#### dr Tomasz Wierzchowski

assistant professor at the Academy of Economics and Humanities in Warsaw ORCID 0000-0002-3986-8187

# PERCEPTION OF THE CONCEPT OF CRIME IN THE INFORMATION SOCIETY OF THE XXI CENTURY

## **Summary**

The purpose of the article is to present the multidimensionality of the perception of both the concept of crime and the factors shaping it in modern society. The author refers to the elements that determine whether an act is or can be a crime. Particular attention was also paid to issues related to information and its role in modern society and the definition of the information society. The reader has the opportunity to see how complex a mechanism is in the process of criminalization of behavioral norms from the point of view of lawyers, political scientists, and sociologists.

**Keywords:** law, crime, criminal legislation, technology, perception, information society

#### **Introductory issues**

Each period in the history of civilization and, criminologically speaking, society, has its defining concepts and signatures, to which reference makes it possible to define a given period in the development of that society. Just as the term "age of steam" positions the framing of this period of history to the English Industrial Revolution of the late 18th and early 19th centuries, the turn of the 20th and early 21st centuries will certainly be remembered as the time of the information society, where the term "information" is the signature to be referred to in every aspect. This raises the natural question of what information is. In the sense of scientific disputation, it is a relatively young concept, as it dates back to the turn of the 20th century – it was introduced in terms of terminology into the branch of physics, which is

thermodynamics<sup>1</sup>. In this way, a quantitative definition of probability calculus was determined. This definition is particularly captured in the aspect of technical sciences (information technology). As can be seen, it reflects practically little of not only the colloquial but also the legal (more on that later) meaning of the term. It is not intuitive and distances the meaning of information as news, making the connection with probability (broadcast messages) and the choice of possibilities associated with it<sup>2</sup>. Of course, in addition to the technical and physical concept of information, there are many conceptual references, such as forms of interpretation of the term that refer to single or multiple systems of reference. From such a position, information, which can be understood by reference to a certain state of affairs as an arrangement of mapping between things or phenomena, as well as a property of messages, messages (their content) – this is the basic meaning of the key term, as indicated by even a cursory analysis of the research material<sup>3</sup>.

Importantly from the point of view of legal discourse, of course, the term "information" also functions in various branches of law. Its importance is recognized only by the courts, which emphasize its complexity<sup>4</sup>. As rightly noted, with the development of society (the information society, as discussed further below) and technological advances, hypotheses and views began to emerge that directly attempt to define the conceptual scope precisely in terms of the right<sup>5</sup>. This is particularly evident not only in the criminal law addressed in this material but also – and perhaps especially – in civil law. Therefore, the adoption of such and not other laws has an undeniable impact both on the regulation of legal protection of information itself and on the legal constructs of which information is an essential part, regardless of the branch of law. This is, of course, confirmed in the doctrine, where the ambiguity of information in the legal sense is raised in unison, as well as its lack of attachment to a specific branch of law and its essence for each<sup>6</sup>. The complexity of this concept is, moreover, the reason why there is no statutory definition of it in the Polish legal order; moreover, due to its indefinability, the information belongs to the "key concepts of civilization" - such as

<sup>&</sup>lt;sup>1</sup> M. Hetmański, Świat informacji, Difin Publishing House, Warsaw 2015, p. 13.

<sup>&</sup>lt;sup>2</sup> *Idem, Epistemologia informacji*, Copernicus Center Press, Krakow 2013, pp. 32–54.

<sup>&</sup>lt;sup>3</sup> Idem, *Świat*..., op. cit., p. 14.

<sup>&</sup>lt;sup>4</sup> Resolution of the Supreme Court of January 22, 2003, I KZP 43/02, OSNKW 2003, no. 1, item 17.

<sup>&</sup>lt;sup>5</sup> M. Barański, *Informacja w ujęciu prawnym przez pryzmat zagadnień technologicznych*, University of Silesia Publishing House, Katowice 2017, p. 12.

<sup>&</sup>lt;sup>6</sup> W. Góralczyk (ed.), *Prawo informacji. Prawo do informacji*, Publishing House of Leon Koźmiński Academy of Entrepreneurship and Management, Warsaw 2006, p. 9.

"matter", "culture", "light"<sup>7</sup>. However, attempts are being made if not to define in full, then at least to identify information common to each branch of law. This requires a certain standardization, which leads us to reject the possibility of using an intuitive and cybernetic-formal model and adopting a semantic model. Information is presented as a certain content, signaled by linguistic signs transmitted by the sender in the form of a message<sup>8</sup>. Dogmatic considerations regarding this content will certainly continue.

Another key element that should be highlighted is the term "information society". Like "information" it is a relatively young concept, as it appeared in the public space after World War II, although it was used in 1937 by economist Friedrich von Hayek in the context of information as a material good<sup>9</sup>. The Second World War, not coincidentally, was a caesura of sorts, as after its end and in light of its political consequences, attempts were made to redefine the society that grew out of the wars (especially the last one) of the industrial era. This was necessary because society in a global sense was divided, as it were, into two conflicting political systems, capitalism and socialism. Hence the initiative to configure a completely new model of society, how different from political categorization, based on functional rather than political assumptions. Somewhat obviously, the dynamic development of such scientific fields as game theory, operations research, cryptology, and information theory had a significant impact on the emergence of this direction. The real breakthrough came in 1960 in the US, when the Commission of the Year 2000 was established to forecast the economic future and long-term social and structural changes<sup>10</sup>.

The term "information society" was first used in 1963 by ethnologist Tadao Umesao, who developed the theory of an information-processing society. It was later popularized by media theorist Kenichi Koyama, who used it in his 1968 treatise *Introduction to Information Theory*. In 1971, the Japan Computer Usage Development Institute approved a plan to implement an information society in Japan and set it as a national goal by the year 2000. One of its authors was Yoneji Masuda, who set the stages for building such a society through specific state actions, such as the establishment of a central

<sup>&</sup>lt;sup>7</sup> K. Dobrzeniecki, *Lex informatica*, Scientific Society of Organization and Management "Organizers' House", Toruń 2008, p. 26; Judgment of the Supreme Administrative Court of June 10, 1999, I SA/Po 1947/98, "Przegląd Orzecznictwa Podatkowego" 2000, no. 3, item 90; K. Tarnacka, *Right to information in Polish constitutional law*, Sejm Publishing House, Warsaw 2009.

<sup>&</sup>lt;sup>8</sup> J. Petzel, Informatyka prawnicza. Zagadnienia teorii i praktyki, Liber, Warsaw 1999, p. 35.

<sup>&</sup>lt;sup>9</sup> J. Papińska-Kacperek, Spoleczeństwo informacyjne, PWN Scientific Publisher, Warsaw 2008, p. 14.

<sup>&</sup>lt;sup>10</sup> Ibid.

data bank, a remotely controlled medical system, and a workforce qualification system – to create the world's first information society in Japan<sup>11</sup>.

In Europe, the term "information society" was popularized by Alain Minc and Simon Nora, who used it in the report *L'Informatisation de la société* produced in 1978 and dedicated to the President of the French Republic. Martin Bangemann (EU Commissioner from 1993 to 1999 responsible for the development of telecommunications and information technology) made a visible contribution to its development. He is also the author of the report *Europe and the Global Information Society – Recommendations to the European Council*<sup>12</sup>.

The definition of the information society remains a separate issue. There is no apparent unanimity regarding both the semantic and material substance of the concept. On the fundamental issue, researchers agree – it is a new socio-economic formation. On the other hand, when describing it, the same factors that define it are not always mentioned; depending on the discipline within which this definition is made (sociology, economics, or, finally, law). The first major definitional attempts were made by the Organization for Economic Cooperation and Development (OECD). In the forum of the organization, the term was used in 1975, and in 1977 an attempt was made to create a model classifying member states on a scale that leads to the information society. In 1988, a document summarizing the meetings of the Committee for Information, Computer, and Communication Policy predicted that the economy of the future would be an information economy, and society would increasingly be an information society. This is expected to mean that information will account for the bulk of the added value of most goods and services, and related spheres of activity will increasingly affect households and citizens<sup>13</sup>. An interesting concept of the information society was presented by H. Kubicek; namely, he defined the information society as a socio-economic formation in which the productive use of a resource such as information and knowledge-intensive production plays a dominant role. The term in question is thus used to describe a society in which individuals – that is, consumers or workers – make total use of information<sup>14</sup>.

<sup>&</sup>lt;sup>11</sup> Y. Masuda, *Computopia*, Diamond Publishing House, Warsaw 1983; idem, *Wprowadzenie do świata informacji*, Pelican Publishing House, Warsaw 1987.

<sup>&</sup>lt;sup>12</sup> A. Mattelart, *Społeczeństwo informacji*, Universitas, Krakow 2004.

<sup>&</sup>lt;sup>13</sup> OECD, *Definition of the ICT Sector*, Annex 1B, http://www.oecd.org/dataoecd/49/44/35930616. pdf (accessed July 2023).

<sup>&</sup>lt;sup>14</sup> J. Papińska-Kacperek (ed.), op. cit., p. 17.

The purpose of this article, of course, is not to focus on the definitional problems of the information society. The defining criterion here will certainly be a high degree of technological development. Hence, these criteria cannot be reduced to processes in the IT sector, but consider the issue in light of all technological progress. Closing this part of the argument, it is necessary to point out one more definitional treatment of the problem, this time by Umberto Eco<sup>15</sup>. According to Eco, society will be classified into three social strata: the TV proletariat, the dignitaries, and the cognitaries. The TV proletariat are people who have trouble coping with modern IT devices, i.e. old people, residents of underdeveloped countries, or people uninterested in new technologies, who conventionally stopped at the stage (era) of television. Digitariats are those who can use modern devices, and have mastered the infosphere and the world of computers and the Internet, but do not think about how they function. The top social class is ICT specialists who can control electronic devices, such as knowing how to program computers – that is, the cognitariat.

A description of the information society would not be complete without at least a cursory mention of its totalitarian model, which is undoubtedly the Social Trust System being tested in China<sup>16</sup>. The Social Trust System is a system being implemented in China to monitor and evaluate citizens' behavior for compliance with the law and the rules of social intercourse. It is based on databases that receive information from all kinds of state registers, courts, and public administration bodies, but also from city monitoring or mobile applications. According to the organizational and theoretical framework, the main goal of establishing a Social Trust System in China was and is to build a society with a high level of trust, in which individuals and organizations will respect the law and non-legal standards of social life. This is done by assigning social ratings to citizens based on their behavior, which directly translates into facilitations or inconveniences in their daily lives. High ratings provide the opportunity to obtain facilitated access to all kinds of public benefits, while low ratings result in a loss of public confidence and consequently, difficult access to benefits, the housing or credit market, and in extreme cases can lead to restrictions on travel, including leaving China. The system, still being developed and refined, in addition

<sup>&</sup>lt;sup>15</sup> U. Eco, Nowe środki masowego przekazu a przyszłość książki, in: M. Hopfinger (ed.), Nowe media w komunikacji społecznej w XX wieku: antologia, Oficyna Naukowa, Warsaw 2002.

<sup>&</sup>lt;sup>16</sup> M. Bartoszewicz, *Chiński system zaufania społecznego*, "Geopolitical Review" 2020, no. 32, pp. 58–67.

to monitoring and assessing the behavior and creditworthiness of citizens, comprehensively covers the activities of businesses with its coverage. Participation in it is mandatory, and it covers all companies registered in China, including foreign companies. Companies' activities are constantly monitored for compliance with legal and extra-legal norms of social intercourse, and a lack of knowledge of the areas in which an entity must comply with the requirements of the System can put it at risk of losing public trust and even being blacklisted<sup>17</sup>. All of this defines how the totalitarian model of the information society works, in which information, in addition to its economic, social, and civilization-forming role, also has the function of controlling society. This is also possible in a democratic society when, for example, IA – artificial intelligence – is given the primacy of self-determination in social issues. It remains a question of the future, but it is reasonable to believe that the legal system is not ready for such a challenge, not only in the field of criminal law but especially in civil law.

## Crime in the information society

The question about the perception of the phenomenon of crime in the information society is not only a question about the perception of the institutions of criminal law. This is primarily a question about the limits of criminalizing an act and defining the legal standard. Returning to the issue of information in legal terms – in the Criminal Code – it is worth recalling that this concept is defined in principle only in the terms of the provisions of Chapter XXXIII, that is, in the context of crimes against the protection of information<sup>18</sup>. The application of basically any interpretation in terms of these provisions prompts a judgment that allows the term "information", in addition to recourse to colloquial language, to direct towards information technology<sup>19</sup>. There are calls in the doctrine to move away from the colloquial, so-called verb definition of information, understanding it as not so much the process of informing, but the message itself, i.e. "sign", "sound", "record", "cipher" hiding some meaningful content<sup>20</sup>. It is clear, therefore, that consideration of the process of information generation and its processing may

<sup>&</sup>lt;sup>17</sup> https://www.kochanski.pl/chinski-system-zaufania-spolecznego/ (accessed: 03.08.2023).

<sup>&</sup>lt;sup>18</sup> Law of June 6, 1997 – Criminal Code, Dz. U. 1997, no. 88, item 553, as amended.

<sup>&</sup>lt;sup>19</sup> E.g. W. Wróbel, Przestępstwa przeciwko ochronie informacji, in: A. Barczak-Oplustil et al., Kodeks karny. Część szczególna: komentarz, t. 2: Komentarz do art. 117–277, 3rd edition, Lex a Wolters Kluwer business, Warsaw 2008, p. 1247.

<sup>&</sup>lt;sup>20</sup> Ibid.

remain a separate issue<sup>21</sup>. Of course, the strictly theoretical considerations did not stop there. It is worth mentioning at this point the jurisprudence of the Supreme Court, which, for example, in its resolution of January 22, 2003, after analyzing the colloquial understanding of information and referring to branches of law other than criminal law, ruled that the conceptual scope of the term "information", which the legislator placed in the Criminal Code, is different from the scope of this concept, which is found in the Constitution, but also from the term used in the press law and from the subject meaning of public information contained in the wording of the Law on Access to Public Information<sup>22</sup>. The judges of the Supreme Court made it clear that the provisions on information placed in the Criminal Code, as well as the provisions of other legal acts regulating the issue at hand, drew a line and concretized the constitutional right to information and freedom of speech, press, and expression, of which information is a component<sup>23</sup>. Of course, the conceptual scope of the term "information" is under permanent study and is also constantly evolving, if only because of new institutions that need to be legitimized both socially and legally - such as "remote work" and "drone law", for example. If we agree with the assertion that the law is a regulator of social and economic life, then, of course, it must be not only known but also understood by the average citizen. Computerization, and the resulting digital services, for example, are the need for new regulations to help protect the public from the intentional and unintentional abuses associated with new technologies.

All of these contentious issues arise naturally but require not only some time for a legal norm to emerge but also appropriate regulation. An important issue is, for example, the protection of values and the right to privacy on the Internet, as well as the right to privacy in connection with ubiquitous monitoring, which on the one hand performs an important and useful social function – general prevention and crime prevention. It is also, in many jurisdictions, evidence when a crime is committed. At the same time, monitoring certainly implies an invasion of privacy, which can be used both by an employer to surveil employees and by government services or, finally, by private individuals who install it to protect their property. And the problems that arise from even a momentary observation and analysis of our reality

<sup>23</sup> Ibid.

<sup>&</sup>lt;sup>21</sup> A. Haręża, E. Prandota-Prandecka, *Fluktuacje pojęcia informacji – zarys rozważań w kontekście nauk penalnych*, in: L. Bogunia (ed.), *Nowa Kodyfikacja Prawa Karnego*, vol. 19, University of Wroclaw Publishing House, Wroclaw 2006, p. 379.

<sup>&</sup>lt;sup>22</sup> Resolution of the Supreme Court of January 22, 2003, I KZP 43/02, OSNKW 2003, no. 1, item 17.

are incalculable. Mention can be made of the issue of potential culpability for the actions and any activity undertaken by the computer program. To whom should responsibility be assigned? Computer owner, software owner, software developer, or computer user? What law should be applied to an online program? The country of origin of the computer owner, the country of the software developer, where the computer is currently operating, or the country on whose servers the online software is installed<sup>24</sup>?

So what is a crime for the information society? From a doctrinal point of view, the definition of a crime (under the criminal law of each country, of course) is sufficiently clarified, as it opens the criminal codification. In the case of Polish criminal law, this is Article 1 § 1: "Only those who commit an act prohibited under penalty by the law in effect at the time of its commission are subject to criminal liability"<sup>25</sup>. The interpretation of this provision is sufficiently known, and it is possible to accept the thesis that it is properly formulated and basically timeless, that is, it meets the conditions on which the law should be made. At the same time, the substantive scope of this provision allows for the criminalization of all qualitatively new acts, provided only that they are recognized as torts by the legislature. Thus, only the intention of a political authority or a real social need will allow some behavior to be considered unlawful (there may be many more of these factors – for the purposes of this discussion, they can be omitted here).

The problem of perception of crime is the problem of understanding in the social space of the legal norm for behavior in qualitatively new technological conditions, although the technological aspect, however most important for the information society, should be treated here auxiliary. Certain behaviors within social and legal norms are permitted by society and there is social acquiescence towards them. This is, of course, a process that results from many factors, including custom, the economic condition of society, the degree to which economic needs are met, the provision of a sense of security, or, finally, the possibility of being a victim of crime (victimization factor), which should be understood here as a personal threat of crime. This last factor remains very important, even crucial – as it explains the need for penalization or lack thereof. These relationships can be explained using the crime of corruption as an example. Why exactly is corruption? Because it is a crime that has two sides – the illegal and the legal (under Polish law). In addition, it is not penalized by the legislature in a single provision but

<sup>&</sup>lt;sup>24</sup> J. Papińska-Kacperek, op. cit., p. 30.

<sup>&</sup>lt;sup>25</sup> Law of June 6, 1997 – Criminal Code, op. cit.

includes several provisions contained in the Penal Code, such as Article 228 of the Penal Code or 229 of the Penal Code and others. By the way, the point here is not to discuss the rationale for corruption in detail. It is important that in public life, in addition to the criminal act, which is subject to criminal regulation and is criminalized, there is a legal form of corruption. Thus, there are behaviors and relationships in public life that are designed to use power to advance vested interests and achieve private gain – it is these processes and decisions that are referred to as legal corruption<sup>26</sup>. Listed here are such behaviors as nepotism, conflict of interest, henchmen, and cronyism<sup>27</sup>. Such behavior is present on both public and private levels. Their perception appears to be a reflection of family entrepreneurship, a manifestation of operability, business resourcefulness, and the ability to establish favorable business relationships. State institutions, by virtue of the tasks they perform and the funds they spend on them, are highly desirable, reliable, and solvent customers for the business world. Organizations in the public and private sectors in many cases combine strong economic ties through ongoing ventures, resulting in sizable sums of money going into the accounts of certain business entities<sup>28</sup>. In contrast, the problem of public perception of such acts is closed by the lack of punishment for them – which allows for their public tolerance. Moral considerations do not count or are toned down in the general acceptance of non-penal behavior. As indicated by the studies conducted, until recently, society still accepted corruption, even criminalized corruption, due to the inability to meet basic social needs, as it were, obvious in the former communist country<sup>29</sup>. Thus, in the public perception of this type of crime, even despite the common knowledge that it is criminalized and morally negative, such conduct is acceptable in certain cases<sup>30</sup>. Why is this the case? There are many reasons

 <sup>&</sup>lt;sup>26</sup> D. Kaufmann, P.C. Vicente, *Legal corruption*, "Economics & Politics" 2011, no. 2, pp. 195–219;
 P. Domadenik, J. Prasnikar, J. Svejnar, *Legal corruption, politically connected corporate governance and firm performance*, "IZA Discussion Papers" 2014, vol. 8321, pp. 1–26; O. Cincer, M. Johnston, *Measuring Illegal and Legal Corruption in American States: Some Results from the Corruption in America Survey*, Edmond & Lily Safra Center for Ethics, Cambridge, Mass. 2015, vol. 58, pp. 1–41.

W. Walczak, Przestępstwa korupcyjne a legalna korupcja – aspekty ekonomiczne i prawne,
 "Homeland Security Review" 2019, no. 21, pp. 44–80.

<sup>&</sup>lt;sup>28</sup> Ibid.

<sup>&</sup>lt;sup>29</sup> A. Siemaszko, B. Gruszczyńska, M. Marczewski, P. Ostaszewski, *Społeczna percepcja zagrożeń korupcyjnych w Polsce*, in: J. Kosiński, K. Krak, A. Koman (eds.), *Korupcja i antykorupcja. Selected Issues. Part III*, Department of Publishing and Printing of the Police Training Center, Warsaw–Legionowo 2012, pp. 13–33.

<sup>&</sup>lt;sup>30</sup> M. Marmola, A. Olszanecka-Marmola, Korupcja i przeciwdziałanie korupcji w Polsce. Wymiar psychospołeczny i prawnopolityczny, University of Silesia Publishing House, Katowice 2021,

for this, including the already mentioned shortages of social goods, which, despite the political transformation, still exist – such as access to medical care. Another reason is that corruption is a crime that does not generate victims (in the common sense). Victimization of all members of society due to corruption is therefore not an obvious phenomenon that belongs to the common consciousness. Thus, in the absence of a concretized and personalized victim, there is a lack of conviction about the harmfulness of the act, as well as its economic costs. Another reference point in this type of crime is its "non-kinetic" nature. Corruption is a non-violent crime, so it does not cause fear. So are economic crimes, which are characterized not only by a lack of violence but also by terminology and *modus operandi* – unlike other crimes – that are completely incomprehensible to the layman.

Violent crimes are always viewed negatively, regardless of their content capacity, degree of social danger, as well as the real threat to the community. Recalling the crime of corruption in these considerations is a deliberate effort since regardless of the degree of technological or economic development of society, this crime will be a constant presence in the catalog of criminalized behavior. This is because it does not only apply to the public sphere (in terms – public power and public funds) but can also apply to the private sector, such as sports competitions. If such assumptions are made vis-à-vis the information society, then the object of greatest protection would remain information. Here, information is the chief asset to be protected, hence the disputes over its criminalization.

Referring to the Polish criminal law system, which has already been mentioned, it must be said that the situation is both simple and, so to speak, archaic, as exemplified by the provisions in the current criminal codification concerning, for example, the crime of espionage and disinformation (Articles 130 and 132 of the Criminal Code). Without wishing to analyze the entirety of the legislation, it is important to note the word "news" that appears in the text, which is undoubtedly synonymous with the term "information". In the context of such an interpretation, it is necessary to amend the above-mentioned provisions – if only because of the nature of modern intelligence (espionage) activities, such as hostile to a state so-called "hybrid" activities, which can undoubtedly also consist of a planned and executed disinformation operation. This status disinformation activities in entirely new factual as well as legal categories – such as "conducting disinformation on the Internet". For formal and material reasons, these can be actions

oriented only to achieve such an effect, as well as linked to others – such as the so-called hate speech<sup>31</sup>. The dissemination through electronic media of opinions that target specific individuals, especially non-public ones, is deeply victimizing and, if only because of its scale and method of transmission, cannot be treated as a typical slander crime under Article 212 of the Criminal Code. The act that fulfills the characteristics of so-called hate speech is much more complicated. Words or otherwise online posts may also contain threats, blackmail, or terms related to any discrimination. It is important that they intentionally affect the condition of the targeted people – including in a group convention. Thus, we are dealing here with a group of crimes that, depending on the specific facts, will be dealt with in a specific criminal classification. The question that arises, however, is whether hate speech can be viewed as a separate crime and thus separately criminalized and included in criminal laws. This is, of course, a dogmatic issue, but one that is noticeable in social discourse and generates great public emotion, especially when human tragedies such as suicide occur as a result of "hate speech". It should be noted that in such states of facts, there is a tendency to include these acts as separate crimes. Here the perception of the crime seems quite simple.

The problem arises when potential criminal acts are covered by acts that are not uniformly perceived but have a common link, such as the place where they are committed – such is the case with cyberspace. Cyberspace is essential to the functioning of the state and actions taken in this area have a direct impact on all key areas, such as infrastructure, for example. Both individual perpetrators and criminal groups and institutions of hostile states can use tools such as cyberterrorism, cyber espionage, *hacking*, and others (all detailed technological descriptions are intentionally omitted here). Examples of such actions are numerous enough, suffice it to mention, for example, the attack on Estonia by cyber criminals in 2007, when vital branches of the country's operations, from websites to critical infrastructure<sup>32</sup>, were blocked in three weeks of cyber attacks.

<sup>&</sup>lt;sup>31</sup> M. Margaret, *The future of social crime control in the hate speech of social media with media literacy*, in: *Proceedings of3rd International Conference on Community Development (ICCD)*, vol. 3, no. 1, October 2021.

<sup>&</sup>lt;sup>32</sup> B. Biernacik, Nauka i najnowsze narzędzia informatyczne w służbie bezpieczeństwa cyberprzestrzeni – piątego wymiaru walki zbrojnej, in: Ł. Roman, K. Krassowski, S. Sagan, D. Wróblewski (eds.), Wykorzystanie nowoczesnych narzędzi informatycznych w identyfikacji zagrożeń, Publishing House of the Alcide de Gasperi School of Euroregional Economy, Józefów 2018, pp. 13–14.

There are, of course, more similar examples. The threat of such action or even the acts committed are perceived by the public primarily as a danger to social order and personal safety. If such actions are accompanied by the aforementioned feelings, they should undoubtedly be considered a perception of criminal activity. Significantly, as emphasized as dogma, cyber security is correlated with so-called global economic security, which should be understood as "a relatively endogenously and exogenously balanced state of functioning of the national economy, in which the occurring risks of imbalances are kept within the designated and acceptable organizational and legal norms and rules of social coexistence"<sup>33</sup>. "Acts committed in cyberspace that can be identified as crimes are primarily asymmetric threats. It is the action of taking advantage of the dissimilarity of the parties by using methods, means, and tactics that are unconventional from the opponent's point of view"<sup>34</sup>. In cyberspace, criminals take advantage of the asymmetrical nature of threats and dangers by launching attacks on its vulnerabilities<sup>35</sup>.

The new social organization which is the information society, moreover, is affected by phenomena that should be qualified not only as criminal acts (we need to think here about a global trend, not just based on the Polish Criminal Code). It is worth mentioning, for example, the problem of digital exclusion as a victimization category. Digital exclusion can be described as a variation of exclusion *per se*<sup>36</sup>. In this view, it must be understood as one of the manifestations of exclusion, e.g. economic or political, and in this context means the literal exclusion of an individual from the reach of the Internet, computer, digital entertainment, or remote work. As is rightly noted, due to the digital nature of the knowledge economy, digital exclusion should be understood not as a variant of exclusion, but as its premise. Digital exclusion is not related to the loss of participation in digital reality but in social reality as such<sup>37</sup>. This is the result, in large part, of the transformation to an information community, in which competence to use *hardware* and

<sup>&</sup>lt;sup>33</sup> K. Raczkowski, Percepcja bezpieczeństwa ekonomicznego i wyzwanie dla zarządzania nim w XXI wieku, in idem (ed.), Bezpieczeństwo ekonomiczne. Wyzwania dla zarządzania państwem, Wolters Kluwer Polska, Warsaw 2012, p. 81.

<sup>&</sup>lt;sup>34</sup> K. Lidel, Bezpieczeństwo informacyjne państwa w dobie zagrożeń terrorystycznych i innych zagrożeń bezpieczeństwa narodowego, in: T. Jemioło, J. Kisielnicki, K. Rajchel (eds.), Cyberterrorism – New Challenges of the 21st Century, Toruń 2008, p. 505.

<sup>&</sup>lt;sup>35</sup> T. Muliński, Zagrożenia bezpieczeństwa dla systemów informatycznych e-administracji, CeDe-Wu, Warsaw 2015, p. 36.

<sup>&</sup>lt;sup>36</sup> A. Jeran, Wykluczenie cyfrowe – aspekty normatywne a rzeczywistość, in: A. Siwik, L. Habera (eds.), Od robotnika do internauty. W kierunku spoleczeństwa informacyjnego, AGH Uczelniane Wydawnictwa Naukowo-Dydaktyczne, Kracow 2009, p. 185.

<sup>&</sup>lt;sup>37</sup> Ibid, p. 185.

information is the equivalent of earlier social competencies such as reading and writing or living by measured time. The lack of these competencies in individuals constitutes real exclusion from society – which statues such a person as a victim in the criminological sense.

## Conclusions

The changing condition of society and the range of stimuli and factors to which it is subjected are variables that directly affect the behavior of individuals, and thus shape legal norms and consequently lead to new laws. Civilizational changes, or those factors that shape society, include the degree of economic evolution of society, the perception of moral changes, the prevailing political systems, and technological changes. Each of these factors is a first factor, as important as the others. In the information society, technology is only a means that defines the most socially significant factor, information.

Information is a tool that allows a society to function in its environment. Through its use, a member of society can expand his or her abilities and skills. This gives it its proper stature and importance. It is one of the basic components of human life<sup>38</sup>. It determines the standard of living of members of society, and lifestyles, and will begin to determine – if it doesn't already – social norms. This is an inevitable and irreversible phenomenon. Until recently, one of the many synonyms for the information society used universally, was globalization. Of course, the two conceptual scopes are different, but there is a material scope that is common – and this already gives a certain synergy.

The perception of a socio-legal phenomenon such as crime, in addition to strictly dogmatic elements based on, among other things, legal theory, is a social phenomenon that is very much influenced by the level of morality (and its understanding) of society and political currents. At the same time, as is well known, the latter are also largely based on public emotions surveyed by polling studios. This was the model until recently. However, it should be felt that the process of perceiving crime in the information society will be linked, obviously, to the procedure of information (in any form) and will realistically affect individuals, or, more precisely, the damage caused by crime to themselves and the property they own. These goods will be inextricably linked to information and its coverage – such as the "hate speech" cited in the text. Of course, such a procedure had been going on before – but it took place through other carriers and communicators. The twilight

<sup>&</sup>lt;sup>38</sup> K. Mordaszewski, D. Laskowski, Prawne aspekty ochrony informacji. Wybrane zagadnienia, in: B. Hołyst, J. Pomykała, P. Potejko (eds.), Nowe techniki badań kryminalistycznych a bezpieczeństwo informacji, PWN Scientific Publisher, Warsaw 2014, p. 19.

of the press in material format and the transmission of information (access to information) in real-time are causing the public to recognize the value of information so that an attack on it in any form is or can be perceived as a crime. When any new form of such an act, which is not regulated by criminal law, is realized, it is very likely to be viewed as a crime. Thus, the degree of society's penalization orientation is based on information.

"Never before, you will say, has the demand for information been so great. This is evidenced by the success of free newspapers, the growing number of news channels reporting news twenty-four hours a day, and the ever-increasing number of visitors to news sites where the information is updated... Whatever the future of traditional media and the development of new forms of mass media, one thing is certain: our society cannot do without information. Neither citizens nor those in charge of politics, the economy, and finance can act or make decisions without adequate data"<sup>39</sup>.

## **Bibliography**

#### Literature

- Barański M., Informacja w ujęciu prawnym przez pryzmat zagadnień technologicznych, University of Silesia Publishing House, Katowice 2017.
- Bartoszewicz M., *Chiński system zaufania społecznego*, "Przegląd Geopolityczny" 2020, no. 32.
- Biernacik B., Nauka i najnowsze narzędzia informatyczne w służbie bezpieczeństwa cyberprzestrzeni – piątego wymiaru walki zbrojnej, in:
  Ł. Roman, K. Krassowski, S. Sagan, D. Wróblewski (eds.), Wykorzystanie nowoczesnych narzędzi informatycznych w identyfikacji zagrożeń, Publishing House of the Alcide de Gasperi School of Euroregional Economy, Józefów 2018.
- Cincer O., Johnston M., *Measuring Illegal and Legal Corruption in American States: Some Results from the Corruption in America Survey*, Edmond & Lily Safra Center for Ethics, Cambridge, Mass. 2015.
- Dobrzeniecki K., *Lex informatica*, Scientific Society of Organization and Management "Organizers' House", Toruń 2008.
- Domadenik P., Praśnikar J., Svejnar J., *Legal corruption, politically connected corporate governance and firm performance*, "IZA Discussion Papers" 2014, vol. 8321.

<sup>&</sup>lt;sup>39</sup> B. Poulet, *Śmierć gazet i przyszłość informacji*, Czarne Publishing House, Volowiec 2011, pp. 255–257.

- Eco U., *Nowe środki masowego przekazu a przyszłość książki*, in: M. Hopfinger (ed.), *Nowe media w komunikacji społecznej w XX wieku: antologia*, Oficyna Naukowa, Warsaw 2002.
- Góralczyk W. (red.), *Prawo informacji. Prawo do informacji*, Publishing House of Leon Koźmiński Academy of Entrepreneurship and Management, Warsaw 2006.
- Haręża A., Prandota-Prandecka E., *Fluktuacje pojęcia informacji zarys rozważań w kontekście nauk penalnych*, in: L. Bogunia (ed.), *Nowa Kodyfikacja Prawa Karnego*, vol. 19, University of Wroclaw Publishing House, Wroclaw 2006.
- Hetmański M., *Epistemologia informacji*, Copernicus Center Press, Krakow 2013.
- Hetmański M., Świat informacji, Difin Publishing House, Warsaw 2015.
- Kaufmann D., Vicente P.C., *Legal corruption*, "Economics & Politics" 2011, no. 2.
- Lidel K., Bezpieczeństwo informacyjne państwa w dobie zagrożeń terrorystycznych i innych zagrożeń bezpieczeństwa narodowego, in: T. Jemioło, J. Kisielnicki, K. Rajchel (eds.) Cyberterrozym – Nowe wyzwania XXI wieku, Toruń 2008.
- Margaret M., *The future of social crime control in the hate speech of social media with media literacy*, in: *Proceedings of 3rd International Conference on Community Development (ICCD)*, vol. 3, no. 1, October 2021.
- Marmola M., Olszanecka-Marmola A., *Korupcja i przeciwdziałanie korupcji w Polsce. Wymiar psychospołeczny i prawnopolityczny*, University of Silesia Publishing House, Katowice 2021.
- Masuda Y., Computopia, Diamond Publishing House, Warsaw 1983.
- Masuda Y., *Wprowadzenie do świata informacji*, Pelican Publishing House, Warsaw 1987.
- Mattelart A., Społeczeństwo informacji, Universitas, Krakow 2004.
- Mordaszewski K., Laskowski D., *Prawne aspekty ochrony informacji. Wybrane zagadnienia*, in: B. Hołyst, J. Pomykała, P. Potejko (eds.), *Nowe techniki badań kryminalistycznych a bezpieczeństwo informacji*, PWN Scientific Publisher, Warsaw 2014.
- Muliński T., Zagrożenia bezpieczeństwa dla systemów informatycznych e-administracji, CeDeWu, Warsaw 2015.
- Papińska-Kacperek J. (red.), *Społeczeństwo informacyjne*, PWN Scientific Publisher, Warsaw 2008.
- Petzel J., *Informatyka prawnicza. Zagadnienia teorii i praktyki*, Liber, Warsaw 1999.

- Poulet B., Śmierć gazet i przyszłość informacji, Czarne Publishing House, Volowiec 2011.
- Raczkowski K., Percepcja bezpieczeństwa ekonomicznego i wyzwanie dla zarządzania nim w XXI wieku, in: idem (ed.), Bezpieczeństwo ekonomiczne. Wyzwania dla zarządzania państwem, Wolters Kluwer Polska, Warsaw 2012.
- Siemaszko A., Gruszczyńska B., Marczewski M., Ostaszewski P., Społeczna percepcja zagrożeń korupcyjnych w Polsce, in: J. Kosiński, K. Krak, A. Koman (eds.), Korupcja i antykorupcja. Wybrane zagadnienia. Part III, Department of Publishing and Printing of the Police Training Center, Warsaw–Legionowo 2012.
- Tarnacka K., *Prawo do informacji w polskim prawie konstytucyjnym*, Sejm Publishing House, Warsaw 2009.
- Walczak W., *Przestępstwa korupcyjne a legalna korupcja aspekty ekonomiczne i prawne*, "Homeland Security Review" 2019, no. 21.
- Wróbel W., Przestępstwa przeciwko ochronie informacji, in: A. Barczak-Oplustil et al., Kodeks Karny. Część szczególna: komentarz, vol. 2: Komentarz do art. 117–277 k.k., ed. 3, Lex a Wolters Kluwer business, Warsaw 2008.

## Sources of law

Law of June 6, 1997 – Criminal Code, Dz. U. 1997, no. 88, item 553, as amended.

## Case law

- Judgment of the Supreme Administrative Court of June 10, 1999, I SA/Po 1947/98, "Tax Jurisprudence Review" 2000, no. 3, item 90.
- Resolution of the Supreme Court of January 22, 2003, I KZP 43/02, OSNKW 2003, no. 1, item 17.

## **Online sources**

- https://www.kochanski.pl/chinski-system-zaufania-spolecznego/ (accessed: 03.08.2023).
- OECD Definition of the ICT Sector, Annex 1B, http://www.oecd.org/dataoecd/49/44/35930616.pdf (accessed: 03.08.2023).

## **Conflict of interest**

No

Source of funding