Volume 22, Issue 2
December 2024

ISSN 1731-8297, e-ISSN 6969-9696
http://czasopisma.uni.opole.pl/index.php/osap

ORIGINAL ARTICLE
received 2023-11-29
accepted 2024-09-16
published online 2024-12-17

The problem of multiple interpretations of the terms "Information" and "Data" in the Polish Criminal Code and its consequences

Problem mnogości interpretacji terminów „informacja" oraz „dane" w polskim Kodeksie karnym i jego konsekwencje

WOJCIECH FILIPKOWSKI
University of Bialystok, Faculty of Law
ORCID: 0000-0001-6248-0888, w.filipkowski@uwb.edu.pl

Citation: Filipkowski, Wojciech. 2024. The problem of multiple interpretations of the terms "Information" and "Data" in the Polish Criminal Code and its consequences. *Opolskie Studia Administracyjno-Prawne* 22(2): 27–42. DOI: 10.25167/osap.5320.

Abstract: This paper examines the legal definitions of "information" and "data" within the Polish Criminal Code (CC), highlighting their implications for criminal liability, particularly in the realm of cybercrime. The research addresses the problem of definitional ambiguity, which poses challenges to the principles of legal certainty and consistency in criminal law. The study employs a dogmatic analysis of both general and specific parts of the CC, including an evaluation of commentaries and relevant judicial decisions. Findings indicate that the interchangeable use of "information" and "data" across various provisions leads to interpretational inconsistencies, potentially broadening the scope of criminal liability in a manner that contradicts constitutional principles. Moreover, the lack of precise legal definitions complicates the application of law by practitioners and undermines efforts to standardize legal frameworks for international cooperation in combating cybercrime. The author concludes that establishing clearer definitions is essential for the effective enforcement of criminal law and the protection of fundamental rights in the digital age.

Keywords: information, data, criminal law, legal definitions, criminal liability

Abstrakt: Niniejszy artykuł analizuje definicje prawne terminów „informacja" oraz „dane" w polskim Kodeksie karnym (KK), podkreślając ich konsekwencje dla odpowiedzialności

karnej, zwłaszcza w obszarze cyberprzestępczości. Badania koncentrują się na problemie niejednoznaczności definicyjnej, która stwarza wyzwania dla zasad pewności i spójności prawa karnego. W pracy zastosowano analizę dogmatyczną zarówno części ogólnej, jak i szczególnej KK, w tym ocenę komentarzy i istotnych orzeczeń sądowych. Wyniki wskazują, że zamienne stosowanie terminów „informacja" i „dane" w różnych przepisach prowadzi do niespójności interpretacyjnych, potencjalnie rozszerzając zakres odpowiedzialności karnej w sposób sprzeczny z zasadami konstytucyjnymi. Ponadto brak precyzyjnych definicji prawnych utrudnia praktykom stosowanie prawa i osłabia wysiłki na rzecz ujednolicenia ram prawnych dla międzynarodowej współpracy w zwalczaniu cyberprzestępczości. Artykuł kończy konkluzja, że wypracowanie precyzyjniejszych definicji jest niezbędne dla skutecznego egzekwowania prawa karnego oraz ochrony praw podstawowych w erze cyfrowej.

Słowa kluczowe: informacja, dane, prawo karne, definicja legalne, odpowiedzialność karna

Introduction

The Convention on Cybercrime of the Council of Europe contains the most important international legal definitions relating to the fight against the category of crime specified in the Convention's title. These definitions include that of the concept of "computer data", described in Article 1 as "any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function." This is a very broad approach, which indicates that data in a computer system can cover a large scope of content, from simple facts and figures to complex ideas and information. This also means that computer data is not just static information, but something that can be manipulated and processed by a computer. It is not limited to textual or numerical data but extends to executable code that can instruct a computer to perform specific tasks or functions. The broad scope of this definition can be considered both an advantage and a disadvantage. It covers a wide range of data types but can also be so extensive that it will lack detail. This breadth can lead to ambiguity in the interpretation of the elements of criminal acts, where precise definitions are of crucial importance. The definition does not clearly define the boundaries of what constitutes "computer data" and what does not. This indirectly demonstrates a scientific problem whose analysis cannot be easily found in the literature on this subject (Gordon and Ford 2006: 13; Jahankhani, Al-Nemrat and Hosseinian-Fa 2014: 149; Shkëmbi and Sina 2013: 327; Rabinská 2019: 285; Phillips, Davidson, Farr, Burkhardt, Caneppele, M.P. Aiken 2022: 379).

The examination of the definitional scope of "information" and "data" is pivotal in the context of combating not only cybercrime through criminal law, as evidenced by the Council of Europe's extensive work on these concepts. A precise understanding of these terms is crucial not only for creating national coherent

legal frameworks but also for ensuring the effective enforcement of laws designed to combat any type of crime related in any ways to those both terms.

Firstly, the standardization of definitions across jurisdictions, as promoted by the Council of Europe, provides a unified legal language that facilitates international cooperation (Miquelon-Weismann 2005: 351-354). In the realm of cybercrime, which is inherently transnational, this consistency is vital. The Budapest Convention on Cybercrime exemplifies how harmonized definitions enable countries to align their national legislation with international standards, promoting seamless cooperation in investigations, extradition, and intelligence sharing. This alignment reduces ambiguities that could otherwise hinder legal processes and the prosecution of cybercriminals across borders.

Moreover, as technology rapidly evolves, the terms "information" and "data" encompass increasingly complex and varied concepts, such as big data, artificial intelligence, and the Internet of Things. The Council of Europe's efforts in defining these terms allow legal frameworks to remain adaptable to emerging technological landscapes. This adaptability is essential for ensuring that laws do not become obsolete in the face of new cyber threats, thereby enhancing the resilience of legal systems against sophisticated cybercrime tactics.

The definitional clarity of "information" and "data" also holds significant implications for the protection of human rights (Clough 214: 708-712). By carefully delineating these concepts, the Council of Europe helps to strike a delicate balance between safeguarding individual rights, such as privacy and freedom of expression, and empowering law enforcement agencies to effectively combat crime. This balance is critical in preventing the misuse of power and ensuring that legal measures against crime do not inadvertently infringe upon fundamental democratic values.

Finally, the Council of Europe's definitional work influences global policy discussions, extending its impact beyond Europe to international forums such as the European Union (Directive 2013/40/EU) or the United Nations (Draft United Nations convention against cybercrime). By establishing robust definitions, the Council contributes to the development of global norms and standards related to data governance, cybersecurity, and digital rights. This leadership in defining key concepts helps shape how nations worldwide formulate their policies, fostering a more secure and rights-respecting digital environment.

The precise definitions of "information" and "data" are not merely academic concerns but are integral to the effective application of criminal law in the fight against crime, especially in the cyber realm. They provide the necessary legal clarity, facilitate international cooperation, ensure adaptability to technological advancements, protect human rights, and influence global policy-making, thereby underscoring the importance of rigorous definitional work in this

field. Without it, discrepancies can arise, hindering cross-border investigations, extradition processes, and the sharing of critical intelligence. By aligning Polish criminal law with international standards, such as those set forth by the Budapest Convention on Cybercrime, Poland can enhance its ability to engage in joint efforts against cybercriminals, streamline legal assistance, and contribute to a more cohesive global response to cyber threats. This alignment not only strengthens Poland's domestic legal framework, but also ensures that it is a reliable partner in the international fight against cybercrime, ultimately contributing to a safer and more secure digital environment worldwide.

Then, transferring the introductory considerations to the Polish criminal law system, it is necessary to begin by presenting dictionary definitions of terms important for the interpretation of the elements of a description of criminal acts. A dictionary of the Polish language contains as many as three possible scopes for the term "information": what is said or written about someone or something, also communicating something, an information-providing department of an office or institution, and data processed by a computer. However, as Barański (2017: 112) and Radoniewicz (2016: 132) rightly point out, the contemporary scope of the meaning of the term has changed. The dictionary meaning is gradually narrowing it to an interpretation typical of economics as well as information and computer technology (ICT).

For further consideration, the first and third of those definitions will be relevant. The same dictionary also contains two definitions of the term "data". First, "data" is colloquially defined as follows: "facts or figures that can be relied on in an argument"; second, data is "information processed by a computer". The latter definition is applied more narrowly, as it refers to ICT that involve processing by computers or similarly functioning devices (e.g., smartphones). This definition is also relevant to the further considerations in this paper, relating to the operation of ICT networks and, consequently, the scope of criminal liability. In the case of both terms, dictionaries of the Polish language even suggest that they are synonymous in selected meanings and that one term can be defined using the other. This supports the view of the primary nature of both terms, which can lead to interpretation problems (Adamski 2000: 37-40). Of key importance for further consideration are the first meanings of these terms. Their comparison can lead to two conclusions. First, data is more primary and objective than information; data is certain facts, situations, or events as perceived by an observer (as well as devices equipped with the appropriate sensors). It can take the form of numbers, e.g., on a certain scale and expressed in specific units of measurement or as a string of characters. In contrast, in the case of information, the element of communication between the sender and the recipient is important.

In a mathematical analogy, data serves as the foundation, while accompanying remarks, forming information, can be objective deductions or subjective opinions. Both undergo transmission, with the recipient capable of processing data by augmenting received information or altering its content. This processing results from examining the message or synthesizing data and information from alternative sources. For these reasons, the two terms cannot be equated or used interchangeably when interpreting the text of a legal act (Barański 2017: 113; Radoniewicz 2016: 131).

As a side note to the deliberations, it should be mentioned that the term "information" is used repeatedly in the text of the Polish Constitution (PC); however, it is not defined. In contrast, commentators on this most important act of national legislation rarely address the essence of the term themselves, and instead – focus on interpreting the adjectives describing it and the subjective (characterization through the person of the sender or the recipient) and objective (the scope and nature) aspects. In the context of the right to access public information (Article 61 PC), it should be understood as a statement that can be verified as to its truthfulness and cannot be invalidated by a conventional decision of a public authority (Sokolewicz and Wojtyczek 2016). Additionally, the issue of information and data protection also appears in the context of the right to privacy (Article 47 PC), secrecy of communications (Article 49 PC), and protection of personal data (Article 51 PC) (Łakomiec 2015: 57). At this point, a mention may be made of the Supreme Court's resolution of 22 January 2003, which in its justification contains the observation that "the Constitution provides a general framework for both the freedom of information and the right to information. The concretisation and limits of this freedom and this right must be sought in other legal acts" (Barański 2017: 60). However, no one has noticed that there is a lack of consistency in the interpretation of the term "information" or "data" within a single piece of legislation – the CC.

1. Research assumptions

The main research problem focuses on different interpretations of the term "information" and "data" as used in the text of the CC. This diversity of interpretations in the legal doctrine poses a significant challenge and needs to be carefully examined because of its implications related to the scope of criminal liability of perpetrators of crimes.

The following specific hypotheses are posed:

1. The lack of clarity of the term "information" and "data" poses a threat to the fundamental principles of legal certainty and definitiveness in criminal law, which can lead to the broadening of criminal liability as a result of broad

interpretations. Such an outcome would contradict the principles enshrined in the Polish Constitution.

2. The use of synonymous terms referring to content makes it difficult for practitioners to apply law consistently.

3. In the chapter describing types of cybercrimes, it is noticeable that the scope is narrowed down to issues related to ICT, which is another example of the inconsistency of the interpretation of the characteristics of different types of criminal acts in a single piece of legislation.

This paper contains a dogmatic analysis carried out separately for the general part (containing the principles of criminal liability and the types of criminal sanctions) and the specific part of the CC, in particular the criminal acts described in Chapter XXXIII (Crimes against the protection of information). For the purpose of this study, an analysis of recently published commentaries on the Penal Code (as available in the electronic legal database LEX) has been presented, including selected judgements of the Polish Supreme Court and the Constitutional Court. In principle, such publications offer the most detailed legal analyses incorporating relevant literature and jurisprudence. On the other hand, the considerations of the scopes of the meaning of the two terms are relevant to the determination of the generic and individual object of an attack, particularly of cybercrimes.

To find a more universal meaning of the results of the ongoing dogmatic research on Polish regulations, the following issues can be identified:

1. Precise definitions of legal terms are important in any legal system. Their absence can lead to controversy and different interpretations of law, which poses a challenge to the justice system not only in Poland, but also in other jurisdictions (Barański 2017: 112).

2. From the perspective of criminal liability, the law should be clear and certain. Otherwise, it can lead to unequal treatment of perpetrators of the same crimes, resulting in unfair or unpredictable judicial decisions.

3. Adequate and fair interpretation and application of the criminal law provides the basis for its effective response to crimes committed, not only in cyberspace.

2. The characteristics of the term "information" in the general part of the CC

In the general part of the CC, there are five provisions in which the terms under analysis are used. A characteristic feature of commentaries on this part of the CC is the fact that the commentators either do not analyse the scope of the meaning of "data" or "information" at all, treat these two terms as syno-

nyms, or only analyse their characteristics. This confirms the observation as to their primary nature, but also suggests that they are used in the sense generally accepted in the Polish language.

The first provision is Article 16 (1) CC, which contains a description of the institution of preparation. As one of its material forms, given as an example is "collecting information". None of the commentators directly addresses the essence of the meaning of the term "information". In their considerations, they focus on the description of the verb "collect", which allows them to determine the context and circumstances of this activity. J. Giezek (2021) defines it as "an act as a consequence of which the perpetrator expands the scope of his or her knowledge, thus eliminating or reducing the extent of his or her ignorance about the surroundings (about someone or something)." V. Konarska-Wrzosek (2023) extends this description using the concepts of "knowledge", "news" and "data". She defines "collecting" as "expanding one's knowledge on a particular subject by acquiring, by any means possible, the news and data needed to commit a crime", and gives several examples. In contrast, M. Małecki (2016) rightly describes "collecting" as a process that consists of two stages. The first involves the acquisition of information, and the second is the perpetrator's cognitive accumulation of the collected data in his or her consciousness and memory, and their intellectual analysis. This author rightly stipulates that information cannot be equated with its carrier. None of the commentators places restrictions on the scope of sensory perception or sources of information (their legal or factual nature).

Another institution described using one of the concepts studied is "aiding and abetting" (Article 18 (3) CC). In this case, too, the legislator mentioned by way of example the activity of "providing advice and information". Such a view – in accordance with the principles of linguistic interpretation – suggests different meanings. M. Kulik (2023) and J. Giezek (2021) do not make detailed determinations in this regard. P. Kardas (2016), on the other hand, does not analyse the two concepts separately, but emphasizes the functional context of this "information transfer", pointing to its relevance to the achievement of the assumed goal, i.e. the commission of a criminal act by another person. On the other hand, V. Konarska-Wrzosek (2023) clearly defines and separates the conceptual scopes used by the legislature. First, she considers "advice" to be guidance or instruction, and the mere fact of providing them indicates communication between two people: their sender and recipient. Therefore, it seems that "advice" is a special type of information, and the use of this term emphasizes the subjective side of this unique criminal act, that is, the immediate perpetrator's desire to facilitate the commission of a criminal act. The phrase "providing information" used in Article 18 (3) CC, on the other hand, leads

to "enriching the perpetrator's knowledge with news". Once again, the effort by some commentators to limit their considerations only to the search for terms synonymous with "information", without defining it more precisely in a synthetic way, but only giving its individual meanings, is becoming apparent.

In the next two examples of the use of the term "information", there are also no considerations concerning the conceptual scope of "information" in the comments analysed. This applies to Article 60 (3) (the so-called "small immunity witness") and Article 114a (3) CC. In the first case, the disclosure of information to a law enforcement agency (the recipient) is one of the prerequisites for applying this institution to the perpetrator (the sender). The CC only describes its scope, i.e., it must relate collectively to the individuals involved in the commission of a crime and the relevant circumstances of its commission (Kulik 2023). In the second case, there is also a lack of analysis by commentators directly on the conceptual scope of the term "information". The very content of the norm enshrined in Article 114a (3) CC defines its source (a criminal record or a court of a member state of the European Union) and its nature (insufficient extent to establish a conviction).

As a side note to the analysis of the general part of the CC, a mention should be made of the legal definition of a document contained in Article 115 (14) CC. The term "record on an information storage medium" was used there. Again, the commentators do not analyse the meaning of the term "information" (Mozgawa, Budyn-Kulik, Kozłowska-Kalisz and Kulik 2023). At the same time, they do not put a limit on what a record is or what the storage medium itself is. The key considerations only relate to their association with a specific law, and the content of the record, which is evidence of a law or legal relationship, or a legally significant circumstance. J. Giezek (2021) comments that the content in question can be expressed in words or graphic signs, and that it "got there as a result of the will of its sender."

3. Characterization of the term "information" based on selected criminal acts specified in the specific part of the CC

The specific part of the CC contains several types of criminal acts where the terms under analysis appear in the description of the objective side or object of protection. Moreover, Chapter XXXIII, titled Crimes against the protection of information, directly relates to the object of the analyses presented herein.

In the case of the first group of provisions – as was the case in the general part of the Criminal Code – it is difficult to find commentators' considerations

on the scope of the terms "data" or "information". Meanwhile, these characteristics appear in Articles 118a (2), 132, 246, 259b, 299, 305, and 311 CC.

Article 118a (2) (6) CC describes crimes against humanity. It contains the formulation of mere characteristics of "information", i.e., those regarding the person or his or her whereabouts, or conveys false information regarding the person or his or her whereabouts, with the intention of depriving such a person of legal protection for an extended period (Budyn-Kulik 2023).

Article 132 CC (intelligence disinformation), on the other hand, uses the term "news" which is synonymous with "information" (Chlebowicz 2012: 45-46). This article criminalizes behaviour whereby the perpetrator, while providing intelligence services to the Republic of Poland, misleads the Polish state authority by, among other things, concealing true information, or providing false information that is of vital importance to the Republic of Poland. The studied comments lack analysis in the context of both terms: "information" or "message" (Budyn-Kulik 2023).

In the description of the objective side of the act under Article 246 CC, as many as four terms were used that are worthy of attention from the point of view of the analyses being carried out. A perpetrator is a public official (or someone acting upon his or her instructions) who uses violence or an unlawful threat, or otherwise physically or mentally abuses another person in order to obtain specific testimony, explanations, information, or statements; all of these terms denote a type of communication between the sender (victim) and the recipient of information (perpetrator). The first two have a specific meaning in the criminal procedural law; the last is a term of legal and juridical language used in its various branches. Only T. Razowski (2012) points out that the last two terms "are so general that they cause the scope of the provision of Article 246 CC to include the impact not only on the accused (the suspect or even the suspected person) and the witness, but also on the expert, interpreter, specialist, and probation officer." Other commentaries lack in-depth linguistic analyses relating to the terms used, indicating their colloquial understanding.

Article 259b CC uses the term "information" as an example of behaviour that conditions the application of extraordinary mitigation of punishment or conditional suspension of the execution of the sentence for the perpetrator of the crime specified in Article 259a CC (crossing the border of the Republic of Poland to commit a terrorist crime), who voluntarily abandoned aiding and abetting other persons in the commission of that crime and disclosed to a law enforcement agency all relevant circumstances of the commission of the act, in particular information about the individuals who committed the crime. Also, in this case, commentators do not undertake to define the essence of the term "information" (Mozgawa 2023).

The term is also used in the description of the grounds for not being subject to punishment or for extraordinary mitigation of punishment for the perpetrator of money laundering offences in Article 299 (8) CC. None of the commentators analysed conducted a detailed analysis of that term (Kulik 2023).

Article 305 (2) CC (interference with a public tender) uses the term "information" to describe the characteristics of the objective side. Commentators only provide possible single meanings of this term that may apply to the commission of this type of act. M. Kulik (2023) quotes O. Górniok's view that "information" should be understood as "any news, regardless of form, concerning the circumstances of the tender." W. Wróbel and M. Iwański (2022), G. Łabuda (2021), and T. Oczkowski (2023) comment on the characteristics of "information" but not its essence.

Furthermore, Article 311 CC (capital fraud) uses the term "information" in the description of the criminal act. Again, it can be noted that in their considerations, commentators omit the definition of the term and focus instead on analysing its characteristics: truthfulness or falsity, and its relevance to the sale or acquisition of securities and an increase or decrease of contributions (Kulik 2023).

The above observations lead to the following conclusion: even though the terms analysed are important for the description of a criminal act or the circumstances affecting the punishment, the commentators do not interpret them or only describe their characteristics or types. Furthermore, references to publications or court judgments concerning the meaning of the term "information" are rare or non-existent.

4. The characteristics of the term "information" in Chapter XXXIII of the Criminal Code

Distinct circumstances arise in delineating the object of protection for criminal acts outlined in Chapter XXXIII CC, titled "Crimes against the protection of information". Unlike other criminal acts, precision in defining the generic object of protection is crucial for consistent interpretation (Lewulis 2021: 19; Siwicki 2012: 249-51). Consequently, commentators strive for a more nuanced interpretation of terms describing both generic and specific objects of protection (Filipkowski 2023: 188).

In this Chapter of the CC, "information" is specified as "news or the sum of news about a person or a state of affairs, concerning facts and constituting a logical whole", the definition attributed to B. Kunicka-Michalska and cited by P. Kozłowska-Kalisz (2023). The protection of information in criminal law is multifaceted, contingent on the nature of the criminal act infringing upon

the integrity, availability, or confidentiality of information. These terms denote, respectively:

- Integrity – it is tantamount to immutability; no one is authorized to change information or data.
- Accessibility – any authorized person is able to see and use the information or data at any time they choose.
- Confidentiality – only authorized individuals are allowed to see the information or data.

These facets assume paramount importance in the realm of criminal law (Adamski 2000: 41-42). Presently, the services proffered in cyberspace to its users hold greater societal and economic significance than the information or data itself. However, within the individual objects of protection delineated in Chapter XXXIII CC, more conventional forms of information are also encompassed. This consideration is pivotal when interpreting descriptions of criminal acts.

W. Wróbel and D. Zając (2016) astutely highlight the evolving understanding of the term "information", a transformation attributed to the escalating computerization and digitization of social life. Formerly linked closely to the act of informing, i.e., conveying specific messages, information is now conceptualized independently of its transmission. Yet, it is crucial to underscore that the activity of transmitting information remains integral. It retains significance for comprehending the essence of information and the intricacies of its creation and processing. The authors also aptly draw attention to the distinctive features of information processing within IT systems.

The transmission of information has evolved beyond human-to-human interactions, with IT systems increasingly playing dual roles as both senders and recipients. They autonomously process information, adhering to predefined criteria. This extends beyond human communication to interactions between devices within IT systems and between devices and humans. Decision-making is progressively reliant on data or information supplied by ICT systems. In Article 265 (1) CC, the Act of 5August 2010 on the protection of classified information, addressing classified information aids in interpreting the term "information". However, it focuses solely on safeguarding its confidentiality, lacking a synthetic definition of the essence of "information". Commentaries on subsequent CC articles (266, 267, and 268) often overlook the term "information", concentrating on breached aspects or violated information services. Exceptions include Lipiński (2021) and Lach (2023), referencing a ruling of the Supreme Court of 5 March 2019 that defines "information" as a set of characters with a specific meaning, limiting this understanding to Chapter XXXIII CC and IT system operations. Article 267 (2) CC on protection, according to Wróbel and Zając (2016), applies only to IT systems processing computer data with intellectual

content. However, the nature of this intellectual content remains ambiguous. Commentary on ICT network-transmitted information highlights the transmission of metadata, protected by criminal law, detailing communication particulars. Regarding Article 268 (2) CC, commentators, such as Kozłowska-Kalisz (2023), emphasize temporal characteristics, relevance, recording form, and the impediment of authorized access. Lipiński (2021) posits that information must possess intellectual content for familiarization. In the context of Article 269b (1) CC, Wróbel and Zając (2016) assert that computer data falls within the broader category of information, while other commentators focus on analysing distinct categories of computer data.

5. Data as an element of the objective side of the description of a criminal act

The Criminal Code contains the term "data" used in four contexts (Filipkowski 2023: 192):

- computer data (Articles 165 (1), 268a (1), 269 (1 and 2), 269a, and 287);
- computer data storage media (Articles 268 (2) and 269 (2));
- personal data (Article 190a (2)); and
- data described in a special way (Articles 190a (2), 219, and 269b (1)).

Some of these contexts directly relate to ICT systems or networks, so they involve cybercrimes.

Article 165 (1) CC pertains to endangering many lives, health, or significant property through interference with computer data processing. D. Gruszecka (2021) anchors the term "data" in Article 1 (B) Budapest Convention, defining it as any representation of facts suitable for computer processing, underscoring its utilitarian function.

In the analysis of Articles 268a (1), 269 (1 and 2), 269a, and 287 CC, the term "data" is recurrent but lacks a clear definition. P. Kozłowska-Kalisz (2023) cites A. Adamski who characterizes data as a record of specific information stored on a computer drive. J. Giezek (2021) references a ruling of the Supreme Court of 30 September 2015, offering a similar definition. W. Wróbel and D. Zając (2016) provide a more intricate scope, defining data as any character sequence with functional meaning within an IT system, distinguishing it from cultural information defined in Article 268a CC.

Contrastingly, Article 296b (1) CC outlines data facilitating unauthorized access, explicitly naming computer passwords and access codes. Although other data types lack explicit definitions, they enable specific operations in an IT system. Wróbel and Zając (2016) consistently view data as an electronic charac-

ter sequence allowing system operations, encompassing biometric data beyond passwords and access codes mentioned in Article 269b (1) CC.

Conclusions

This paper undertakes to examine the concepts of "data" and "information" within the context of the CC. The study aims to delineate the comprehensive scope of these terms and their ramifications on criminal culpability. The ensuing conclusions, as extrapolated from the investigation (also referenced in Filipkowski 2023: 196), are as follows: "data" and "information" emerge as fundamental concepts intricately interconnected, particularly within the milieu of the information society and the data-centric economy. While these terms find mention in both the general and specific sections of the CC, their explication by commentators remains cursory. This suggests that their interpretations are generally confined to colloquial language, inherently less precise than the legal lexicon. A notable exception lies in Chapter XXXIII, where commentators expound on these terms within the context of ICT systems. Defining both terms synthetically proves challenging. "Data" is posited as a record of information stored on any data storage medium, arising from human activity or the functioning of IT systems, even without human cognizance, oversight, or approval. "Information" is construed as a set of characters endowed with specific meaning in accordance with accepted linguistic rules of content construction. The last proposal to define the scope of the concept is in line with the subjective (cognitivist) model of capturing "information" raised by Barański (2017: 114). It involves a sender and a recipient, constituting an element of the communication process in interpersonal, human-IT, and exclusive IT system interactions. To elucidate the scope of these terms, the legislature incorporates additional characteristics germane to describing a criminal act, manifesting as adjectives (pertaining to truthfulness, falsity, relevance, or objective scope) or functional descriptions (pertaining to meaning or scope of use in conjunction with selected verbs).

These study findings accentuate the imperative to address the multifaceted challenges entwined with interpreting the term "information" and "data" in the CC. Ambiguity and the plethora of potential interpretations not only imperil legal certainty, but also elicit constitutional apprehensions. In its judgment of 25 May 1997, the Constitutional Court noted that the absence of a legal definition in a given piece of legislation, where a concept is used that does not have a fixed meaning and is understood in various ways, depending on the purpose of the regulation of the specific law, is a "technical-legislative defect" (Barański

2017: 114). This seems to be the situation with the regulations contained in the Criminal Code.

The proposed delineations of these terms bear pivotal significance in ensuring a more coherent application of criminal law in Poland, thereby directly impacting the efficacy of prosecuting and combating crimes, including those committed in the cyberspace.

In conclusion, this analysis of legal challenges and predicaments in Poland serves as a springboard for contemplating universal challenges in the realm of criminal law in other countries. Clarity and certainty in the law, safeguarding human rights, and adapting legal frameworks to evolving technologies transcend national boundaries, resonating with legal systems worldwide.

Abbreviations

CC – Criminal Code
IT – information technology
ICT – information and computer technology
PC – Polish Constitution

References

Legislation

Act of 2 April, 1997, The Constitution of the Republic of Poland, Official Journal of the Republic of Poland of 1997, No. 78, item 483.

Act of 5 August, 2010, on the protection of classified information, Official Journal of the Republic of Poland of 2019, item 742.

Act of 6 June, 1997, the Criminal Code, Official Journal of the Republic of Poland of 2022, item 1138.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Official Journal of the European Union of 2013, L 218/8.

The Convention on Cybercrime of the Council of Europe, European Treaty Series – No. 185, Official Journal of the Republic of Poland of 2015, item 728.

Judicial decisions

Judgment of the Constitutional Court of 25 May, 1999, ref. U 19/97 OTK 1998, no. 4, item 47.

Ruling of the Supreme Court, 30 September, 2015, II KK 115/15. LEX No. 1866883.

Ruling of the Supreme Court, 5 March, 2019, II KK 208/18. LEX No. 2639897.

Resolution of the Supreme Court, 22 January, 2003, I KZP 43/02, LEX No. 57085.

Secondary sources

Adamski, Adam. 2000. *Prawo karne komputerowe*. Warszawa: C.H. Beck.

Barański, Michał. 2017. *Informacja w ujęciu prawnym przez pryzmat zagadnień terminologicznych*. Katowice: Wydawnictwo Uniwersytetu Śląskiego.

Budyn-Kulik, Magdalena. 2023. In: *Kodeks karny. Komentarz aktualizowany*, (ed.) Marek Mozgawa. LEX.

Chlebowicz, Piotr. 2012. Interpretacja pojęcia dezinformacji w świetle art. 132 k.k. *Studia Prawnoustrojowe* 15: 41–48.

Clough, Jonathan. 2014. A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. *Monash University Law Review* 40(3): 698–736. https://ssrn.com/abstract=2615789.

Draft United Nations convention against cybercrime. https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf.

Filipkowski, Wojciech. 2023. Dane i informacja jako przedmioty zamachu cyberprzestępstwa. In: *Współczesne oblicze prawa karnego, prawa wykroczeń, kryminologii i polityki kryminalnej*, (eds.) Janusz Bojarski, Natalia Daśko, Jerzy Lachowski, Tomasz Oczkowski, Agata Ziółkowska. 187–196. Warszawa: Wolters Kluwer.

Giezek, Jacek. 2021. In: *Kodeks karny. Część ogólna. Komentarz*, (ed.) Jacek Giezek. LEX.

Gordon, Sara and Richard Ford. 2006. On the definition and classification of cybercrime. *Journal in Computer Virology* 2: 13–20. DOI: 10.1007/s11416-006-0015.

Gruszecka, Dagmara. 2021. In: *Kodeks karny. Część szczególna. Komentarz*, (ed.) Jacek Giezek. LEX.

Jahankhani, Hamid. Ameer Al-Nemrat and Amin Hosseinian-Far. 2014. Chapter 12, Cybercrime classification and characteristics. In: *Cyber Crime and Cyber Terrorism Investigator's Handbook*, (eds.) Francesca Bosco, Andrew Staniforth and Babak Akhgar. 149–164. Walham: Elsevier Science.

Kardas, Piotr. 2016. In: *Kodeks karny. Część ogólna. Tom I. Cześć I. Komentarz do art. 1-52*, (eds.) Włodzimierz Wróbel and Andrzej Zoll. LEX.

Konarska-Wrzosek, Violetta. 2023. In: *Kodeks karny. Komentarz*, (ed.) Violetta Konarska-Wrzosek. LEX.

Kozłowska-Kalisz, Patrycja. 2023. In: *Kodeks karny. Komentarz aktualizowany*, (ed.) Marek Mozgawa. LEX.

Kulik, Marek. 2023. In: *Kodeks karny. Komentarz aktualizowany*, (ed.) Marek Mozgawa. LEX.

Lach, Arkadiusz. 2023. In: *Kodeks karny. Komentarz*, (ed.) Violetta Konarska-Wrzosek. LEX.

Lewulis, Piotr, 2021. O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber” i „komputerową” dla celów praktycznych i badawczych. *Prokuratura i Prawo* 3: 12–32.

Lipiński, Konrad. 2021. In: *Kodeks karny. Część szczególna. Komentarz*, (ed.) Jacek Giezek. LEX.

Łabuda, Grzegorz. 2021. In: *Kodeks karny. Część szczególna, Komentarz*, (ed.) Jacek Giezek. LEX.

Łakomiec, Katarzyna. 2015, Konstytucyjne gwarancje ochrony prywatności informacyjnej wobec rozwoju nowych Technologii. *Przegląd Legislacyjny* 1(91): 57–73.

Małecki, Mikołaj. 2016. In: *Kodeks karny. Część ogólna. Tom I. Cześć I. Komentarz do art. 1-52*, (eds.) Włodzimierz Wróbel and Andrzej Zoll. LEX.

Miquelon-Weismann, Miriam F. 2005. The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process? *UIC John Marshall Journal of Information Technology & Privacy Law* 23: 329–362.

Mozgawa, Marek. 2023. In: *Kodeks karny. Komentarz aktualizowany*, (ed.) Marek Mozgawa. LEX.

Mozgawa, Marek and Magdalena Budyn-Kulik, Patrycja Kozłowska-Kalisz, Marek Kulik. 2023. In: *Kodeks karny. Komentarz aktualizowany*, (ed.) Marek Mozgawa. LEX.

Oczkowski, Tomasz. 2023. In: *Kodeks karny. Komentarz*, (ed.) Violetta Konarska-Wrzosek. LEX.

Phillips, Kirsty. Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele and Mary P. Aiken. 2022. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Science* 2: 379-398. DOI: 10.3390/forensicsci2020028.

Rabinská, Ivana. 2019. Preservation and Rendition of Computer Data in Slovak Criminal Procedure Code. *International and Comparative Law Review* 19(2): 285–299. DOI: 10.2478/iclr-2019-0025.

Radoniewicz. Filip. 2016. *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*. Warszawa: Wolters Kluwer.

Razowski, Tomaz. 2021. In: *Kodeks karny. Część szczególna. Komentarz*, (ed.) Jacek Giezek. LEX.

Shkëmbi, Aldo and Darjel Sina. 2013. Cybercrime in the Perspective of the European Legal Framework. *Mediterranean Journal of Social Sciences* 4 (9): 327–331. DOI: 10.5901/mjss.2013.v4n9p327.

Siwicki, Maciej. 2012. Podział i definicja cyberprzestępstw. *Prokuratura i Prawo* 7-8: 246–25.

Sokolewicz, Wojciech and Krzysztof. Wojtyczek. 2016. In: *Konstytucja Rzeczypospolitej Polskiej. Komentarz, Tom II*, (eds.) Leszek Garlicki and Marek Zubik. LEX.

Wróbel, Włodzimierz and Dominik Zając. 2016. In: *Kodeks karny. Część szczególna, Tom II, Cześć II, Komentarz do art. 212-277d*, (ed.) Włodzimierz Wróbel and Andrzej Zoll. LEX.

Wróbel, Włodzimierz and Mikołaj Iwański. 2022. In: *Kodeks karny. Część szczególna, Tom III, Komentarz do art. 278-363 k.k.*, (ed.) Włodzimierz Wróbel and Andrzej Zoll. LEX.