009, the percentage of convicted people amounted to 50%. In those years, a judgment of conviction was issued in every second or third case for the destruction of IT data.

Figure 7. The number and percentage of people convicted for destruction of IT data (Article 269 of the Penal Code)

Rysunek 7. Liczba i odsetek osób skazanych za niszczenie danych informatycznych (art. 269 k.k.)

Source: own elaboration based on: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ [access: 18.05.2017]

In the case of the number of people convicted for violation of the law regarding the destruction of data of special importance for the defense of the country, security in communication, functioning of government administration until 2007 (inclusive), the largest number of people was convicted on the basis of Article 269 § 1 (see Figure 8), while from 2008 the predominant number convicted on the basis of Article 269 §2 the Penal Code.
Figure 8. The number of people convicted for violation of the law in the scope of destruction of IT data (Article 269 of the Penal Code)
Rysunek 8. Liczba osób skazanych za naruszenie prawa w zakresie niszczenia danych informatycznych (art. 269 k.k.)


In 2005 a new type of crime was introduced into the Penal Code, as specified in Article 269a the Penal Code. It consists of disrupting the work of a computer system or a computer network. From 2005 to 2011 the number of final convictions pronounced for the committing this crime has increased (see Figure 9). At the same time, from 2006, the percentage of people convicted per year for committing a crime under Article 269a of the Penal Code was never higher than 18%.

Figure 9. Number and percentage of people convicted for computer sabotage (Article 269a of the Penal Code)
Rysunek 9. Liczba i odsetek osób skazanych za sabotaż komputerowy (art. 269a k.k.)

In 2014 for violation of Articles 268 and 268a of the Penal Code, as many as 19 imprisonment sentences were pronounced. In addition, the penalty of imprisonment was imposed on eight judgments with a fine. The fine itself was imposed 5 times, and its level was in the range of PLN 501 - 1,500. The restriction of freedom was pronounced three times. The court also ruled public works 3 times against the perpetrators.

Figure 10. The penalty for thwarting and obstructing the use of information from Articles 268 and 268a of the Penal Code in 2014

Rysunek 10. Wymiar kary w zakresie udaremniania i utrudniania korzystania z informacji z art. 268 k.k. i 268a k.k. w roku 2014

<table>
<thead>
<tr>
<th>Punishment Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fine (PLN 501-800)</td>
<td>2</td>
</tr>
<tr>
<td>Fine (PLN 801-1000)</td>
<td>3</td>
</tr>
<tr>
<td>Fine (PLN 1001-1500)</td>
<td>2</td>
</tr>
<tr>
<td>Restriction of freedom (4-6 months)</td>
<td>2</td>
</tr>
<tr>
<td>Restriction of freedom (7-12 months)</td>
<td>1</td>
</tr>
<tr>
<td>Community punishment</td>
<td>3</td>
</tr>
<tr>
<td>Imprisonment (3 months)</td>
<td>3</td>
</tr>
<tr>
<td>Imprisonment (4-5 months)</td>
<td>5</td>
</tr>
<tr>
<td>Imprisonment (6 months)</td>
<td>7</td>
</tr>
<tr>
<td>Imprisonment (7-11 months)</td>
<td>4</td>
</tr>
<tr>
<td>Imprisonment and fine</td>
<td>8</td>
</tr>
</tbody>
</table>

Source: ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ [access: 18.05.2017].

Thus, the penalty of imprisonment was the most often, which the courts ruled for violation of Articles 268 and 268a of the Penal Code in almost every second case (see Figure 11). In addition, the penalty of imprisonment along with a fine was ruled by the courts in every fifth case. Fine in seventeen percent, community punishment in eight percent, and a restriction of freedom in seven percent of cases.
In the case of penalties administered by courts for offenses under Articles 269a and 269b of the Penal Code it should be noted that in 2014 only two such penalties were pronounced (Figure 29). These were: imprisonment for a period of one year and imprisonment for a period of 6 months.

Figure 12. The types of penalties judged by the courts for computer sabotage and destruction of IT data under Articles 269a and 269b of the Penal Code in 2014

Rysunek 12. Wymiary kar orzekanych przez sądy za sabotaż komputerowy i niszczenie danych informatycznych z art. 269a k.k. i 269b k.k. w roku 2014

To summarize the information regarding the type of penalties imposed in 2014 as a result of committing offenses against the protection of information, it is pointed out that in 50 cases the penalty of imprisonment was imposed and in 23 cases it was a combination of imprisonment with a fine. The penalty of a fine was imposed in 43 cases. The restriction of freedom without supervision was pronounced in 37 cases, and with supervision in 9 cases. Therefore, the most often punishment is imprisonment, which as a result was pronounced in almost every third case (31%) – Figure 13. In addition, the courts often decided to adjudicate on this type of penalty combined with a fine (14%). The penalty of fine was imposed in every fourth case, as was the restriction of freedom without supervision. At the same time, only every twentieth convicted person in 2014 experienced a restriction of freedom with supervision.
It should be emphasized that in 2014 the courts for crimes committed against the protection of information did not adjudicate punitive measures in the form of a ban on taking positions or prohibiting the profession.

**De lege lata and de lege ferenda conclusions**

Analyzing the collected statistical data, it should be stated that in the cases of adjudicating on crimes against the protection of information in public institutions, the sentences of imprisonment and fines were predominant in the scope of issued guilt decisions. The penalty of restriction of freedom with the decision of supervision was adjudicated very seldom, i.e. in every twentieth conviction case. At the same time, the courts did not rule against the ban on performing public functions or holding specific positions against people who committed such acts, which should be a natural consequence of a final conviction.

From the analysis of statistical data made available by the Ministry of Justice and the Police, it can be concluded that in cases involving crimes against information protection in public institutions a small number of convictions are made. However, it should not be explicitly seen as the main reason of a low number of convictions in relation to the amount of offenses reported to the Police. Even the best-formulated procedures of access to personal data and securing them against unauthorized disclosure do not provide a full guarantee of compliance with the law in this regard. It is up to the Police, the prosecutor’s office and the courts to determine whether the
norms contained in the Acts will not be only “dead norms of the law”. In addition to such tools as provisions of criminal law, among others, the actions taken by law enforcement authorities should be taken into account. It is also necessary, in public organizations, to observe standards regarding professional ethics, organizational activities, including control, internal monitoring, and a high level of management rules for dealing with data subject to protection.

**Bibliography**


Dyrekcja 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych, Dz. Urz. WE L 281 z 21.11.1995 r., P. 0031.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997 nr 78, poz. 483, z późn. zm.


Konwencja o ochronie praw człowieka i podstawowych wolności, Rzym, 4 listopada 1950 r., zmieniona Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz.U. 1993 nr 61, poz. 284, z późn. zm.


Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997 nr 133, poz. 883, z późn. zm.

Wyrok ETPCz w sprawie Segerstedt-Wiberg.

Wyrok ETPCz z 16 lutego 2000 r. w sprawie Amann p. Szwajcarii Recueil des arrêts et décisions, 2000 II.

Wyrok ETPCz z 22 września 1993 w sprawie Klass, Sygn. 27/1992/372/446.
Wyrok ETPCz z 26 marca 1987 r. w sprawie Leander p. Szwecji, Skarga nr 9248/81.

Wyrok ETPCz z 4 maja 2000 w sprawie Rotaru, Skarga nr 28341/95.

Wyrok ETPCz z 6 czerwca 2006 r. w sprawie Segerstedt-Wiberg and Others przeciwko Szwecji, Skarga nr 62332/00.

**Author's resume:**

**Anna Słowik, PhD** – lecturer at the Management Department of The Stanisław Pigoń State Higher School of Vocational Education in Krosno, Doctor of Judicial Science, lawyer, in 2013-2014 assistant at the Department of Administration Science of the University of Rzeszow, in 2009-2011 lecturer at the Faculty of Law and Administration of Maria Curie-Skłodowska University in Lublin and at the Jan Zamoyski College of Humanities and Economics in Zamość, manager of private medical facility.

**Nota o Autorze:**

**Dr Anna Słowik** – wykładowca w Zakładzie Zarządzania Państwowej Wyższej Szkoły Zawodowej im. S. Pigonia w Krośnie, doktor nauk prawnych, adwokat, w latach 2013-2014 asystent w Katedrze Nauki Administracji Uniwersytetu Rzeszowskiego, w latach 2009-2011 wykładowca na Wydziale Prawa i Administracji Uniwersytetu Marii Curie-Skłodowskiej w Lublinie i w Wyższej Szkole Humanistyczno-Ekonomicznej w Zamościu, manager prywatnej placówki medycznej.

**Contact/Kontakt:**

Anna Słowik
ul. Kopalniana 22
38-400 Krosno
tel.: 601 418 188
e-mail: slowikanne@gmail.com