polish 2(222)'23
sociological
review
ISSN 1231 – 1413
DOI:10.26412/psr222.05

WOJCIECH MINCEWICZ
University of Warsaw

Explication and Classification of Social Deviations on the Internet: Cyberdeviation as a New Social Phenomenon

Abstract: The aim of the presented study is to conceptualize and regulate the meaning of the term *social cyberdeviation*. The analysis carried out in the first part was based on the etymological and inductive methods, as well as contextual analysis with the definitions of cross-border cybercrime. To achieve the aim of the work and indicate the contents of the concept, it turned out to be necessary to determine whether it is possible to indicate the existence of standards among the online virtual community that are recognized by most of its members. The nominal definition of *cyberdeviation* as a violation of the norms prevailing in the virtual community is the starting point for the second part of the article, the purpose of which is to classify activities that violate the norms in cyberspace. The gradation of behavior indicates that the situations on the Internet are: low-intensity activities that focus primarily on social norms, not legal norms; medium intensity, where the criterion is a violation of a legal norm; high intensity acts that are legally penalized nor accepted in the entire community, which clearly violate social norms.

Keywords: cyberdeviation, cybercrime, cyberspace, virtual community, netiquette, anomy

Introduction

In 2022, 62.5 percent of the world's population had access to the Internet. 4.95 billion people use the global network, with 350 million more people added during the year (Global Digital Report 2022). The constant development shows that the Internet is a vehicle of civilizational change in the modern world. Even the industrial revolution did not have such a significant impact on the everyday life of man and the evolution of social structure as modern progress in technology and IT. Cyberspace is a place where, from the turn of the 20th and 21st centuries, a new virtual society is being created, and the Internet itself has permanently changed humanity (Castells 2001, 2004). Its development has launched a new research field in other areas of science. The technological dimension is naturally the domain of IT specialists, but it is also a challenge for lawyers—where it is essential to establish the norms of national and international law (see Akdeniz 2016; Svantesson 2016; Savin 2020; Hörnle 2021)—as well as for political scientists, defining the relations between the power of the citizen and the development of the Internet (see Rydlewski 2021) or sociologists (see Jemielniak 2019). The Internet is an immanent part of modern human life. However, it is sometimes used in an undesirable way. With the development of the Internet, the phenomena observed in everyday life are transferred. Unfortunately, this includes those of a negative nature, which, in the language of science, are associated with the concept of *social evil*. Among the scientific disciplines that examine significantly harmful social phenomena, four basic research directions have developed: social pathology, social disorganization, deviation, and social stigma (Cygielska 1976). These terms, although synonymous, draw attention to various accents of the same phenomenon (Podgórecki 1969). All of the above are directly related to the violation of social norms and values (Pospiszyl 2009). The central category for the presented study is the concept of deviation, which can be defined in two ways—legally and socially—and associated in the field of science with criminology and sociology.

The presented study analyzes social evil on the Internet from a sociological perspective and has theoretical aspirations as well as methodological. Its initial objective is to conceptualize the concept of cyberdeviation based on "classical" theories of deviation. The presented multidimensional analysis of the meaning of the concept and the attempted explication are intended to be an introduction to further empirical studies. The analysis of existing materials and original studies indicates that the literature lacks a semantic cluster that would explain the importance of social deviations on the Internet. Hence, to establish the meaning of the term, the theoretical reflection should be as precise and standardized as possible. The scope of the term will be determined via the etymological and inductive methods as well as contextual analysis limited to the intersection definition—cybercrime (Pawłowski 1978; Mider 2013). The conclusion of the considerations will be to propose a definition of a nominal nature, which will establish the meaning of the term "cyberdeviation" (Mayntz et al. [1969] 1985). In the second part, the author attempts to create a classification of deviant behaviors in the gradation-vertical approach. There are two ways of classifying deviant behavior in sociological works. The first is related to an exhaustive enumeration of types of behavior that are considered deviant. This may lead to the creation of a specific catalog of deviant behaviors, which will be helpful in further conceptual work. The formulation of such a catalog is based on subjective assessments of the researcher and includes behaviors that the researcher considered violating certain norms adopted in each society.[1] The second way of distinguishing deviant behaviors consists in classifying a given behavior as deviation provided that this behavior is found not to comply with the behavioral patterns, values, norms, social order, standards, social goals, and rules expected by society (Macharski and Gizbert-Studnicki 1975).

Social Pathologies as a Threat in the Space of Security: an Outline of a Literature Review

Behavior of a pathological nature: (1) violates the applicable social norms, (2) is contrary to the generally accepted system of values, (3) is destructive in nature, the consequence of which is social harm, (4) requires taking organized actions aimed at counteracting and responding to and the elimination of the effects of their appearance in public space. In the 21st century, there is a significant increase in interest in the issues of behavior and pathological phenomena, both in theoretical and empirical dimensions (see, e.g., Salakhova et al. 2016; De Souza 2017; Hirvonen 2018; Laitinen and Särkelä 2019; Thompson 2019;

[1] Understanding Society—Internet Society presented in the further part of the paper.

Jacobsen and Nørup 2020). Successive authors focus on conducting empirical research aimed at learning about: (1) the essence of pathological phenomena (Messas and Tamelini 2018; Pawłowski et al. 2019; Wites 2019; Has et al. 2020; Gerasimoski 2021), (2) the causes of and the factors that determine them (Nomokonov 2017; Shatyr et al. 2017; Ortega-Esquembre 2020; Cover 2020), (3) conduct preventive activities (Liba 2008; Ahmadi and Branch 2011; Button and Marsh 2019), (4) quantity and degree of intensity (Percival and Currin-Percival 2013; Koretsky and Steshich 2019; Weber et al. 2020). The concept of "social pathology" is often combined with the concept of social deviation, which will be discussed later in the work. Deviation in the sociological sense is most often treated as: behavior considered by society to differ in meaning from the average behavior of a given group, i.e., from the norm expected in each situation under given conditions (Ruch, Zimbardo 1971). Research on deviations from social norms on the Internet, which is the subject of interest in this study, is becoming more and more popular.

Analysis of the Concept of Cyberdeviation

The first step of the considerations is an etymological analysis of the concept of cyberdeviation to establish the relationship of individual parts of the word, as well as to find the meaning for each of the elements from which they were created. The concept itself is a derivative—a complex unit with a two-part structure. The word prefix "cyber" is derived from cybernetics (*Greek*: Kybernetes). The term was borrowed from Greek, where it meant proficiency in the art of steering. The original meaning of the concept—the art of governance—was developed in a philosophical essay—*Essai sur la philosophie des sciences, or exposition analytique d'une classification naturelle de toutes les connaissances humaines* (Ampere 1856). The creator of cybernetics as an independent scientific discipline is the mathematician Norbert Wiener in his work *Cybernetics or Control and Communication in the Animal and Machine* (1948), where the title itself can be treated as the first definition of the concept. Cybernetics is applicable to systems where the flow of information forms a closed circle. Hence, in broad terms, it means the study of control systems implemented in living nature, technology, and society, and the transfer of information within these systems. The prefix "cyber" imposes meaning associations with information and its flow, and the management of this process. Its present universal significance was acquired thanks to the development of science-fiction literature and the further increase in the importance of the Internet. In the sociolect of the Internet, the prefix "cyber" is used when a given phenomenon is observed in a virtual, paraphysical space created by new technologies (Siwicki 2013). For the first time in relation to virtual space, the prefix "cyber" was used by William Gibson, who wrote about cyberspace in *Burning Chrome* (1982) and later introduced the term "*consensual haullucination*" (1984) in *Neuromencer*. Cyberspace is understood as interconnected infrastructure networks of information technologies, including the Internet, telecommunications networks, computer systems, and systems that manage production and control processes, by means of which users from all over the world can communicate and cooperate with each other (Force 2017).

The word formation basis of the analyzed concept is deviation (Latin *devio*—I go out of the way). The term originates from Emile Durkheim's theory of anomie. The development of subsequent research perspectives on the issue of deviation took place in the 20th century. The following forms were then established and developed: functional and structural theory, theory of social control, and social reaction. The first, primary in relation to the others, is the functional-structural orientation. It is related to the process of growing up, reference groups, and society itself, which, according to theoreticians, creates behaviors inconsistent with accepted norms. Researchers look for causes of breaking norms in the structure and functions of society. The key to understanding the essence of deviation in this approach is to explain the ambiguous concept of anomie, which can be understood both as the objective state of society, the mental position of an individual, or as behavioral reactions to the dysfunction of society. In broadly descriptive terms, this will mean the lack of a state of norms that would be appropriate for the entire socio–cultural structure (Durkheim [1897] 1967). On the other hand, the narrow meaning indicates that an anomy is a disturbance in the regulations between individual functions of the elements of the entire social system, which means that social solidarity is not created because of the division of labor (Durkheim 1911/1960). According to Robert King Merton, anomie means the breakdown of a specific cultural structure that occurs where there is a discrepancy between culturally defined goals and the means of achieving them that are available in each social group (1968/2002).

The second trend—social control—assumes that deviant behavior is a consequence of its lacking. Theorists (e.g., Hirschi 1969; Zamecka 1987) point out that deviation is made possible by a dysfunctional society that is unable to prevent deviation from arising. The weakening of the social power over an individual contributes to the rise and development of the individual. The theory of control emphasizes the importance of external and internal forces, keeping the individual within a state of conformity to the norms. The weakness or breakdown of control mechanisms increases the possibility that the individual will become deviant (Welcz 1985). The first and central assumption of the theory of social control is the claim that man is an immoral being. The second assumption is the belief that conformism, and not deviation, should be explained. The third common point of any theory of social control is the belief that there are no forces that motivate people to deviate, because these tendencies are natural. Theorists also assume that within each community there is only one unified system of values and one system of behavioral norms regulating the implementation of these values (Siemaszko 1993). Therefore, social control protects social cohesion, order, and the normative system adopted in the community.

The third leading trend explicitly recognizes that there are unambiguous regulations that define deviant behavior. The theory of social stigma is related to the social reaction to behavior considered to be deviant. It is one of the most important perspectives included in the interactionist trend. The theory of social stigma is sometimes called labeling theory or stigma theory. The theoretical assumptions of this trend were formulated by Edwin Lemert, who considered social and cultural forces to be the main source of deviation. According to him, the deviant behavior of an individual and his status as a deviant matures within a social and cultural organization that society describes as pathological. In this case, the individual cannot categorize certain activities as appropriate or not. Lemert distinguishes two types of deviation: primary (behavior that violates the norm randomly and has no significant impact on the identity of the individual) and secondary (behavior that significantly violates the norm, and the deviant's etiquette becomes the basis of the individual's identity) (Lemert 1951). In the case of secondary deviation, we observe stigma, which is a strong negative view that significantly changes the way a person perceives himself. Such a stigma becomes a feature that places an individual within a specific framework of behaviors assigned to him in a permanent, unchanging manner (Goffman 1963/2009). In Lemert's concept, an individual passively receives stimuli from the environment and has no possibility of defense against deviant labels. These thoughts were further developed by Howard Becker, who based his considerations on social reaction as the cause of deviation. In his opinion, the essence of deviant behavior consists in the fact that certain social groups create deviation by establishing rules (norms) whose violation is a sign of deviation. The standards set apply to all members of the community, and those who do not adapt become outsiders (1963). From the perspective of Howard Becker, deviation is not a qualitative feature of an act of behavior, but rather a consequence of others behavior towards the perpetrator of norms and sanctions. Such an interpretation changes the focus, and deviation is no longer an action, but a consequence of other people applying rules and sanctions to the deviant. The deviant in this case is the unit to which the label will be assigned. The deviation behavior will be marked as such by people. Therefore, the reaction of society to the observed behavior is crucial.

The above review of definitions shows the diverse scope and content of the concept of deviation. The criterion for identifying a phenomenon and behavior as deviant is the generally understood norm, which is understood as a rule or regulation (Ossowska 1966). The norm in a broad sense is social and legal; hence, the concept of deviation is of interest to at least two disciplines of science: criminology and sociology. Criminology studies behavior that explicitly violates the criminal law. Therefore, criminologists will be interested in methods that determine the level of crime, trends within categories of crime, and strategies to combat it. Sociologists, on the other hand, use the research of criminologists to study deviations from the norm in a broader sense. The sociology of deviation also seeks to determine why a given behavior violates the norm, i.e., the basic predicate of social life. From a sociological perspective, the concept of deviation will refer to individual behavior and group activities. Deviation researchers pay attention to social power, and when examining deviations, one should bear in mind what standards are being discussed (Giddens 2001/2004). It should be noted that the standards may differ from each other due to the cultural background. Understanding deviation as a violation or deviation from the norms in force in each group or society usually coexists with assigning an objective character to both these norms and deviations. Apart from the ontological status of the subject of research, two states of social organization can be distinguished in everyday social life: the state of normality and the state of abnormality. Thus, to simplify, deviation will mean the violation of a certain norm, which is associated with the emergence of a state of abnormality.

In the axiological sense, when the term "norm" is used in relation to the Internet, it is necessary to decide whether it is possible to indicate any norms prevailing in cyberspace. The concept of "netiquette," that is, a set of rules in a virtual community, may be helpful in trying to define such norms. The internet ethics code arises spontaneously and is created by internet users for others. Netiquette is heterogeneous. Hence, in the sociolect of the Internet, netiquette is point to, which differ from each other due to:

content, form, level of detail, recipients, or the range of impact of solutions. Despite the differences, it should be emphasized that the normative and regulatory core refers to the most generalized principles of social co-existence and remains constant for each netiquette. The first netiquette is a document by Arlande H. Rinaldi of Florida Atlantic University—*The Web. User guidelines and rules of etiquette* (Pręgowski 2012). Since the publication of the Rinaldi label, hundreds of documents have been written, known as netiquette. It is impossible to reach a consensus for all internet users as to the rules prevailing in cyberspace, but it is necessary to identify the "point of agreement," i.e. actions taken in the virtual space, which in quantitative terms are not accepted by most of the virtual community.

Understanding the deviation or spread of behavior that violates the norms in each community, based on theoretical considerations in relation to cyberspace, implies the need to ask whether such a community also exists on the Internet? The dichotomous division between *Gesselschaft-Gemeinschaft* created by Ferdinand Toennies (1912) is presented as classic for community research. This typology concerns both the historical dimension of societies and various types of bond within a society. The classical arrangements became obsolete when cyberspace began to develop intensively. The dynamics of development forced the necessity to conceptualize the definition of a virtual community. The forerunner of research in this field is Howard Rheingold, who defined the virtual community as a group of people who may or may not meet face-to-face and who exchange words and ideas via the keyboard and the web (1993). However, he did not distinguish between activities in the virtual and real world. Barry Wellman and Milena Gulia (1999) took up reflection on the virtual community a few years later. Among the important questions that they formulated in their work, it seems to be important about relationships established and then observed online? Among the predicates that allow for the development of a virtual community, they distinguished: a sense of intimacy and uniqueness, voluntary commitment, a desire for companionship, interests, a multitude of relationships that can be maintained for a long period of time, a sense of reciprocity of relationships. Mark Smith distinguished five features of the virtual community that distinguish it from an actual community in the real world, namely: nonspatiality, asynchronicity, acaterality, astigmaticity, and anonymity (1992). Two extreme positions are confronted in the discussion on virtual communities. One posits that the virtual community is a new separate community of people with common goals, interests, or shared knowledge (Szpunar 2004; Pańkowska 2007). The second characterizes a virtual community as a "pseudo-community". In this case, there is no community in the classical sense. However, even a conservative approach emphasizing a community of interests and lifestyles gives a subjective feeling that an individual belongs to a separate community. Dominant in quantitative terms is the modernist/dynamic attitude, indicating that a new type of community has emerged in cyberspace, completely dependent on technical infrastructure. Interestingly, people who would never meet in the real-world bond in cyberspace, and this connection is sometimes stronger than in primary reference groups and with established systems of norms.

On a normative basis, activities that violate the norms in an online community should be considered a cybercrime, which is a concept that intersects with the term cyberdeviation. The term "cybercrime" was spread by the so-called Lyon Group, operating within the G8, tasked with carrying out analytical work on new forms of crime (Adamski 2000).

Due to numerous terminological doubts, cybercrime is still not specified in the criminal codes of many countries. It is impossible to define unambiguously all the qualities of the term because this type of crime is constantly evolving, which is a consequence of the development of technology. Therefore, it is easier to indicate important features, which include: immaterial nature, lack of defined geographical boundaries, decentralized actions of perpetrators, lack of one control and supervision center over its entirety, fluid and plastic nature, universal availability, processing, and computing in real time (Nowak 2010). In the 1960s, when there was a need to specify the factors that would define this problem, terms such as computer crime or computer-related crimes were used more often. In the first phase, these terms were understood in two ways. On the one hand, the computer was the object or environment of the attack. In other terms, the term Internet crime was used to describe crimes committed by people with advanced IT skills (Siwicki 2013). The term computer crimes gained importance in the 1970s and 1980s, and Crime by Computer (Parker 1976) is considered the most famous work created at that time.

In the early years of the Internet, some authors also argued that cybercrime should be considered a subcategory of computer crime, which they consider any type of crime committed via the Internet or other networks. Computers and computer networks, they argued, could be used to commit crimes in several ways (Shinder 2002). However, this position has become obsolete and remains a minority one. It is characteristic of the first generation of cybercrime development, which David Wall defines as the use of computers for criminal activities. In the second generation, information networks are used to carry out acts of cybercrime. The third assumes the advanced use of technological possibilities of information and communication networks (Wall 2007). The very concept of "computer crime" is very imprecise and should be treated more as a slogan than as a definition of a specific type of criminal activity (Jakubski 1996). Due to the development of modern technologies, computer crime has become too general a category. The omnipresence of modern technologies in every area of society's life means that defining the phenomenon only through the computer as a tool has simply become nontransparent, because the relationship between this form of crime and the Information and Communication Technology sector has become more and more visible. Therefore, institutions such as the Council of Europe, the United Nations, and individual researchers regard cybercrime as a separate category. In the *Council of Europe Convention* of 2001—*Council of Europe Convention* on Cybercrime, there are provisions ordering the prosecution of crimes against the confidentiality, integrity, and availability of data and computer systems (Council of Europe 2001). Furthermore, the ratifying countries agreed to adapt their legislation. It has become obligatory to introduce solutions that will be recognized as a crime action that interfere with the data stored on the computer, resulting in the loss of intellectual property. Furthermore, by introducing laws, states created regulations that would prevent the dissemination of pornography involving minors. Its provisions were supplemented by the *Additional Protocol* (Council of Europe 2003), which contained provisions obliging the countries of the parties to introduce provisions prohibiting the spread of racial hatred and xenophobic content in cyberspace (Białoskórski 2011).

From the classification and ordering perspective, the definition developed during the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders seems to be more useful. At that time, a division was proposed: cybercrime in the narrow sense and cybercrime in the broad sense. This division was created on the basis of previous experiences. Back in the 1990s, the Federal Bureau of Investigation (FBI) defined cybercrime as any activity in which a computer or computer network is a tool, object, or environment of criminal activity (Siwicki 2013). The issue of cybercrime was also discussed by the institutions of the European Union. The response to threats arising in cyberspace is to be a joint communication of the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions, which is referred to as the Cyber Security Strategy of the European Union: open, safe, and protected cyberspace. In a document issued on February 7, 2013, we read: the Community's economy has been repeatedly the victim of cybercrimes committed both against the private sector and individuals. In these communications, the term cybercrime refers to a wide range of different types of criminal activity for which computers and information systems constitute the primary criminal tool or are the primary target of the criminal activity. Cybercrime includes traditional crimes (for example, fraud, forgery, and identity theft), content-related crimes (online distribution of child pornography or incitement to racial hatred) and crimes specific to computers and information systems (attacks on information systems, including attacks involving blocking services / systems, and malware) (see: European Commission 2013). Therefore, the following have been distinguished: common cybercrimes, cybercrimes related to the content of information, and cybercrimes involving the use of electronic communications networks to infringe goods protected by criminal law. These breaches are particularly dangerous, as they can target critical infrastructures, with dramatic consequences for the entire community.

Cybercrime is one of the fastest growing forms of crime in the world. Due to the closeness of the term and the fact that legal norms are violated, the concept of "cyber-deviation" is compared with cybercrime. Both terms can be juxtaposed due to the prefix "cyber," indicating the space where these acts are performed, and their word formation basis can be compared. The concept of deviation is much broader and means a procedure that is not necessarily a violation of legal norms. However, much deviant behavior is not legally sanctioned (Giddens 2001/2004). In legal terms, deviation constitutes a breach of (or deviation from) the applicable legal norm. Thus, the legal definition states that any deviation from the law, an action inconsistent with the legal code, will be a deviation. The concept of deviation in social terms is more difficult to define because such behavior does not have to violate legal norms, but it violates social norms, i.e., accepted and acceptable rules of behavior that reflect the values present in each culture (Sztompka 2002). It is worth remembering that both legal and social norms change in time and space, which makes it difficult to define them in general—universal terms, especially in isolation from the features of place and time and from the normative criteria of a given community.

* * *

The content presented so far allows us to present the content of the term "cyberdeviation". The analysis carried out shows that deviation is a natural stage in the development of societies and social phenomena. Understanding deviation as a violation of the norms prevailing within a given community forces us to reflect on whether the Internet can indicate generalized norms of social co-existence and identify a new type of community—the virtual community. Considering the above problem on several levels, it is necessary to indicate the heterogeneous nature of the existing standards, broken down by their content, form and level of detail. In addition, the area of interpersonal relations that is shaped by the use of the Internet is not of a homogeneous nature. Members of individual communities are grouped according to the community of interests and views, building mutual relations, and performing transactions. Platforms where processes involving the above became possible in the initial phase of Internet development after 1995 include various kinds of forums and closed groups, for example, in User Network. The creation of Facebook in 2004, which as of September 2021 is actively used by 2.89 billion people throughout the world (Statista 2021), as well as other social networks, allows these communities to constantly develop and strengthen their mutual bonds. An important attribute of a community created in cyberspace is its virtual character, geographically unlimited. However, the limitation is a dependence on the technical infrastructure. The inclusion criteria are the result of a consensus within the community. These criteria may just be a formal barrier related to registration (e.g., Facebook, Twitter, Instagram), but also a contractual one related to certification for a new community member and meeting additional criteria related to knowledge and interests (e.g., the Preppers community). Within each community, separate norms of behavior are shaped, which are codified—for instance, in the form of regulations—or universal, where on axiological grounds, for example, the promotion of pedophilia or political extremism is unacceptable. Violation of the standards will, in extreme cases, result in exclusion from the virtual community.

Classification of Deviant Behavior in the Virtual Community

In an attempt at classification, the present study uses the semantic proximity of the term cybercrime. Cybercrime, broadly understood, refers to a wide range of criminal activities for which computers and information systems are the primary tool or the target of criminal activity. Cybercrime includes traditional crimes (fraud, counterfeiting), content crimes (distribution of pornographic content), as well as crimes typical of computers and information systems (attacks on information systems) (see European Commission 2013; Viano 2017; Chandra & Snowe 2020). Cybercrimes are a separate category from computer crime, which should be associated with online behavior consisting of direct interference with both the data contained in the media and the computer itself where it is stored (Simmons 2016). Cybercrime is a broader category than computer crime because it can be committed using other tools. The act and purpose of the action are also different. On the other hand, according to Michal Sowa, Internet crimes are those in which network services (opportunities offered via the Internet) have enabled or at least facilitated the perpetrator to carry out the intended criminal act or its individual stages. In other words, we talk about online crime when, without the use of the Internet, it would not be possible, or it would be much more difficult, to commit a specific act (2002). The literature offers several suggestions for typologizing cybercrimes. In one of the first documents relating to cybercrime—the *Council of Europe Convention*—a distinction was made between computer counterfeiting, computer fraud, crime related to the nature of information contained in an IT system, and offenses related to infringement of copyright and related rights. However, as indicated, these divisions are anachronistic and are not applicable today in the face of technological progress.

Another more elaborate idea of classifying cybercrimes, one that generally covers the issues, suggests that individual actions should be classified. Then the classification is made in relation to the articles of the Penal Code. In the first place, the following cybercrimes can be mentioned: breach of confidentiality, integrity and availability of data, or illegal access to systems through hacking, wiretapping, fraud, espionage, sabotage, as well as all crimes against information protection, all formalized in Poland in the Penal Code. These crimes are defined and prosecuted mainly in articles 267–269 of the Penal Code, that is, the so-called "hacking articles." The second type in this classification is cybercrimes, where the computer becomes a criminal tool. In this case, the diffusion of "traditional" crimes into cyberspace is observed and empirically confirmed. On the other hand, the ICT device connected to the network becomes a tool in the hands of the perpetrator. Committing this type of crime is facilitated by technical capability. Examples include online auction fraud, forgery, illegal invoice manipulation, or the use of credit cards. The third type of crime is content-related cybercrime. These are the so-called content offenses, i.e., those related to the content of the message. They include, but are not limited to, child pornography, offering to commit a crime, or disseminating false information in virtual space, using a computer or other electronic tool. Subsequently, messages containing xenophobic content or incitement to racial hatred are mentioned as more serious acts. The last subcategory of content-related cybercrimes involves the most serious transgressions such as sending criminal threats, cyberstalking, and grooming of minors. They violate not only legal norms, but most of all social norms. The last category consists of all other cybercrimes that have not been previously categorized. The following are examples of this: acts related to the infringement of copyright and other related rights. They are a type of crime that can only be committed in the virtual space, but are also prosecuted by law, as well as condemned by the entire Internet communities (Kosiński 2015; Jagiełło 2018).

Although the above typology seems to be complementary in terms of methodology and arrangement of the issues, in practical terms, such an extensive one is not applicable. When applying quantitative categories, it should be noted that most studies indicate a dichotomous division of cybercrime types. This is also done by Interpol (*International Criminal Police Organization*). According to the Interpol classification, cybercrime can be considered in two aspects:

- vertical: crimes specific to cyberspace, such as hacking or computer sabotage;
- horizontal: crimes committed outside cyberspace but by using computer technology (e.g., computer fraud, counterfeiting money, money laundering, etc.) (Bałazy 2018).

Another dual-aspect approach relates to computer crimes sine qua non. According to H. Cornwall, there are four groups of such offenses. First, it is necessary to list those that are impossible outside the computing environment, i.e., manipulations with data sets or information hacking. The second group of crimes are those that are facilitated by computers. This group includes, for example, fraud or information theft. The third group is those committed with the passive participation of computers (e.g., fraud or causing damage to economic and private interests). The last type of crime in this approach is crimes committed by professionals using computers. Here, an example may be *phishing* or *sniffing* (Nowak 2010).

The above classifications of cybercrimes constitute an important source of knowledge and are a starting point for further work that establishes individual behaviors as deviant. Due to the wide spectrum of the observed phenomena, it is necessary for methodological purposes to indicate the criteria for inclusion in each group. A constant variable that remains unchanged for each type of cybercrime will be the instrument of the act, that is, the computer or other device connected to the network. On the other hand, the type of act committed by the perpetrator, as well as the purpose of his action, will change.

At the lowest level of the proposed continuum, there will be acts that are not prosecuted in any way on a normative basis but that violate the norms adopted by Internet users—that is, the norms of a given community. In other words, low-intensity acts tend to focus primarily on social, rather than legal, norms. Therefore, these will be behaviors that originate in the category of computer crimes and can only occur in cyberspace. An example would be *SQL injection*. Other low intensity attacks also include those related to braking system algorithms[2] (Stokłosa et al. 2001). All activities in which the cybercriminal uses cryptography should be classified within this category. The main motivation for acts of low intensity in the social dimension is the particular interest of the deviant. He or she does not receive financial benefits from it (or they are minimal). The act itself does not cause significant physical changes and is related to the errors of the person responsible for the security of the system.

One level higher in the adopted classification is medium intensity cybercrime. This broadest category includes all acts penalized on a legal basis. The category of these acts will be opened by all crimes against confidentiality, integrity, and availability of data. The so-called hacking articles define the actions that are characteristic of this group of people who operate in cyberspace. Crimes of medium intensity also include all crimes in which the legally protected right to information protection has been violated. The provision contained in Article 267 of the Penal Code, which reads as follows, is exhaustive for these acts:

> §1. Whoever without authorization gains access to information not intended for him, by opening a closed letter, connecting to the telecommunications network, or breaking or bypassing electronic, magnetic, IT or other special protection thereof, shall be subject to a fine, the penalty of restriction of liberty, or the penalty of deprivation of liberty for up to two years.
> §2. The same punishment shall be imposed on anyone who, without authorization, gains access to all or part of the IT system.
> §3. The same punishment shall be imposed on anyone who, to obtain information to which he is not entitled, sets up or uses a listening device, visual device, or other device or software (The Act of June 6, 1997. The Penal Code).

The behaviors described in the first paragraph concern hacking *sensu stricto*. The following paragraphs refer to the phenomenon of hacking in a broad sense. Medium-intensity cybercrimes are criminal activities carried out in virtual space, as they are all standards that one can be convicted of breaking. To perform an act of medium intensity, certain skills related to the fluent operation of computer systems are necessary. It is not

[2] The basic algorithms include: Data Encryption Standard, Commercial Data Masking Facility, International Data Encryption Algorithm.

possible for someone who does not know the basics regarding the security of information systems and the methodology of their operation to commit such an act.

However, in the social world, including cyberspace, there is another group of acts. In order of classification, these will be acts of high intensity. They are a group of acts that are also codified and violate legal norms but go beyond the so-called hacking code. Moral relativism means that not all norms *expressis verbis* contained in hacking paragraphs are unambiguously assessed by the entire society. Sometimes they are even accepted because the system of norms adopted in the society allows them to be made. However, the group of high-intensity cybercrimes is an act that is legally penalized outside hacking clauses and is also not accepted in the entire community—in other words, it violates social norms. They constitute a serious breach of the norms of behavior in the virtual community, and it is most often Internet users who help prosecute their perpetrators. This is related to the moral condemnation of acts involving extreme deviation. An example of such behavior is the distribution of child pornography on the Internet, child grooming, or online stalking. Of course, it is inaccurate to say that they are condemned by the entire community, but they are condemned by the vast majority. Crimes related to the use of ICT networks and systems, as well as new technologies and crimes committed with the use of computers and ICT networks, constitute the final group of acts referred to as cybercrime.

Discussion and a Starting Point for Further Research

The article attempts to conceptualize the definition of social cyberdeviation, based on the most popular and well-known research trends. Widely understood as a violation of norms by an individual or group of people in cyberspace, it is an analytical category that requires further explication based on social sciences, to which the above article is aimed. “Cyberdeviation” will be used as a term to name and analyze a certain segment of social reality. The etymological core, as well as the semantic proximity to the term cybercrime, make the term a natural reference to negative social phenomena. Cybercriminals and cybercriminal networks are becoming more sophisticated; profit-oriented activities generate a great deal of financial gain and are associated with relatively low risk. All this means that cybercrime will continue to grow. Although in Poland this problem is statistically invisible (Krakowiak 2019), the global trend shows that it will continue to develop.

Deviation as a research category is useful in determining behaviors and phenomena in social life, such as pathology and disorganization. Thanks to Florian Znaniecki, the concept was extended without becoming evaluative (1934/2001). The definition of its content and the regulation of its meaning in the above study is to serve as a starting point for further research. Research on deviance distinguishes and analyzes various categories of behavior and their perpetrators, as well as the state of social perception about these acts. The classic interpretative approach focuses on explaining the reasons why an individual’s behavior is considered to violate the norms. In research on cyberdeviation referring to classical theories, one should take into account the different rules of functioning in the virtual space, basic ontological variables, i.e. time and space. They force the need to redefine, or rather adapt, theories known from physical reality to virtual space. Cyberspace creates, and in some cases neutralizes, variables that are significant, sometimes even constitutive, for individual orientations. For example, the Internet creates a sense of anonymity among its users, which is additionally reinforced by the lack of physical space for interpersonal contacts. As a result, the form, and degree of activity are not determined by the social context. In such circumstances, it is difficult to obtain social control, and the possibility of concealing one's true identity gives psychological comfort and a sense of impunity. Therefore, the study of the etiology of individual phenomena must take into account the factors that naturally create and develop cyberspace.

The second stream of empirical research on the phenomenon of cyber-deviation is its recognition in society and a sense of threat. The dominant research in this case will be quantitative techniques. First, the researcher will identify behaviors that violate the norms and then examine their impact on society. Second, it will be interesting to cognitively compare the level of recognition of individual acts in the category of cybercrime, and the knowledge and awareness of the public about them. Despite the rapid development of the Internet as a medium, the public's awareness of the threats facing everyone in cyberspace is still insufficient and highly unsatisfactory. Violation of the norms of social co-existence in cyberspace, although it is contested within the community, may cause misunderstanding within the society.

The last element to be examined when characterizing the Internet as a source of deviation is the paraphysical space in which users move. The resulting cyberspace makes it possible to develop new forms, activities that are not observed in physical reality. The Darknet—a network that is hidden and maximally anonymous—plays a special role in generating deviation. Access to it is possible only with the use of appropriate specialized browsers. The Darknet has developed forms of activity, such as classic online stores, with an assortment that goes beyond the standard offered to ordinary users. The so-called Darkmarkets, the most famous of which is the Silk Road founded by Rosa Ulbricht, offer easy access to a range of services and products. There, it is possible to "order" a murder or a beating anonymously without ever meeting the perpetrator, to purchase prohibited substances or content that violates the law (Mazur 2016; Ormsby 2018/2019). The aspect of anonymity seems to strengthen the feeling of impunity, and, from a psychological point of view, it tempts and facilitates the violation of the norms of social co-existence.

Activities that are worth investigating in sociology have been identified above. We will not see them outside the window on the street. Although research in the area of deviation is still conducted and repeated in subsequent studies (see Anderson 2017; Gibbs 2017; Deflem & Triplett 2018; Goode 2019), these efforts are directed only at the real world. The virtual space for which the research field was indicated in the presented study is ignored. Empirical research should be carried out using classical methods adapted to the new space, with an established position in social sciences.

Conclusions

The aim of the work has been achieved. The defined framework of the analysis allowed for the reconstruction of the concept of cyberdeviation, which led to the article. The author suggests this term to be understood broadly as: violation of norms by an individual or a group of people in cyberspace. The proposed classification indicates the existence of cyberdeviation with: (1) a low degree of intensity, which are not prosecuted in any way on the normative basis but violate the norms adopted among Internet users; (2) medium intensity, that is, behavior that is outright breaking the law; (3) a high degree of intensity, that is, behavior that not only breaks the law, but is also morally and ethically reprehensible enough to exclude the perpetrator from the social space. An important element that should be taken into account when conducting research is the criminal law of a given country, which, despite the global nature of the Internet, is a determinant of legal norms. In the case of the presented article, the case of Poland was analyzed as the author's country of origin. Therefore, the scope of legal norms outlined in the work is not universal, and such norms should always be considered in empirical work for the analyzed case. The issue of social cyberdeviation should be the subject of research both in the area of one discipline and in an interdisciplinary approach. An exclusively sociological perspective allows empiricists to develop classical trends in empirical-analytical research. Classic methods and techniques of measurement, well-established in the practice of social sciences, may be used in the research. Due to the fact that research is conducted in cyberspace, due to the different reality of the Internet world, it is required to modify and adapt it to technical conditions. The interdisciplinary approach, which is the basis of the above study, allows to refer to the achievements of psychology and law, broadening the perspective of conducted research.

References

Adamski, A. 2000. *Prawo karne komputerowe*. Warszawa: CH Beck.

Ahmadi, S.M., Branch, N. 2011. Family and its Role in the Prevention of Social Pathologies, *Australian Journal of Basic and Applied Sciences 5*(10): 1324–1329.

Akdeniz, Y. 2016. *Internet Child Pornography and the Law: National and International Responses*. London: Routledge.

Ampere, A.M. 1856. *Essai sur la philosophie des sciences, ou Exposition analytique d'une classification naturelle de toutes les connaissances humaines*. Paris: Mallet-Bachelier.

Anderson, L. 2017. *Deviance: Social Constructions and Blurred Boundaries*. Berkeley: University of California Press.

Bałazy, A. 2018. *Cyberprzestępstwa — na co jesteśmy narażeni?* [online:] Available at: https://www.s-net.pl/blog/2018/05/09/cyberprzestepstwa-jestesmy-narazeni/ (Accessed 30 October 2020).

Becker, H. 1963. *Outsiders, Studies in the Sociology of Deviance*. Glencoe: The Free Press.

Białoskórski, R. 2011. *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku: Zarys problematyki*. Warszawa: Wydawnictwo Wyższej Szkoły Cła i Logistyki.

Button, M.E., & Marsh, I. (Eds.). 2019. *Suicide and Social Justice: New Perspectives on the Politics of Suicide and Suicide Prevention*. London: Routledge.

Castells, M. 2001. *The Information Age* (Vol. 98). Oxford: Blackwell Publishers.

Castells, M. 2004. *The Network Society A Cross-cultural Perspective*. Cheltenham: Edward Elgar.

Chandra, A., & Snowe, M.J. 2020. A taxonomy of cybercrime: Theory and design, *International Journal of Accounting Information Systems 38*: 100467.

Council of Europe. 2001. *Convention on Cybercrime. ETS NO. 185, Council of Europe, Explanatory Report to the Convention of Cybercime*. 23.XI.2001, ETS-No. 185. Budapest.

Council of Europe. 2003. *Additional protocol to the convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems: Strasbourg, 28.1.2003*. Council of Europe publ.

Cover, R. 2020. Subjective connectivity: rethinking loneliness, isolation and belonging in discourses of minority youth suicide, *Social Epistemology 34*(6): 566–576.

Cygielska, K. 1976. *Przegląd teorii*, in: Adam Podgórecki (eds.), *Zagadnienia patologii społecznej*. Warszawa: Państwowe Wydawnictwo Naukowe, pp. 83–119.

De Souza, L.G.D.C. 2017. Social pathologies, false developments and the heteronomy of the social: Social theory and the negative side of recognition, *Filozofija i društvo 28*(3): 435–543.

Deflem, M., & Triplett, R.A. 2018. Anomie, Strain, and Opportunity Structure: Robert K. Merton's Paradigm of Deviant Behavior, *The Handbook of the History and Philosophy of Criminology*, 140.

Durkheim, E. [1911] 1960. *De la division du trevall social.* Paris: Alcan.

Durkheim, E. [1997] 1967. *Le suicide: etude de sociologie.* Paris: Alcan.

European Commission. 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *adopted February*, *7*.

Force, J.T. 2017. Security and Privacy Controls for Information Systems and Organizations (No. NIST Special Publication (SP) 800-53 Rev. 5 (Draft)). National Institute of Standards and Technology.

Gerasimoski, S. 2021. The Social Pathology of "New Normality" Dyring the Covid-19 Pandemics, *НА ФАКУЛТЕТОТ ЗА БЕЗБЕДНОСТ* 19: 19–26.

Gibbs, J.P. 2017. The sociology of deviance and social control, in: M. Rosenberg and R.H. Turner, *Social Psychology*. London: Routledge, pp. 483–522.

Gibson, W. 1982. *Burning Chrome*. New York: HarperCollins Publ.

Gibson, W. 1984. *Neuromancer*. New York: Dell Books.

Giddens, A. 2004. *Socjologia* [*Sociology*], (A. Szulżyńska, Trans.). Warsaw: Wydawnictwo Naukowe PWN. (Orginal work published 2001).

Global Digital Report. 2022. Digital in 2022: Global Internet Use Accelerates. [online:] Available at: https://datareportal.com/reports/digital-2022-global-overview-report (Accessed 28 january 2023).

Goffman, E. 2009. *Stigma: Notes on the management of spoiled identity*. New York–London–Toronto: Simon and Schuster.

Goode, E. 2019. *Deviant Behavior*. London: Routledge.

Has, A., Kopański, Z., Rozbicka, A., & Kollar, R. 2020. Other social pathologies-violence and gambling addiction, *Journal of Public Health, Nursing and Medical Rescue* 2: 34–38.

Hirschi, T. 1969. *Causes of Delinquency*. Berkeley: University of California Press.

Hirvonen, O. 2018. On the ontology of social pathologies, *Studies in Social and Political Thought* 28: 9–14.

Hörnle, J. 2021. *Internet Jurisdiction Law and Practice*. Oxford: Oxford University Press.

Jacobsen, B., Nørup, I. 2020. Young people's mental health: Exploring the gap between expectation and experience, *Educational Research 62*(3): 249–265.

Jagiełło, D. 2018. Karnoprawne ramy odpowiedzialności za przestępstwa popełnione w cyberprzestrzeni, in: C. Banasiński, et al. (eds.), *Cyberbezpieczeństwo: zarys wykładu*. Warszawa: Wolters Kluwer, pp. 449–468.

Jakubski, K.J. 1996. Przestępczość komputerowa — zarys problematyki, *Prokuratura i Prawo* 12: 34–50.

Jemielniak, D., 2019. *Socjologia internetu*. Warszawa: Scholar.

Koretsky, D., Steshich, E.S. 2019. Suicides as an element of studying homicidal crime, *Russian Journal of Criminology 13*(2): 207–214.

Kosiński, J. 2015. *Paradygmaty cyberprzestępczości*. Warszawa: Difin SA.

Krakowiak, L. 2019. *Cybeprzestępstwa w Polsce są statystycznie niewidoczne*, [online:] Available at: https://www.computerworld.pl/news/Cyberprzestepstwa-w-Polsce-sa-statystycznie-niewidoczne,413041.html (Accessed 30 October 2020).

Laitinen, A., Särkelä, A. 2019. Four conceptions of social pathology *European Journal of Social Theory 22*(1): 80–102.

Lemert, E. 1951. *Social Pathology: a Systematic Approach to the Theory of Sociopathic Behavior*. New York: McGraw-Hill Book Company.

Liba, J. 2008. School in prevention of social-pathological phenomena in pupils from social from socially disadvantaged and educationally less inspiring environment, *School and Health* 21: 123–130.

Macharski, J., and Gizbert-Studnicki, T. 1975. O pojęciu dewiacji w socjologii, *Ruch Prawniczy, Ekonomiczny i Socjologiczny 37*(4): 231–245.

Mayntz, R., Holm, K., and Huber, P. 1985. *Wprowadzenie do metod socjologii empirycznej* [*Einfuhrung in die Methoden der empirischen Soziologie*] (Transl. W. Lipnik). Warszawa: Państwowe Wydawnictwo Naukowe. (Original work published 1969).

Mazur, M.K. 2016. *Polskojęzyczna społeczność przestępcza zorganizowana w sieci darknet*. Poznań: ICLAT.pl.

Merton, R. 2002. *Teoria socjologiczna i struktura społeczna* [*Social Theory and Social Structure*] (Transl. E. Morawska, J. Wertenstein-Zuławski). Warszawa: Wydawnictwo Naukowe PWN. (Orginal work published 1968).

Messas, G., Tamelini, M. 2018. The pragmatic value of notions of dialectics and essence in phenomenological psychiatry and psychopathology, *Thaumàzein Rivista di Filosofia* 6: 93–115.

Mider, D. 2013. Analiza pojęcia cyberterroryzmu. Próba uporządkowania chaosu, *Annales Universitatis Mariae Curie-Skłodowska, sectio K—Politologia 20*(2): 81–114.

Nomokonov, V.A. 2017. Causes of crime in contemporary Russia: the problem is getting worse, *Russian Journal of Criminology 11*(2): 247–257.

Nowak, M. 2010. Cybernetyczne przestępstwa — definicje i przepisy prawne, *Biuletyn EBIB* 4: 113.

Number of daily active Facebook users worldwide as of 2nd quarter 2021, https://www.statista.com/statistics/346167/facebook-global-dau/ (Accessed 6 September 2021).

Ossowska, M. 1966. *Podstawy nauki i moralności*. Warszawa: Państwowe Wydawnictwo Naukowe.

Ormsby, B. 2019. *Darknet* [*The Darkest Web*] (Trans. A.M. Nowak). Kraków: Znak. (Original work published 2018).

Ortega-Esquembre, C. 2020. Social pathologies and ideologies in light of Jürgen Habermas: a new interpretation of the thesis of colonization, *Humanities and Social Sciences Communications 7*(1): 1–9.

Pańkowska, M. 2007. Programy badań i rozwoju technologicznego jako środowisko powstania społeczności wirtualnych, in: H. Sroka and T. Porębska-Miąc (eds.), *Systemy Wspomagania Organizacji SWO 2007*. Katowice: Wydawnictwo Akademii Ekonomicznej.

Parker, D.B. 1976. *Crime by Computer*. New York: Scribner.

Pawłowski, M., Kułakowska, A., & Piątkowski, Z. 2019. Mobbing jako patologia zarządzania współczesnymi organizacjami, *Postępy Techniki Przetwórstwa Spożywczego* 2: 155–166.

Pawłowski, T. 1978. *Tworzenie pojęć i definiowanie w naukach humanistycznych*. Warszawa: Państwowe Wydawnictwo Naukowe.

Percival, G.L., Currin-Percival, M. 2013. Exploring the contextual determinants of individual attitudes toward immigrants and criminal activity and their spillover policy implications, *International Migration 51*(6): 1–23.

Podgórecki, A. 1969. *Patologia życia społecznego*. Warszawa: Państwowe Wydawnictwo Naukowe.

Pospiszyl, I. 2009. *Patologie społeczne*. Warszawa: Wydawnictwo Naukowe PWN.

Pręgowski, M.P. 2012. *Zarys aksjologii internetu: netykieta jako system norm i wartości sieci*. Toruń: Wydawnictwo Adam Marszałek.

Rheingold, H. 1993. *The Virtual Community: Homesteading on the Electronic Frontier* (Vol. 32). Reading, MA: Addison-Wesley.

Ruch, F.L., Zimbardo, P.G. 1971. *Psychology and Life*. Glenview, Ill.: Scott, Foresman and Company.

Rydlewski, G. 2021. *Rządzenie w epoce informacji, cyfryzacji i sztucznej inteligencji*. Warszawa: Dom Wydawniczy Elipsa.

Salakhova, V.B., Bulgakov, A.V., Sokolovskaya, I.E., Khammatova, R.S., & Mikhaylovsky, M.N. 2016. Substantive (Content-Related) Characteristics of Deviant Behavior as a Social and Psychological Phenomenon, *International Journal of Environmental and Science Education 11*(17): 10609–10622.

Savin, A. 2020. *EU Internet Law*. Cheltenham: Edward Elgar Publishing.

Shatyr, Y.A., Mulik, I.G., Ulesikova, I.V., Delaru, V.V., & Mulik, A.B. 2017. Systematization of the Factors of Formation of Social Deviations, *Logos et Praxis 16*(3): 136–144.

Shinder, D.L. 2002. The Scene of the Cybercrime—Computer Forensics Handbook Syngress Publishing.

Siemaszko, A. 1993. *Granice tolerancji: O teoriach zachowań dewiacyjnych*. Warszawa: Wydawnictwo Naukowe PWN.

Simmons, R. 2016. The failure of the Computer Fraud and Abuse Act: Time to take an administrative approach to regulating computer crime, *Geo. Wash. L. Rev. 84*: 1703.

Siwicki, M. 2013. *Cyberprzestępczość*. Warszawa: Wydawnictwo CH Beck.

Smith, M. 1992. Voices from the WELL: The logic of the virtual commons. Masther Thesis. University of California at Los Angeles. Los Angeles. TENET (Texas Education Network) (1996): Curriculum Infusion Guide. Documento electrónico.

Sowa, M. 2002. Odpowiedzialność karna sprawców przestępstw internetowych, *Prokuratura i Prawo* 4: 62–79.

Stokłosa, J., Bilski, T., & Pankowski, T. 2001. *Bezpieczeństwo danych w systemach informatycznych*. Poznań: Wydaw. Naukowe PWN.

Svantesson, D.J.B. 2016. *Private international law and the internet*. Alphen aan den Rijn: Kluwer Law International BV.

Szpunar, M. 2004. Społeczności wirtualne jako nowy typ społeczności — eksplikacja socjologiczna, *Studia socjologiczne 2*(173): 95–133.

Sztompka, P. 2002. *Socjologia: analiza społeczeństwa*. Kraków: Znak.

The Act of June 6, 1997, as amended changes. The Penal Code (Dz.U. 1997 nr 88 poz. 553).

Thompson, M.J. 2019. Hierarchy, social pathology and the failure of recognition theory, *European Journal of Social Theory 22*(1): 10–26.

Tönnies, F. 1912. *Gemeinschaft und gesellschaft: grundbegriffe der reinen Soziologie*. Berlin: Karl Curtius.

Viano, E.C. 2017. Cybercrime: Definition, typology, and criminalization, in: *Cybercrime, Organized Crime, and Societal Responses*. Cham: Springer, pp. 3–22.

Wall, D. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Weber, I., Gianolla, C., Sotero, L. 2020. Suicide and structural violence. Systematic review of a correlation marked by colonialism, *Sociedade e Estado* 35: 189–228.

Welcz, Z. 1985. Powstanie i rozwój teorii naznaczania społecznego, *Studia Socjologiczne 1*(96): 65–86.

Wellman, B., Gulia, M. 1999. Virtual communities as communities, *Communities in Cyberspace*, pp. 167–194.

Wiener, N. 1948. *Cybernetics or Control and Communication in the Animal and the Machine*. Cambridge, MA: MIT Press.

Wites, T. 2019. *Patologia społeczna. Perspektywa geograficzna*. Warszawa: Wydawnictwo Naukowe Scholar.

Zamecka, J. 1987. Kontrola społeczna i dewiacja społeczna jako zjawiska współzależne, *Studia Socjologiczne* 3: 297–307.

Znaniecki, F. [1934] 2001. *Ludzie teraźniejsi a cywilizacja przyszłości*, Warszawa: Wydawnictwo Naukowe PWN.

Biographical Note: Wojciech Mincewicz (Ph.D.), assistant professor at the Department of Political Sociology and Political Marketing, University of Warsaw. He is interested in the problems of cryptocurrencies and blockchain technology in political and social terms, sociology of internet, social deviation, political infobrokering, political participation. Manager and contractor of research projects financed by the National Science Centre, Poland and NGO's.

ORCID iD: 0000-0003-0460-9158

E-mail: w.mincewicz@uw.edu.pl