DOI: 10.31648/sp.11957

Katarzyna Pruszkiewicz-Słowińska
University of Warmia and Mazury in Olsztyn
ORCID: 0000-0001-8441-0143
katarzyna.slowinska@uwm.edu.pl

Provisions of criminal law in personal data protection – some remarks

First, it should be noted that a breach of personal data protection regulations may result in administrative liability (in particular, the imposition of an administrative fine), civil liability, criminal liability and, in certain situations, disciplinary liability[1]. The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L119 of 2016, p. 1, as amended)[2], hereinafter referred to as the GDPR, does not explicitly provide for criminal liability for the processing of personal data in a manner contrary to the provisions of the Regulation. Administrative fines are the essential sanctioning instrument stipulated in the GDPR. While personal data controllers are aware of civil and administrative liability, they are often unaware that they may potentially incur criminal liability. According to the GDPR Fines and Data Breach Survey Report, prepared by the law firm DLA Piper in January 2025, Poland is among the EU states with the highest occurrence of personal data protection violations. In 2024, it ranked third (alongside the Netherlands and Germany) among 31 European countries in terms of reported personal data protection breaches[3].

The GDPR does not obligate EU Member States to introduce criminal liability for unlawful processing of personal data into their legal systems.

[1] P. Poniatowski, *Niedopuszczalne lub nieuprawnione przetwarzanie danych osobowych – aspekty prawnokarne*, „Prokuratura i Prawo" 2021, No. 10, pp. 62–89.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ EU L119 of 2016, p. 1, as amended).

[3] DLA Piper GDPR Fines and Data Breach Survey, https://www.dlapiper.com/en/insights/publications/2025/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2025 (accessed: 17.09.2025).

However, according to Recital 149 of the GDPR, "Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation (…)".

Furthermore, according to Article 84(1) GDPR, "Member States shall lay down the rules on other penalties applicable to infringements of this Regulation, in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive". The EU legislator operates under the premise that sanctions for infringements of the Regulation's provisions – in the form of administrative fines – may be supplemented in the national laws of Member States with other types of penalties. EU law requires that sanctions introduced in domestic legislation apply to the infringements that are not otherwise subject to administrative fines. National regulations in this regard should therefore be formulated to avoid a conflict of norms and double punishment for the same infringements[4].

The Polish lawmaker has taken advantage of that possibility, as Article 107 of the Act on the Protection of Personal Data of 10 May 2018 (hereinafter as AoPPD)[5] introduces the offence of unlawful processing of personal data and, in Article 108, the offence of obstructing verification of compliance with personal data protection regulations and failing to provide the President of the Personal Data Protection Office with the data necessary to determine the grounds for the administrative financial penalty. Such offences are liable to a fine, restriction of liberty or imprisonment for up to two years (or up to three years in the case of processing special categories of data). Proceedings in cases of the kind take place pursuant to the provisions of the Code of Criminal Procedure.

With respect to criminal liability for breaches of personal data protection regulations, it should also be noted that, next to the AoPPD, such liability is formulated, e.g., in the Criminal Code[6], specifically in Chapter XXXIII entitled *Offences Against the Protection of Information*, as well as in Article 190(a) § 2 of the Criminal Code, which provides for identity theft.

Criminal liability had existed in the Polish legal system even before the provisions of the General Data Protection Regulation entered into force on

[4] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, [in:] idem, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, 2022, Legalis, Article 84.

[5] Act on the Protection of Personal Data of 10 May 2018 (consolidated text Journal of Laws of 2019, item 1781).

[6] Criminal Code Act of 6 June 1997 (consolidated text Journal of Laws of 2025, item 383).

25 May 2018. The previous Act on the Protection of Personal Data[7] included Chapter 8, which contained criminal law provisions. It established penalties on the unlawful processing of personal data (ordinary and sensitive) (Article 49), the disclosure of personal data to unauthorized persons (intentional or unintentional) (Article 50), violation of personal data security rules (Article 51), failure to report a data set for registration (Article 52), failure to comply with the information obligation (Article 53), and obstruction or prevention of control (Article 54). However, as an instrument of personal data protection, that system was considered ineffective in the literature. It was emphasized that "the illusory nature of protection, which resulted, among other things, from the construction of offences specified in Articles 53 and 54 of the Act as exclusively intentional, or from the limitation of the application of Article 49(1) and (2) of the AoPPD to actions involving personal data sets. At the same time, the recognition of failure to report a personal data set for registration or breach of information obligations towards the data subjects seemed, given the degree of unlawfulness of such acts and their social harmfulness, to be an unjustified criminalization of an act that should not be considered criminal"[8].

The intention of the lawmaker was for the new criminal law provisions not to reiterate the previous ones, which contained overly general descriptions of the features of the offences and were therefore only reluctantly applied by law enforcement authorities and courts[9]. Over the 20 years during which AoPPD of 1997 remained in force, law enforcement authorities initiated approximately 300 cases per year, the vast majority of which ended with a decision to discontinue criminal proceedings. During that period, nearly 300 individuals were convicted, with fines being the most common penalty. Moreover, the aim behind the adoption of criminal law provisions was to establish criminal liability for exceptional situations involving the most serious violations. The authors of the draft stated that the criminal liability provided for in Articles 107 and 108 of the AoPPD would only supplement the system of sanctions for non-compliance with personal data protection regulations, as it was centered on administrative fines and civil liability.

The offence specified in Article 107 AoPPD consists of such processing of personal data that is inadmissible or happens to be carried out by an unauthorized person. In order to bring a charge under Article 107 AoPPD, the processing of personal data must qualify as not permitted, i.e. take place

---

[7] Act on the Protection of Personal Data of 29 August 1997 (Journal of Laws of 2016, item 922 and of 2018, items 138 and 723).

[8] P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warsaw 2015, pp. 513–514.

[9] Uzasadnienie projektu ustawy o ochronie danych osobowych [Rationale to the draft of the Act on the Protection of Personal Data], Sejm print No. 2410, Sejm of the 8th Term, p. 46.

despite the failure to meet at least one prerequisite – relevant to the type of processed data – which render it lawful, or be carried out by an unauthorized individual, i.e. a person who has not been duly authorized to do so. The authorization to process data may stem from provisions of the law, a contract or an authorization granted by a competent entity; it should be stressed that such authorization to process data cannot be presumed. The offence under Article 107 AoPPD is a formal one, as it does not require any effect of the perpetrator's act to occur. Legal doctrine maintains that, besides the processing of one's personal data, it will have produced some effect for the data subject or resulted in an interference with that person's privacy. The offence under Article 107 AoPPD can only be committed intentionally[10].

Court rulings offer certain examples of specific actions that were found to have constituted inadmissible processing of personal data:

- unauthorized access to personal data by persons who have access to a database (for purposes other than those for which they have been authorized);
- logging in by a healthcare professional and reviewing the data of patients other than their own,
- making photocopies of court documents from cases in which one is neither a party nor a participant.

In one of the cases heard by the District Court in Legionowo (case No. II K 90/20), the defendant instructed a receptionist to photocopy two pages of a patient's medical record. This was due to a legal dispute initiated by the patient for payment following an erroneous medical diagnosis. Undoubtedly, the file in question was not a private document of the physician, even if she had made parts of it. The defendant did not have the right to process the personal data of the injured party by photocopying those documents, especially since the defendant used them to pressure the former into dropping a legal dispute with her. The court found that the defendant had committed the offence specified in Article 107(2) AoPPD and conditionally discontinued the proceedings against her for a probationary period of one year[11].

In another case before the District Court in Toruń (case No. II K 1544/21), the defendant, a gynecologist, processed personal data in a manner that was not permitted, logging into an online system using a personal identification number (PESEL) to see the profile of a man unknown to her, which contained his sensitive data concerning his health and sick leave. The man had never been a patient of the defendant, nor had he authorized the defendant

[10] P. Barta, [in:] P. Litwiński (ed.), *Ustawa o ochronie danych osobowych. Komentarz*, 2018, Legalis, Article 107.

[11] Judgment of the District Court in Legionowo of 19 October 2020, case No. II K 90/20, Legalis.

to log into the system. The court found the defendant guilty of an offence under Article 107 AoPPD and conditionally discontinued the proceedings for a probationary period of one year[12].

In the case heard by the District Court in Leszno (case No. II K 761/21), the indictment stated that the defendant, while reviewing the case No. III Nsm 121/18, processed without authorization the personal data of parties and participants in other proceedings ongoing before the District Court in Rawicz, Family Division III, in that he made photocopies of materials that were not an integral part of the files made available to him, contrary to the order granting consent to make photocopies of the materials from file III Nsm 121/18 that had been indicated in the request for permission to make photocopies. The court found the defendant guilty of the offence under Article 107 AoPPD and imposed a fine in the amount of 80 (eighty) daily rates at PLN 20 (twenty zloty) each[13].

At this point, it may be worthwhile to mention a case examined by the District Court for Lublin-Zachód in Lublin. The defendant was charged with publishing a public post on his profile on a website, which contained witness interview transcripts that included personal data, specifically the first and last names and dates of birth of the persons mentioned, as well as the names of parents of two victims, even though the processing of the data was not permitted and the individual was not authorized to do so (i.e. an act under Article 107(1) of AoPPD). The court acquitted the defendant of the alleged offence, stating that Article 2(2)(c) GDPR stipulates that the Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity. The AoPPD directly implements the Regulation, meaning its provisions apply exclusively to matters related to the public, service, or commercial sector concerning natural persons, but not to actions of natural persons in their private lives. Posts published on one's account on the F. platform should certainly be considered as such[14].

It should be underlined that although infringements under the Act on the Protection of Personal Data and offences against information protection are independent of each other, a single action may meet the criteria specified in several provisions of criminal law. The definition of personal data processing is very broad. In practice, there may be numerous situations where such processing is not permitted or is carried out by an unauthorized person, and it may also overlap with offenses against information protection pursuant

[12] Judgment of the District Court in Toruń of 23 June 2022, case No. II K 1544/21, Legalis.

[13] Judgment of the District Court in Leszno of 5 June 2023, case No. II K 761/21, Lex No. 3625042.

[14] Judgment of the District Court in Lublin of 20 February 2020, case No. III K 1/20, Lex No. 3388516.

to Chapter XXXIII of the Criminal Code[15]. When a person acting without authorization obtains access to information which is not intended for them, their action meets the criteria of two offences, i.e., Article 267 § 1 CC and Article 107(1) AoPPD. A violation of data protection regulations may also constitute an act that fulfils the criteria in Article 286 CC and Article 107(1) AoPPD. In such cases, a cumulative legal classification will be applied in accordance with Article 11 § 2 of the CC.

Here, a case heard by the District Court in Kętrzyn offers an example (case No. II K 306/21). According to the indictment, the defendant sought financial gain by having numerous victims make payments in the total amount of PLN 6,647.00 to a medical treatment fundraiser she had launched on the X platform, in which she misrepresented her actual health. She did not achieve the goal, as her actual health was determined, and the transfer of the collected amounts was suspended. In addition, having no relevant authorization, she processed the personal data of an injured party by sending a scan of the latter's identity card to the fundraising entity (i.e. an act under Article 13 § 1 CC in conjunction with Article 286 § 1 CC, further in concurrence with Article 107(1) of the Act on the Protection of Personal Data of 10 May 2018 in conjunction with Article 11 § 2 CC). In that particular case, the Court found the defendant guilty of the offences and deemed it appropriate to impose a six-month imprisonment sentence, despite a previous clean record. The Court also decided to suspend the sentence conditionally for a probationary period of one year. The Court asserted that this was the most severe of the penalties listed in the Code, but that it was the lowest possible sentence, given the defendant's previous clean criminal record, as well as her remorse and awareness of the reprehensible nature of her act. The positive criminological prognosis for the defendant warranted the conditional suspension of the custodial sentence. In the Court's opinion, the defendant's stance offered real grounds for assuming that she will not reoffend in the future[16].

Regarding offences against the protection of personal data, it would be legitimate to employ the nomenclature specific to criminal law. Thus, the person who initiates the preparatory proceedings in a case would be the injured party, as opposed to the claimant. Meanwhile, the party against whom the criminal proceedings are conducted would be the suspect at the preparatory stage and the defendant at the trial stage. Thus, the personal data controller or data processor who is a natural person would be the suspect (defendant). The person or entity against whom the offence relating to the protection

[15] J. Schabowski, *Nielegalne przetwarzanie danych osobowych. Sankcje karne*, [in:] P. Litwiński (ed.), *Odo. Compliance. Praktyczny komentarz z przykładami i orzecznictwem*, 2025, Legalis.

[16] Judgment of the District Court in Kętrzyn of 18 January 2022, case No. II K 306/21, Lex No. 3302162.

of personal data has been committed would be the injured party. One of the most important rights of the party aggrieved through unauthorized processing of their personal data is to notify the law enforcement authorities about the offence that may have been committed. If a decision is made to institute preparatory proceedings, the person who has reported the offence becomes a party to the preparatory proceedings and acquires all the rights due to the injured party. They are informed of their rights and obligations, which they acknowledge by signing. The most important rights of the injured party are listed in Article 300 § 2 of the Code of Criminal Procedure. Among other things, the injured party has the right to legal assistance (a representative – solicitor, legal counsel), the right to use the services of an interpreter, the right to participate in the proceedings, the right to personal data protection, the right to request access to case files, the right to information, the right to appeal against procedural decisions, and the right to lodge a complaint against a decision to refuse to institute or discontinue preparatory proceedings (Article 306 CCP). They may participate in relevant activities, review files with the prosecutor's consent, and have the right to initiate evidence, thereby submitting motions for evidence. They have the right to submit a request for redress of damage or relief in accordance with Article 46 CC. Additionally, under Article 49a CCP, they may request that the court order the perpetrator to compensate for material or non-material damage (relief for a violation of personal rights). The injured party has numerous rights, including the right to initiate evidentiary proceedings and the possibility of filing appeals. However, the injured party ceases to be a party to the proceedings upon the filing of an indictment or its substrates, e.g., a motion for conditional discontinuation of proceedings (Article 336 § 1), or a motion for a conviction and the imposition of penalties agreed with the defendant or other measures provided for the offence with which they have been charged[17]. Hence, in court proceedings, the injured party loses their status as a party by the very fact of having been injured. If they wish to actively participate in such proceedings, they must submit a declaration stating that they will act as an auxiliary prosecutor. The injured party who intends to act as an auxiliary prosecutor in the trial brings charges alongside the prosecutor (Article 53 CCP) or (in certain situations – Article 55 § 1 CCP) in their stead[18].

Here, it is worth noting that, from the perspective of the General Data Protection Regulation, the principle of accountability is of key importance. In line with that principle, the controller is obliged to demonstrate that data

[17] K. Eichstaedt, [in:] D. Świecki (ed.), *Kodeks postępowania karnego*, Vol. 1: *Komentarz aktualizowany*, 2025, Lex, Article 49.

[18] See more broadly in H. Paluszkiewicz, [in:] K. Dudka (ed.), *Kodeks postępowania karnego. Komentarz*, 2023, Lex, Article 53.

is processed in compliance with the GDPR or to prove that they are not at fault for the damage that ensued. This principle reflects a change in the approach to compliance with personal data protection regulations by obligated entities. The controller's accountability for compliance with the principles of personal data processing stems from their legal responsibility to fulfill obligations, but it is not confined to that responsibility alone. Set out in Article 5(2) GDPR, the principle of accountability is further elaborated on in Article 24, which imposes an obligation on the controller to implement adequate technical and organizational measures to ensure that data is processed in accordance with the Regulation and to produce evidence that this is the case[19].

The principle of accountability is the opposite of the principle of presumption of innocence, regulated in Article 5 § 1 CCP, which states that "the defendant shall be presumed innocent until proven guilty and convicted by a final judgment". In a situation where law enforcement authorities charge a suspect under Article 107 AoPPD, the suspect's silence may work to their disadvantage. If a person charged with unlawful processing of personal data is unable to demonstrate that they are processing personal data in accordance with Article 6(1) or Article 9(2) GDPR, it may be assumed that they are either ignorant of the legal basis for personal data processing or are trying to conceal it. Regarding the attribution of criminal liability for the unauthorized processing of personal data, another vital element is the principle of minimization, which assumes that personal data must be adequate, relevant, and limited to what is necessary for the purposes for which they are processed. It is worth noting that controllers who process data in accordance with the above principles are less vulnerable to personal data protection breaches. The documentation of personal data processing and the training of personnel responsible for processing personal data within an organization are the duties of the data controller. Persons who have been authorized by the controller to process personal data and have been trained in this regard should be aware of their criminal liability for unauthorized processing of personal data.

A person whose data has been processed unlawfully may report a possible offense and may also seek to exercise their rights in civil proceedings by filing a lawsuit for infringement of personal rights, as provided in Articles 23 and 24 of the Civil Code. They may also lodge a complaint with the regulatory authority, the President of the Personal Data Protection Office.

The dynamics of offences under the Act on the Protection of Personal Data from 1999 to 2023 are shown in the table below.

---

[19] P. Drobek, [in:] E. Bielak-Jomaa, D. Lubasz (eds.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, 2018, Lex, Article 5.

Table 1. Total number of personal data protection offences in 1999–2023

Year	Proceedings instituted	Determined offences	Detected offences	Detection rate (%)
2023	514	742	572	76.99
2022	430	229	102	44.35
2021	468	819	628	76.60
2020	440	340	270	79.20
2019	330	509	466	91.60
2018	309	613	562	91.70
2017	374	179	114	63.70
2016	387	213	154	72.00
2015	381	2,192	2,114	96.40
2014	397	869	790	90.60
2013	372	1,624	1,556	95.80
2012	325	97	46	32.20
2011	317	106	46	43.00
2010	330	279	225	80.10
2009	387	332	261	78.60
2008	360	154	102	66.20
2007	327	506	445	87.80
2006	375	151	91	59.10
2005	355	173	113	63.80
2004	382	706	647	91.10
2003	337	761	711	93.20
2002	381	1,306	1,252	95.80
2001	347	592	560	94.10
2000	290	470	436	92.60
1999	152	58	43	74.10

Source: official website of the National Police Headquarters, https://www.policja.pl (accessed: 15.09.2025).

Table 1 shows the total number of offences under the Act on the Protection of Personal Data. Between 2002–2003 and 2013–2015, a sharp increase was observed in the number of identified offences (e.g., 2,192 offences were determined in 2015 compared to 706 in 2004). After 2016, the number of offences fluctuated significantly, starting at a low level in 2012 (97) and then

suddenly rising to 819 in 2021. It should be noted that the detection rate remained very high (above 90% in 2001–2005, 2013, and 2015). However, a notable drop below 50% was observed in 2012 (32.2%) and 2022 (44.35%), which may suggest that identifying perpetrators proved problematic in certain periods. In most years, the number of proceedings fluctuated between 300 and 400, then grew markedly after 2018, culminating in 2023 with 514 proceedings. This substantial increase may be attributed to the implementation of the GDPR in 2018, which heightened public awareness and consequently led to an increase in the number of reports. Increasingly, violations are occurring online. The rise of cybercrime has an impact on the scale of detected offences, while the decline in the detection rate after 2018 may result from the more complex nature of the cases.

In summary, the intention behind adopting criminal law provisions to protect personal data was to ensure recourse to criminal liability, but only in exceptional situations involving the most serious infringements. An analysis of the relevant statistical data from the National Police Headquarters suggests that the number of criminal proceedings in cases under Articles 107 and 108 remains stable. Furthermore, a review of selected criminal cases heard by national courts reveals that such proceedings often conclude with a conditional fine or a custodial sentence. There is no doubt that the provisions pertaining to criminal liability have a deterrent effect on the average citizen. Nonetheless, regarding the principle, their effectiveness in achieving the GDPR's goals may be questionable, as it depends on whether one of the essential principles of criminal sanctions – namely, the promptness and inevitability of punishment – is actually implemented in practice. Undoubtedly, after the provisions of the General Regulation came into effect, awareness of one's rights has increased among citizens, who have thus exercised their rights by initiating criminal or civil proceedings or by lodging a complaint with the regulatory authority.

References

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, C.H. Beck, Warsaw 2015.

Bielak-Jomaa E., Lubasz D. (eds.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, 2018, Lex.

Dudka K. (ed.), *Kodeks postępowania karnego. Komentarz*, 2023, Lex.

Fajgielski P., *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, [in:] idem, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, 2022, Legalis.

Litwiński P. (ed.), *Ustawa o ochronie danych osobowych. Komentarz*, 2018, Legalis.
Poniatowski P., *Niedopuszczalne lub nieuprawnione przetwarzanie danych osobowych – aspekty prawnokarne*, „Prokuratura i Prawo" 2021, No. 10.
Schabowski J., *Nielegalne przetwarzanie danych osobowych. Sankcje karne*, [in:] P. Litwiński (ed.), *Odo. Compliance. Praktyczny komentarz z przykładami i orzecznictwem*, 2025, Legalis.
Świecki D. (ed.), *Kodeks postępowania karnego*, Vol. 1: *Komentarz aktualizowany*, 2025, Lex.

Summary

Provisions of criminal law in personal data protection: some remarks

Keywords: penal law, injured party, personal data, personal data processing, breach.

Numerous academic studies have addressed the criminalisation of personal data protection offences in the Polish legal system. However, few publications offer structured information on the rights of injured parties in criminal proceedings where their personal data has been processed without legal grounds or authorisation. Although criminal law provisions pertaining to the protection of personal data have been in place since the Act on the Protection of Personal Data of 29 August 1997 and are now set out in the applicable Act on the Protection of Personal Data of 10 May 2018, many data controllers still process personal data without realising that they are continually exposing themselves to liability. This raises the question of the extent to which the new provisions on personal data breaches have ensured more effective and precise protection.

This study aims to analyse selected criminal law provisions regarding personal data protection, taking into account the rights of parties affected by unauthorised personal data processing. The paper approaches the issue from a legal theoretical standpoint, employing elements of dogmatic analysis. There is also a practical dimension to this, as the study discusses cases that have been heard in national courts.

The intention behind introducing criminal provisions for the protection of personal data was to impose criminal liability only in exceptional situations involving the most serious violations. However, an analysis of selected criminal cases heard by national courts shows that these proceedings often result in a conditional fine or imprisonment. While there is no doubt that the provisions shaping criminal liability have a deterrent effect on the average citizen, their effectiveness in achieving the objectives of the GDPR is questionable.

Streszczenie

Przepisy karne w ochronie danych osobowych – kilka uwag

Słowa kluczowe: prawo karne, pokrzywdzony, dane osobowe, przetwarzanie danych osobowych, naruszenie.

Zagadnienie kryminalizacji przestępstw przeciwko ochronie danych osobowych w polskim porządku prawnym jest przedmiotem wielu opracowań naukowych. Brakuje jednak publikacji, które porządkowałaby informacje na temat uprawnień pokrzywdzonego w procesie karnym w przypadku przetwarzania jego danych osobowych bez podstawy prawnej lub bez upoważnienia. Przepisy karne dotyczące ochrony danych osobowych funkcjonowały już w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (obecnie w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych), jednak nadal wielu administratorów przetwarza dane osobowe, nie mając świadomości, że codziennie naraża się na konsekwencje. W związku z tym powstaje pytanie, na ile wprowadzenie nowych przepisów w zakresie naruszeń bezpieczeństwa danych osobowych rzeczywiście zapewniło większą skuteczność i doprecyzowanie systemu ich ochrony.

Przedmiotem i celem niniejszego opracowania jest analiza wybranych przepisów karnych w zakresie ochrony danych osobowych z uwzględnieniem uprawnień pokrzywdzonego przestępstwem nieuprawnionego przetwarzania danych osobowych. Artykuł ma charakter teoretycznoprawny z wykorzystaniem elementów analizy dogmatycznej. Podjęta tematyka ma swój także wymiar praktyczny – przedstawia wybrane sprawy rozpoznawane przez sądy krajowe.

Intencją wprowadzenia przepisów karnych w ochronie danych osobowych było obwarowanie odpowiedzialnością karną jedynie sytuacji wyjątkowych, obejmujących najcięższe naruszenia. Analiza wybranych spraw karnych rozpoznawanych przez sądy krajowe wskazuje, że postępowania te kończą się warunkowym wymierzeniem kary grzywny lub karą pozbawienia wolności. Nie ulega wątpliwości, że przepisy kształtujące odpowiedzialność karną mają dla przeciętnego obywatela walor odstraszający, jednak co do zasady ich skuteczność może budzić wątpliwości.