Artykuły
Zeszyty Naukowe KUL 65 (2022), nr 1 (257)
DOI: 10.31743/znkul.13610

Małgorzata Gruchoła*, Justyna Szulich-Kałuża**

Digital Competence in Cybercrime Behaviours: A Study Based on Eurobarometer Research

Introduction

As is evident from the Eurobarometer study carried out in 2017 on the order of the European Union, its citizens are fascinated by the new digital technologies. The majority of those tested (67%) positively appraised their influence on the quality of life.[1] However, technical skills and humanistic competence do not always go with a positive approach to technology. In 2019, 70% of EU citizens declared having technological skills as regards making use of digital appliances in everyday life, whereas regarding humanistic competence, the result was 52%.[2] In encouraging EU citizens to use digital technologies in everyday life, one should take particular note of the problems of cybercrime and cyber-safety. One of the potential forms of gaining knowledge about these, of forming attitudes and skills, is digital competence.

* Dr hab. Małgorzata Gruchoła, prof. KUL – Katedra Komunikacji Wizualnej i Nowych Mediów, Instytut Dziennikarstwa i Zarządzania, Wydział Nauk Społecznych, Katolicki Uniwersytet Lubelski Jana Pawła II, e-mail: malgorzata.gruchola@kul.pl, ORCID: 0000-0002-2367-0416.

** Dr hab. Justyna Szulich-Kałuża, prof. KUL – Katedra Komunikacji Wizualnej i Nowych Mediów, Instytut Dziennikarstwa i Zarządzania, Wydział Nauk Społecznych, Katolicki Uniwersytet Lubelski Jana Pawła II, e-mail: justyna.szulich-kaluza@kul.pl, ORCID: 0000-0002-6845-168X.

[1] European Union, *Attitudes Towards the Impact of Digitization and Automation on Daily Life*, Special Eurobarometer 460, Brussels 2017.

[2] European Union, *Attitudes Towards the Impact of Digitalization on Daily Lives*, Special Eurobarometer 503, Brussels 2020.

Methods

The aim of the article is a study of the scope of components (skills, knowledge and attitudes) of digital competence (technologic and humanistic) in cybercrime behaviours in a relational hold, based on the example of internet levels (technical, social and informative) as well as the confrontation of theoretical assumptions with the frequency with which they are experienced by EU citizens. We will use the definition of the internet taking into account its three levels,[3] which in our opinion may correspond with the three areas of competence. The internet is made up of the levels: technical – a widespread, dispersed network composed of networks linked to each other, demanding technical skills; social – a society which makes use of this network and develops it, demanding social competence, and informative – enclosing a collection of resources which are found in this network, conditioned by informative competence. We treat the area of social and informative competence together as humanistic competence, complementary to each other.

We accepted two hypotheses in the research project: 1) The catalogue formulation of digital competence (so-called traditional) focusing on social-demographic traits should be replaced by a relational formulation taking into account all the components of digital competence: knowledge, attitude and skills. 2) Citizens of the EU countries possess greater digital competences of a technological character than of a humanistic one (social and informative) and more often admit to falling prey to cybercrime behaviours of a technological kind than of a humanistic one. In order to solve the title problem and to verify the hypotheses we shall apply the following research methods: a quantitative and qualitative analysis of available data, the comparative method, the historical method and the analytical-synthetic method. Fourteen Eurobarometer reports will be analysed, among others: 5 Standard Eurobarometer and 9 Special Eurobarometer carried out in all EU countries in the years 2011–2020.[4]

Literature review

Cybercrime – establishing the definition

In the scientific and public discourse there are a few designations of cybercrime, precisely stating the essence of the phenomenon – a crime linked

[3] M. Gruchoła, *W pajęczynie globalnej sieci*, "Społeczeństwo i Rodzina" 2016, vol. 47, no. 2, pp. 94–116.

[4] Archives of reports: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/General/.

to network systems, a crime using advanced informative technologies.[5] It is a particular manifestation of cyber-violence and has as its aim the subjection of individuals or groups in defiance of their will by attacks not in keeping with the law, using informative systems of processing data, with the intention of steering someone in such a way as to achieve their own aims and benefits. The perpetrators of cybercrimes may be divided into three categories of groups: traditional organized activities in the offline environment, organized criminal groups, in the online environment and organized groups ideologically and politically motivated.[6]

The domain of cybercrime understood as every illegal action perpetrated with the help of systems or computer networks[7] may be considered in vertical and horizontal formulation. The first concerns crimes specific of the cyber-area beyond which they cannot be perpetrated e.g. hacking (botnets, zombies), crimeware (the infection of devices with malicious software, viruses, trojan horses) or spamming. In a horizontal formulation, crimes are found in which the utilization of computer instruments and informative techniques considerably simplified their execution e.g. online material which promotes racial hatred or religious extremism, the theft of identity, cyberlaundering.[8]

Cybercrime takes on different forms which may be all in all collected in several activities: the utilization of instruments and informative technologies to derange the privacy, safety and physical, psychic well-being of both the individual as well as of social groups, among others, by promoting race hatred and direct physical attacks. The instruments and informative technologies may serve in cybercrime as objects of crime (thefts, the destruction of equipment by infection with software viruses), the subjects of criminal behaviour (the circle of committing crime: attacks of the denial type of service, virus attacks, theft of data), instruments and conveyors of crimes (the publication of illegal contents).[9] A few characteristic attributes of cybercrime should be indicated which, on account of their dynamism of change, ought to be subject to empirical research: the change of activity of criminal action from online to offline; the appearance of new kinds of cybercrime in connection with technological

[5] S. Gordon, R. Ford, *On the Definition and Classification of Cybercrime*, "I Comput Virol" 2006, no. 20, pp. 13–20; M. Gruchoła, *Polityka Unii Europejskiej w zakresie cyberprzestępczości*, in: *Patologie w cyberświecie,* ed. S. Bębas, J. Plis, J. Bednarek, Wyższa Szkoła Handlowa, Radom 2012, p. 149.

[6] P. Grabosky, *Cybercrime. Keynotes in Criminology and Criminal Justice Series*, Oxford University Press, Oxford 2016.

[7] D.L. Shinder, E. Tilttel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, tłum. J. Dobrzański, K. Masłowski, Wydawnictwo Helion, Gliwice 2006.

[8] D.S. Wall, *Cybercrime, Media and Insecurity. The Shaping of Public Perceptions of Cybercrime,* "International Review of Law, Computers &Technology" 2008, vol. 22, nos. 1–2, pp. 45–63.

[9] D. Johnson, D. Post, *Law and Borders: The Rise of Law in Cyberspace*, "Stanford Law Review" 1996, vol. 48, no. 5, pp. 1367–1402.

progress; difficulties with the protection of electronic proofs, documenting criminal activity. For a full picture of the phenomenon, the humanistic character of cybercrime should be emphasised, which is expressed in the objectifying of the subject, the reduction of the subject to the position of an object, an object ready to use, in order to form it in a desired way.[10] Speaking of the humanistic dimension, we also take into account the dangers as regards the fundamental values of society, laws of man, democracy and law and order.

Digital competence – the traditional and the relational approach

In the literature on the subject and in the relevant recommendations of European institutions, the three-partite structure of competence is repeated: knowledge, skills and attitudes.[11] In EC recommendation of 22 May 2017 on the European Qualifications Framework for lifelong learning[12] competence is defined as a proven ability of applying knowledge, skill and individual, social, as well as methodological predispositions in work, learning and in professional and personal development.

The literature on the subject also reveals two main ways of defining the notion of digital competence: the catalogue formulation – called traditional way – and the relational formulation.[13] Digital competence in the "traditional" approach is described as an unchanging catalogue, an explicit (identical for each one) set of information resources and skills, which the users of the internet should be acquainted with. The only category used to distinguish between subtypes of competence under this approach are the demographic criteria of the users, without taking into account their individual predispositions, expectations or experience. The educational process is a transfer of a range of knowledge and skills elaborated by experts with the omission of attitudes.[14]

[10] M. Foucault, *Power/Knowledge. Selected Interviews and Other Writings 1972–1977*, Harvester Wheatsheaf, New York 1980.

[11] European Parliament and the Council, Recommendation of the European Parliament and of the Council of 18 December 2006 on Key Competences for Lifelong Learning (2006/962/EC), OJ L 394, 30.12.2006, pp. 10–18.

[12] Council of the European Union, Council Recommendation of 22 May 2017 on the European Qualifications Framework for Lifelong Learning and Repealing the Recommendation of the European Parliament and of the Council of 23 April 2008 on the Establishment of the European Qualifications Framework for Lifelong Learning (2017/C 189/03), OJ C 189, 15.06.2017, pp. 15–28.

[13] G. Siadak, *Kompetencje cyfrowe polskich uczniów i nauczycieli – kierunek zmian*, "Ogrody Nauk i Sztuk" 2016, vol. 6, pp. 368–381; M. Gruchoła, *Kompetencje medialne nauczycieli w dobie nowych technologii. Kilka refleksji socjologa i kulturoznawcy*, "Lubelski Rocznik Pedagogiczny" 2019, vol. 38, no. 3, pp. 95–116. DOI: 10.17951/lrp.2019.38.3.95-116.

[14] G. Siadak, *Kompetencje cyfrowe…*, p. 370.

In the second approach – the relational one – its authors notice that informative-communicative technologies do not constitute a separate area of the activity of individuals, but are an integral part of each of these: education, professional work and rest.[15] They highlight the need for adapting the level of digital competence to the individual needs of the internet users.[16] The basis of this model lies in an understanding of digital competence as functional competence (based on informative and informatory competences), applied in all areas of human activity with particular regard to the component of technical skills and knowledge, yet not omitting attitudes, either.[17] Digital competence in a relational approach is understood as "set of informative competences comprising skills of obtaining information, understanding it, as well as the estimation of its reliability and informative competences comprised of skills regarding the use of the computer and other electronic devices, use of the internet and of different types of appliances and programs, as well as the creation of digital subject matter".[18]

Sonia Livingstone proposes a definition with four components: "media literacy is the ability to access, analyse, evaluate and create messages across a variety of contexts".[19] Center for Media Literacy (CML) – an educational organization to promoting media literacy proposes a broader definition of media literacy education as "a framework for accessing, analysing, evaluating, creating and participating with media content".[20] The *DIGCOMP* report contains an analogical theoretic perspective: *A Framework for Developing and Understanding Digital Competence in Europe*, in which five areas of digital competence were singled out (1. information, 2. communication, 3. content creation, 4. security, 5. problem solving) as well as 21 depicted competences in all spheres of human activity. Although each area has its own specificity, there are a few overlapping common points and connections with other areas. For each of the above areas of competence a series of connected competences was identified, encompassing technical and operational skills.[21] As Michael Hoechsmann i Stuart Poyntz[22]

[15] J. Jasiewicz, M. Filiciak, A. Mierzecka et al., *Framework Directory of Digital Skills*, Centrum Cyfrowe Projekt Polska, Warszawa 2015, pp. 23–29.

[16] G. Siadak, *Kompetencje cyfrowe…*, p. 371.

[17] M. Gruchoła, J. Szulich-Kałuża, *Kompetencje medialne w komunikacji wizualnej*, Wydawnictwo KUL, Lublin 2020.

[18] *Społeczeństwo informacyjne w liczbach 2014*, ed. V. Szymanek, Ministerstwo Administracji i Cyfryzacji, Warszawa 2014, p. 17.

[19] S. Livingstone, *The Changing Nature and Uses of Media Literacy*, Media@LSE Electronic Working Papers 4, London School of Economics and Political Science, London 2003, p. 6.

[20] Center for Media Literacy, *About CML*, https://www.medialit.org/about-cml (accessed: 11.05.2022).

[21] A. Ferrari, *DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe*, Report EUR 26035 EN, Luxembourg 2013, pp. 38–41.

[22] M. Hoechsmann, S. Poyntz, *Media Literacies: A Critical Introduction*, Wiley-Blackwell, Malden 2012.

demonstrate, technical skills deprived of critical abilities cannot be considered as a digital competence *tout court*. In the definition of digital competences, as Małgorzata Bogunia-Borowska and Kamil Łuczaj[23] remark, their three components should be taken into account: technical skills, an ability to create independently media products and a capacity for critical reflection (that is, humanistic competence). Janice Richardson includes among them hermeneutic competences such as: critical thinking, a knowledge of human rights and basic values, the right to guard personal data, the right to protect psychic and physical health, the right of access to knowledge and information, the right to decide about digital identity, the knowledge of one's own culture.[24] These proposals delineate humanistic competences.

Summing the theoretical part of the article, a conclusion can be formulated regarding the necessity of a change of the approach from a catalogue one to a relational one, as well as the broadening of the scope of the notion of digital competence to cover the component of attitudes. In taking into account functional competences, the relational formulation comprises all the components: technical skills, knowledge and attitudes. It encompasses technological and humanistic competences. A catalogue formulation of digital competences in focusing on socio-demographic aims often does not take into consideration changes of awareness, of generation, culture and information, and thus omits humanistic competences. Digital competences in the article will be analysed in the relational formulation, including competences, knowledge and attitudes. We make use of the definition contained in the *DIGCOMP* report*: A Framework for Developing and Understanding Digital Competence in Europe*,[25] based on the above quoted Recommendations of the European Parliament and Council from the years 2006 and 2017.

Areas of digital competences: technological and humanistic

Among the ten criminal activities most frequently mentioned in 2019 by EU citizens, three directly refer to the humanistic section (the remaining to the technical one). These are: child pornography online: 96%, identity theft: 95% and online content which promotes racial hatred or religious extremism: 91%. They were estimated as the most harmful of cybercrime actions. However, the least harmful one was "The infection of devices with malicious software"

[23] M. Bogunia-Borowska, K. Łuczaj, *Kompetencje medialne młodzieży w wieku gimnazjalnym. Co i w jaki sposób badać?*, "Państwo i Społeczeństwo" 2017, vol. 17, no. 3, pp. 135–150.

[24] *European Schoolnet*, http://www.eun.org (accessed 15.02.2022).

[25] A. Ferrari, *DIGCOMP: A Framework…*, pp. 38–39.

(83%) – an example of cybercrime from the technical dimension.[26] Proper use of the internet demands adequate technological competence (technical gradation) as well as humanistic competence: knowledge (informative gradation) and attitudes (social gradation). The scope of analyses undertaken in the article is presented in table 1.

Table 1. The areas of analysis

Types of competences	Competence areas	Competences	Components of competences	Layers of the Internet	Criminal activity
Technological competence	5. Problem solving	5.1 Solving technical problems 5.2 Identifying needs and technological responses 5.3 Innovating and creatively using technology 5.4 Identifying digital competence gaps	1. Skills	Technical	The infection of devices with malicious software
Humanistic competences	1. Information	1.1 Browsing, searching, & filtering information 1.2 Evaluating Information 1.3 Storing and retrieving information	2. Knowledge	Informational	
	4. Safety	4.1 Protecting devices 4.2 Protecting data and digital identity 4.3 Protecting health 4.4 Protecting the environmen	3. Attitudes	Social	Online material which promotes racial hatred or religious extremism

Source: own study based on: A. Ferrari, *DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe*, Report EUR 26035 EN, Luxembourg 2013, p. 39; M. Gruchoła, *Kompetencje medialne nauczycieli w dobie nowych technologii. Kilka refleksji socjologa i kulturoznawcy*, "Lubelski Rocznik Pedagogiczny" 2019, vol. 38, no. 3, p. 98.

[26] European Union, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 499, Brussels 2019.

Results and discussion

Technological competences in the area of skills

Skills mean an ability to apply knowledge and the use of know-how in order to solve problems and carry out tasks. In the context of the European Qualifications Framework, skills are described as cognitive (involving the use of logical, intuitive and creative thinking) or practical (involving manual dexterity and the use of methods, materials, tools and instruments). Every online activity demands certain practical skills. Although since 2012 the number of EU citizens using the internet grows systematically (from 54% in 2012 to 76% in 2019); a growth of 22 percentage points – abbreviated: pp) a considerable difference is noticed on the national level. Respondents declaring daily use of the internet are mainly from countries of Western (NL: 96%, SE: 95%) and Northern Europe (DK: 92%), considerably less often, citizens of Rumania: 61%, Bulgaria: 64% and Poland: 65% (table 3). Seven out of ten examined persons (70% in 2019, 71% in 2017) think they use digital technologies properly in everyday life. At the same time, every fourth EU citizen (27% in 2019, 25% in 2017) admits not having such skills. In 2019, those who evaluated their skills the best were citizens of the Netherlands and Sweden: both 87%, Denmark: 84% and Germany: 81%; whereas a much lower level was reported by Greeks: 55%, Italians, Bulgarians and Rumanians: all 57% (table 3). The data proved a need for advocacy for the utilization of technologies by a decided majority of the EU citizens. One may presume that this is due to the active creation of digital resources, the introduction of innovations in technology and the solution of conceptual problems using digital tools.

In the years 2017–2019, in a decided majority of EU member states, together with a rise (of 10 pp), the number of people using the internet daily which demand technological skills noted not a rise, but a minimal fall of hardly 1 pp of technical skills in the EU citizens (from 71% to 70%), with a slight, that is, 1 pp rise in humanistic competences (from 51% to 52%) (table 2).

Technical skills of EU citizens are varied depending on member states. Falling tendencies were noted in nineteen EU countries (CY, LV both 1 pp, CZ, EE, LU, RO, FI, SE, UK all 2 pp, EL, NL, SK all 3 pp, DK, PL both 4 pp, ES: 5 pp, FR, LT both 6 pp, MT: 9%, IT: 11 pp), whereas eight countries reported increase (HU:15 pp, AT: 9 pp, DE: 8 pp, PT: 5 pp, BE, HR, SI all 4 pp, BG: 3 pp). Only in Ireland an equal level of technical skills was noted (80%). The greatest fall of declared skills was noted in Italy (12 pp), whereas their increase in Hungary

Table 2. Everyday internet use and the level of digital competences (data expressed as a percentage)

Year	Use of the Internet				Technological competences (digital skills)			Humanistic competences (information level)		
	Everyday Internet use	Often/ sometime	Never	No Internet access	Totally agree	Totally disagree	Don't know	Total well informed	Total not well informed	Don't know
2019	76	9	13	2	70	27	3	52	47	1
2017	66	13	19	2	71	25	4	51	46	3
2014	56	18	20	6	-	-	-	47	50	3
2012	54	16	22	5	-	-	-	38	59	3

Source: own study based on: European Commission, *Media Use in the European Union*, Standard Eurobarometer 78, Brussels 2012, p. 5; European Union, *Cyber Security*, Special Eurobarometer 390, Brussels 2012, p. 6; European Union, *Cyber Security*, Special Eurobarometer 423, Brussels 2015, p. 6; European Union, *Media Use in the European Union*, Standard Eurobarometer 86, Brussels 2016, p. 4; European Commission, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 464a, Brussels 2017, p. 6; European Commission, *Media Use in the European Union*, Standard Eurobarometer 88, Brussels 2017, p. 4; European Union, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 499, Brussels 2020, p. 9; European Union, *Attitudes Towards the Impact of Digitalization on Daily Lives*, Special Eurobarometer, Brussels 2020, p. 8.

(15 pp) (table 3).[27] In 2019, the mean percentage level of EU citizens who declared daily use of the internet (76%) surpassed by 6 pp the number of respondents declaring the possession of digital skills (70%). In 2017, however, a reverse dependency was noted: the number of the respondents declaring the possession of technical skills (71%) surpassed by 5 pp the number of respondents using the internet daily (66%). It should be noted that the above conclusions do pertain equally to all the citizens in EU member states. In 2019, a reverse dependency was noted in five out of the twenty-eight examined countries. In Portugal: by 6 pp, in Slovenia and Poland: by 5 pp, Germany: 4 pp and Austria: by 1 pp. The mean level of technical skills of their citizens surpassed the mean level of people using the internet daily. Analogically, in 2017, different conclusions were formulated for three of the 28 countries of the EU. The percentage of people using the internet daily surpassed the percentage of their skill reports (Hungary, Netherlands: both 1 pp and France: 2 pp). In two of these countries an equal percentage level of people declaring daily use of the internet and declaring technical skills was noted (in Belgium: 72% and Bulgaria: 54%) (table 3).

In 2019, the greatest difference in the level of technical skills and daily use of the internet was noted in Spain: 16 pp, in Italy: 15 pp and Malta: 13 pp. While two years earlier in Rumania: 17 pp, in Italy: 16 pp and in Crete and Poland: both 15 pp. In 2017, as well as in 2019, Italy belonged to the group of three countries of the EU where the greatest difference was noted between the level of technical skills and the daily use of the internet. In 2017, the level of skills was greater there by 16 pp than the level of people using the internet daily, while in 2019, the result was smaller by 15 pp (table 3). This shows the dynamism of the examined dependence. Skills in the area of criminal action, such as the infection of devices with malicious software, can be used to verify the level of technical skills of EU citizens. It is seen as cybercrime from the technical domain with the lowest degree of harmfulness (83%).

It is evident from research by Eurobarometer that the increase in the level of fear of becoming a victim of malicious software (from 43% in 2012, 45% in 2013, 66% in 2014, 69% in 2017, 71% in 2018 to 66% in 2019) is the cause of the diminishing of the number of EU citizens who claim that they are able to protect themselves from cybercrime with the help of antivirus software (from 74% in 2014: 71% in 2017 to 59% in 2019). Only in 2017 one notices a comparable level. One should also note the comparable lowering tendency of the number of respondents who affirm that they "Totally Agree": by 15 pp and "Totally Disagree": by 14 pp, with the attitude "You are able to protect yourself sufficiently

[27] European Union, *Attitudes Towards the Impact of Digitalization on Daily Lives*, Special Eurobarometer 503, Brussels 2020, pp. 60, 67.

against cybercrime by using antivirus software".[28] The data obtained show an understanding of the risk and digital menace, the capability of a critical opinion of one's own possibilities and of accessible digital instruments and of the lessening skill of protecting one's own devices by EU citizens.

Does the fear of becoming a victim of contamination of appliances by malicious software motivate one to improve technical skills? In 2019, despite declared fears (66%) and a lack of technical skills (30%), EU citizens did not know what skills they should improve precisely (24%). Nearly every fourth respondent asked about the obstacles impeding the improvement of digital skills pointed out that "they don't know what specific skills they should improve", which constitutes a third of those examined declaring that they have such skills.[29] The above situation indicates a lack of skills in the recognition of deficiency in the range of their own digital competence, of the understanding of the need of raising and updating their own competence, or the need of current observation of new technological solutions.

The greatest difference between the level of fear of becoming a victim of infected appliances and the level of obstacles hindering the improvement of technical skills was observed in: Portugal: 67 pp, Bulgaria: 60 pp and Greece: 58 pp; whereas the lowest in: Sweden: 12 pp, Netherlands: 13 pp and in Denmark: 14 pp. The latter citizens declared the highest level of digital skills. To the group of countries with the lowest level of digital skills and the lowest level of knowledge concerning what definite skills should be improved belongs Greece: 55% compared to 15%. At the same time, it is a country where the level of fear surpasses by 7 pp the mean level established for countries of the EU.

The level of fear of becoming a victim of cybercriminal action of a technological character is not derivative of the experience of EU citizens of being a cyber victim. It is evident from Eurobarometer studies that from the year 2014 a constant level of fear persists (66%), together with a systematically diminishing number of people admitting having been a victim of an infection of their appliance (with 47% in 2014, 42% in 2017, 33% in 2018 to 28% in 2019). The mean level of fear in member countries of the EU in 2019 (66%) surpassed more than twofold the indicator of real experiences (28%).

The data in Eurobarometer also indicate that in the following years the difference between the level of fear and the level of frequency of being a victim of cybercrime of a technological nature increases. In 2014, the greatest difference

[28] European Union, *Cyber Security*, Special Eurobarometer 423, Brussels 2015; European Commission, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 464a, Brussels 2017; European Union, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 499, Brussels 2020, p. 20.

[29] European Union, *Attitudes Towards the Impact of Digitalization on Daily Lives*, Special Eurobarometer 503, Brussels 2020, p. 60.

was noted in Ireland: 43 pp, in the Republic of Cyprus and Greece – both 38 pp and 37 pp in Great Britain, whereas five years later, in 2019 it increased to 66 pp in Bulgaria, 65 pp in Portugal and 55 pp in Greece. A high level of fear may be derivative of the recognition by the EU citizens of a deficiency as regards skills of protection of one's own appliances, of the understanding of the risk linked to the use of the internet and of the ignorance of current strategies of avoiding cybercrime.

Humanistic competences in the field of knowledge and attitudes

Digital competences in the humanistic (informative) domain: knowledge

In accordance with the Recommendation of the European Parliament and the Council on the establishment of the European Qualifications Framework for lifelong learning, "knowledge" means the outcome of the assimilation of information through learning. It is a body of facts, principles, theories and practices related to the field of work or study. Knowledge is described as theoretical and/or factual.[30]

The ability to assess critically the content and trustworthiness of information, being a derivative of knowledge possessed, conditions the level of information on the subject of cybercrime behaviour. The collected data (table 2) evidently show that the number of citizens of the EU who consider themselves well informed – that is possessing sound and trustworthy information – systematically increases (from 38% in 2012 to 52% in 2019). Despite the number of persons declaring a lack of information (from 59% in 2012 to 47% in 2019), the conclusion comes to mind that competence in the domain of critical assessment of information, its processing or understanding is possessed by only half of the citizens of the EU (52%). This result indicates a great neglect in the domain of humanistic competences.

In 2019, the Danes and Germans thought themselves to be the best informed: 80%, the Dutch: 73% and Swedes: 72%. The lowest level of being informed was declared by the citizens of Bulgaria: 30%, Italy: 31% and Rumania: 32%. In fourteen out of twenty-eight countries, an increase in the level of information was noted (ES: 8 pp; EE, MT: 5 pp; DK, EL, NL: 4 pp; LT: 3 pp; CZ, HR, PL, RO, SI: 2 pp; LV, FI: 1 pp). In five, the level as of 2017 was preserved, whereas in nine countries, a decreasing tendency was observed (DE, HU, SK, UK: a decrease of 1 pp; BE: 3 pp; IT, SE: 4 pp; PT: 5 pp, IE: 6 pp). The greatest increase was observed in Spain: by 8 pp and in Estonia and Malta: both by 5 pp, with the greatest decrease in Ireland: 6 pp and Portugal: 5 pp.

[30] Council of the European Union, Council Recommendation of 22 May 2017…, p. 20.

The data collected allow one to confirm the hypothesis that the citizens of the EU possess greater digital competence of a technological nature than of a humanistic one. In 2017, the level of technical skills surpassed by 20 pp the level of information (humanistic competences), while two years later the advantage was by 18 pp. The data obtained also indicate an increasing tendency in the domain of humanistic competences with a slight decrease in technical skills (table 2, 3). The increase in humanistic competences may be one of the causes of the decrease in the level of trust that the citizens of the EU have towards the internet. In the years 2012–2019, the number of the respondents who think themselves to be well informed (from 38% to 52%) increases, while at the same time, the number of those trusting the internet decreases (from 35% to 30%).[31] It should be stressed that only a complex strategy of EU countries in the domain of humanistic competence makes it possible to collect knowledge of the working mechanisms of information making, its search and management, principles of indexing, classification and providing access through diverse appliances and conveyors. This knowledge enables analysis, critical assessment and interpretation concerning cybercriminal actions. Its lack observed in the EU countries is determined, among others, by a declining trust in the media.

The level of digital competence of the EU citizens is derivative of media politics of member states. Eurobarometer data clearly shows groups of EU countries in which the highest as well as the lowest level of both kinds of competence is noticed. The highest level of technological and humanistic competence is reported for the Netherlands, Sweden and Denmark; while the lowest for Bulgaria, Rumania and Italy. The greatest discrepancy between the level of technological and humanistic competence in 2019 was noticed in Portugal and Croatia: both 32 pp, Belgium: 30 pp and Slovenia: 29 pp; whereas in 2017: in Italy: 34 pp, Croatia and Spain, both 30 pp and Belgium and Rumania: 29 pp. A comparable level of both competences in 2019 occurred in Germany: 81% to 80%, in Malta: 59% to 60%, and in Lithuania: 59% to 56%; whereas in 2017: again in Germany: 73% to 76% and in Hungary: 52% to 42%. Although the mean result for all EU countries indicates a greater level of digital competence of a technological rather than a humanistic nature, two exceptions from this regularity were noted. In 2019, humanistic competences surpassed by 1 pp technical skills in Malta (59% to 60%), while in Germany in 2017: 73% to 76%. The level of information on the subject of cybercriminal action determines attitudes of the EU citizens, a further component of digital competence.

[31] European Union, *Attitudes Towards the Impact of Digitalization on Daily Lives*, Special Eurobarometer 503, Brussels 2020, p. 67; European Commission, *Media Use in the European Union*, Standard Eurobarometer 76, Brussels 2011, p. 5; European Union, *Media Use in the European Union*, Standard Eurobarometer 90, Brussels 2018, p. 15.

Table 3. Daily use of the Internet and the level of digital competence (data expressed as a percentage)

Country	2019							2017						
	Everyday Internet use	Technological competences			Humanistic competences			Everyday Internet use	Technological competences			Humanistic competences		
		1	**2**	**3**	**4**	**5**	**6**		**1**	**2**	**3**	**4**	**5**	**6**
EU28	76	70	27	3	52	47	1	66	71	25	4	51	46	3
HU	70	67	32	1	41	59	0	53	52	41	7	42	58	0
AT	78	79	17	4	53	46	1	66	70	27	3	53	44	3
DE	77	81	16	3	80	19	1	67	73	24	3	76	22	2
PT	67	73	21	6	41	57	2	59	68	27	5	46	51	2
BE	83	76	23	1	46	54	0	72	72	26	2	43	57	0
HR	74	71	27	2	39	60	1	52	67	27	6	37	61	2
SI	67	72	27	1	43	56	1	64	68	29	3	41	57	2
BG	64	57	33	10	30	66	4	54	54	37	9	30	67	3
IE	82	80	19	1	60	39	1	68	80	11	9	66	33	1
CY	75	65	29	6	49	50	1	57	66	22	12	49	49	2
LV	75	74	23	3	47	50	3	70	75	21	4	46	52	2
CZ	69	65	31	4	45	54	1	61	67	28	5	43	56	1
EE	78	73	20	7	57	42	1	72	75	19	6	52	44	2
LU	84	77	20	3	62	37	1	76	79	17	4	62	35	3
RO	61	57	35	8	32	67	1	42	59	34	7	30	68	2
FI	86	76	21	3	68	31	1	76	78	17	5	67	31	2

SE	95	87	12	1	72	28	0	88	89	8	3	76	24	0
UK	83	77	21	2	70	29	1	78	79	17	4	69	30	1
EL	67	55	44	1	42	57	1	53	58	40	2	38	61	1
NL	96	87	13	0	73	27	0	91	90	9	1	69	30	1
SK	67	60	32	8	44	54	1	52	63	28	9	45	52	3
DK	92	84	14	2	80	19	1	87	88	10	2	76	22	2
PL	65	69	28	3	55	43	2	58	73	24	3	52	46	2
ES	79	63	34	3	45	55	1	62	68	26	6	38	62	0
FR	77	64	34	2	52	46	2	72	70	28	2	52	46	2
LT	69	59	37	4	56	42	2	61	65	32	3	53	43	4
MT	72	59	34	7	60	32	8	67	68	22	10	55	34	9
IT	72	57	40	3	31	67	2	53	69	27	4	35	59	6

Legend: **1** – Total "Agree", **2** – Total "Disagree", **3** – Don't know, **4** – Total well informed, **5** – Total not well informed, **6** – Don't know

Source: own study based on: European Union, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 480, Brussels 2019; European Union, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 499, Brussels 2020; European Commission, *Media Use in the European Union*, Standard Eurobarometer 88, Brussels 2017; European Union, *Attitudes Towards the Impact of Digitisation and Automation on Daily Life*, Special Eurobarometer 460, Brussels 2017; European Union, *Attitudes Towards the Impact of Digitalization on Daily Lives*, Special Eurobarometer 503, Brussels 2020.

Digital competence in the humanistic (social) domain: attitude

In the above quoted Council recommendation of 2017, attitudes are conceived as the motivators of continued competent performance. They include values, aspirations and priorities. The role of such motivators is played by the attitudes of the EU citizens in face of the increasing, although unsystematic, risk of becoming a victim of a cybercriminal action (from 74% in 2012 to 83% in 2019). The most frequently declared attitude (89% in 2012, 86% in 2019) is active protection of personal data by avoiding their disclosure, the national access of information concerning oneself on the internet. EU citizens are aware of the principles of protection of privacy as regards themselves and other persons; of the influence and durability of digital information published by themselves, and of the existing dangers. This attitude may be a result of fear concerning their safety, which is not guaranteed by the administrators of internet websites (72% in 2012, 74% in 2019), or public authorities (66% in 2012, 67% in 2019).

The indicator of digital competence in the humanistic field may be the attitude of EU citizens in respect of online content which promotes racial hatred or religious extremism. If we compare how the level of fear of becoming a victim of such content increased in the years 2012-2019 (from 41% to 53%) with possible attitudes of cyber security (the avoidance of personal data, trust in respect of the administrators of the website and national institutions), then we can notice that the rise of the level of fear does not influence any change in the attitude of the internet users. The possibility of avoiding the revealing of personal data as well as the fear of protection by administrators of the network and national institutions, all have remained on a comparative level during the last seven years. Analogically appears the level of attitudes of persons declaring contrary opinions – Totally disagree: "You avoid disclosing personal information online" – 10% in 2012, 12% in 2019; "You are concerned that your online personal information is not kept secure by websites" – 25% in 2012, 23% in 2019; "You are concerned that your online personal information is not kept secure by public authorities" – 31% in 2012, 30% in 2019 (table 4).

In the years 2012–2019, of 28 member countries of the EU only in two a decline in the level of fear of online material promoting racial hatred was noted; in the remaining twenty-six, an increase is noted. The greatest dynamic of growth of fear, with a mean result of 12%, was noted in Rumania: by 24 pp, Bulgaria: by 22 pp and Poland: by 21 pp. While its decline was noticed in Hungary: by 7 pp and the Czech Republic: by 1 pp. In 2019, the greatest level of fear was revealed by the citizens of Spain: 73%, Ireland: 70% and Poland: 68%; with the lowest in Sweden: 22%, Netherlands: 26% and Denmark: 30%. The difference between countries oscillates around 50 pp, with a mean result for EU countries of 53%. In addition, one notices a certain, unchanging group of countries of the EU, both of the highest (Spain, Ireland), as well of the lowest level of fear (Sweden,

Table 4. Attitudes to cyber-security (data expressed as a percentage)

Attitudes	Could you please tell me to what extent you agree or disagree with each of the following statements?														
	Total "Agree"					Total "Disagree"					Don't know				
	2019	2018	2017	2014	2012	2019	2018	2017	2014	2012	2019	2018	2017	2014	2012
You avoid disclosing personal information online	86	79	71	74	89	12	11	25	23	10	2	4	4	3	1
You are concerned that your online personal information is not kept secure by websites	74	68	73	73	72	23	21	25	24	25	3	3	2	3	3
You are concerned that your online personal information is not kept secure by public authorities	67	62	65	67	66	30	27	32	30	31	3	3	3	3	3
You believe the risk of becoming a victim of cybercrime is increasing	83	79	86	85	74	13	10	11	12	16	4	3	3	3	10

Source: own study based on: European Union, *Cyber Security*, Special Eurobarometer 390, Brussels 2012; European Union, *Cyber Security*, Special Eurobarometer 423, Brussels 2015; European Commission, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 464a, Brussels 2017; European Union, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 480, Brussels 2019; European Union, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 499, Brussels 2020.

Table 5. The level of fear and frequency of being a victim of cybercrime of a humanistic nature (data expressed as a percentage)

Country	Concerns about becoming a victim of online material which promotes racial hatred or religious extremism *versus* frequency of being a victim																											
	2019						2018						2017						2014						2012					
	1	**2**	**3**	**4**	**5**	**6**	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**2**	**3**	**4**	**5**	**6**
	53	44	3	13	85	2	65	32	3	18	80	2	51	47	2	18	81	1	46	51	3	14	85	1	41	57	2	15	83	2
	C			F			C			F			C			F			C			F			C			F		
EU28	53			13			65			18			51			18			46			14			41			15		
BE	55			20			71			27			44			19			44			19			36			20		
BG	66			10			65			6			60			15			44			16			44			16		
CZ	49			14			60			18			48			18			45			20			50			20		
DK	30			20			42			24			32			15			33			12			23			7		
DE	41			17			57			21			34			16			28			11			28			13		
EE	33			19			39			22			21			18			24			16			29			21		
IE	70			11			82			13			60			14			61			14			54			12		
EL	45			6			52			7			39			9			44			7			42			9		
ES	73			8			78			10			66			10			72			11			63			14		
FR	60			14			77			21			55			16			49			14			51			15		
HR	55			20			66			23			55			17			58			22			-			-		
IT	62			10			69			13			64			18			59			12			49			15		
CY	60			12			69			15			56			20			43			14			56			17		
LV	61			12			66			17			49			15			37			17			46			14		
LT	56			8			70			12			53			19			45			14			49			15		
LU	47			19			67			24			49			18			39			12			42			15		

HU	39	15	50	13	44	14	36	17	46	30
MT	49	16	65	15	62	26	50	25	45	18
NL	26	20	49	26	20	22	20	20	16	11
AT	41	15	55	19	48	20	41	18	34	18
PL	68	10	71	14	68	26	49	22	47	20
PT	59	3	58	7	55	8	59	20	57	18
RO	59	13	74	17	57	23	46	24	35	26
SI	44	11	53	12	39	9	39	10	34	12
SK	33	11	43	13	34	12	23	12	32	26
FI	40	25	60	30	32	28	23	15	35	23
SE	22	36	38	47	18	35	20	28	12	21
UK	51	8	32	14	61	20	54	12	39	12

Legend: **1** – Total "Agree", **2** – Total "Disagree", **3** – Don't know, **4** – Total well informed, **5** – Total not well informed, **6** – Don't know

Source: own study based on: European Union, *Cyber Security*, Special Eurobarometer 390, Brussels 2012; European Union, *Cyber Security*, Special Eurobarometer 423, Brussels 2015; European Commission, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 464a, Brussels 2017; European Union, *Europeans' Attitudes Towards Internet Security*, Special Eurobarometer 480, Brussels 2019; European Union, *Europeans' Attitudes Towards Cyber Security*, Report, Special Eurobarometer 499, Brussels 2020.

Netherlands, Estonia), which may indicate a stagnation of attitudes of some of their citizens in the face of menace to privacy, personal data or psychic health.

The increasing level of fear of becoming a victim of cybercriminal action of a humanistic nature is not a derivative of the noted frequency of being a victim of a given cybercrime. Although until 2018 a rising tendency is noted both in respect of fear, as in the experience of EU citizens, their increase is incomparable. The level of fear rose by 24 pp (from 41% in 2012 to 65% in 2018: the highest level), in that time the level of experience rose by 3 pp, and the next year (2019), fell by 5 pp, which marked the lowest result in the span the last seven years (13%). On average, the level of fear surpasses three times the level of frequency of being a victim. The greatest difference – over four times – was noted in 2019, while the lowest in 2012. Although not systematically, the number of the respondents who do not fear this type of cybercrime has dwindled (from 57% in 2012 to 44% in 2019). More than eight out of ten EU citizens have never come across internet content promoting racial or religious hatred.

Although the mean result for EU countries indicates a higher level of fear in respect of declared experiences, we cannot come to a similar conclusion regarding all EU countries. An exception is Sweden where, in the years 2012–2019, the level of fear was lesser than the frequency of being a victim. In subsequent years, the following proportions were noted: 2019: 22% to 36%; 2018: 38% to 47%; 2017: 18% to 35%; 2014: 20% to 28%; in 2012: 12% to 21%. Sweden was also among the countries with the lowest level of fear and the highest level of declarations of being a victim of content promoting racial hatred. Whereas Spain, in all the years analysed, was found to be in the group of three countries with the greatest difference between the level of fear and the frequency of being a victim. The data obtained indicate that in subsequent years the difference has grown, although not linearly, between the level of fear and the level of experience. In 2012, the greatest discrepancy: 49 pp was noted for Spain, after six years, it increased to 69 pp in Ireland, while in 2019, the highest level was reached in Spain: 65 pp.

Cybercrime of a technological and humanistic nature

Eurobarometer data analysis proves that the EU citizens more often admit to being victims of cybercrime of a technological nature (annual average of 37.7% of the respondents are victims of appliances affected by a malicious software) than of a humanistic kind (online content promoting racial hatred or religious extremism: 15.3%). In the years 2014–2019, nearly every four out of ten examined persons were victims of cybercriminal action of a technological nature, while 15.3%, that is less than half of the technological victims were victims of cybercriminal action of a humanistic kind: 15.3%. Although a decreasing tendency

is noted, both in the level of victims of cybercrime of a technological nature, as well as of a humanistic one, they are not comparable. In the years 2014–2019, the number of cybercriminal actions of a technological nature diminished by 19 pp, whereas of a humanistic one: by 1 pp. During the last five years, the discrepancy also diminished by 19 pp between the number of victims who at least once experienced cybercrime of a technological and a humanistic nature (2019: 15 pp, 2018: 15 pp, 2017: 24 pp, 2014: 33 pp). For a few years now, a permanent, low percentage (1.5%) is noted of EU citizens who do not know whether they were victims of cybercriminal action at any time.

Table 6. The frequency of being a victim of cybercriminal action (data expressed as a percentage)

Year	The frequency of becoming a victim of cybercriminal action					
	Technological criminal activity (the infection of devices with malicious software)			Humanistic criminal activity (online material which promotes racial hatred)		
	Total at least once	Never	Don't know	Total at least once	Never	Don't know
2019	28	70	2	13	85	2
2018	33	65	2	18	80	2
2017	42	57	1	18	81	1
2014	47	52	1	14	85	1
2013	-	-	-	14	85	1
2012	-	-	-	15	83	2
Total	150	244	6	92	499	9
Average	37.5	61	1.5	15.3	83.2	1.5

Source: own study based on: European Union, *Cyber Security*, Special Eurobarometer 390, Brussels 2012; European Union, *Cyber Security*, Special Eurobarometer 404, Brussels 2013; European Union, *Cyber Security*, Special Eurobarometer 423, Brussels 2015; European Commission, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 464a, Brussels 2017; European Union, *Europeans' Attitudes Towards Internet Security*, Special Eurobarometer 480, Brussels 2019; European Union, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 499, Brussels 2020.

Drawing upon an analysis of data contained in Eurobarometer[32], one may conclude that as regards cybercrime of a technical nature, a comparable level of respondents is noticed who perceive it as "a very serious crime": 42% with the level of EU citizens who have experienced it (33%). Whereas for cybercrime of a humanistic nature, the percentage of the respondents who perceive it as a "a very serious crime": 61% is comparable with a level of fear of becoming its

[32] European Union, *Europeans' Attitudes Towards Internet Security*, Special Eurobarometer 480, Brussels 2019.

victim: 65%. Six out of ten citizens of the EU are anxious about it and perceive it as a serious crime, while less than two out of ten people examined are its victims.

Conclusion

The purpose of the article was a study of the scope of digital competence (technological and humanistic) in cybercriminal action, under a relational approach to the notion of competence, based on the example of internet levels, as well as the confrontation of theoretical assumptions with the frequency with which it is experienced by the citizens of the European Union. Analyses of the literature on the subject and of Eurobarometer data enabled verification of the adopted research hypotheses. The analyses carried out confirm the first hypothesis. The relational approach to the notion of competence, as opposed to the catalogue one, takes into account all the components of competence (skills, knowledge, attitudes). Apart from technological sub-competences, it also includes humanistic sub-competences (social, informative and cultural), which are missing in the catalogue approach. This is why the relational approach should substitute the catalogue approach to digital competences, which focuses merely on socio-demographic qualities and fails to allow for the component of attitudes. The second hypothesis, assuming that the EU citizens possess greater digital competence of a technological nature than of a humanistic kind, and that they more often admit being a victim of cybercriminal action of a technological nature than a humanistic one, was partially confirmed. Although the mean result for EU countries indicated greater digital competence of a technological nature than of a humanistic one (by 20 pp in 2017 and 18 pp in 2019), we cannot, however, extrapolate this conclusion over all EU citizens. Two exceptions are noted from this dependence. In 2019, humanistic competences surpassed by 1 pp technological competences in Malta, while in 2017, by 3 pp in Germany. Also observed was a comparable level of technological and humanistic competences in 2019 in Germany: 81% to 80%, in Malta: 59% to 60% and in Lithuania: 59% to 56%; whereas in 2017: again in Germany: 73% to 76% and in Hungary: 52% to 42%. In a longer perspective, the mean result for EU countries indicates a growing tendency in the domain of humanistic competences with a slight fall of technical skills. Also noticed was a group of countries in which both the highest level of technological and humanistic (Netherlands, Sweden, Denmark, and Germany) competences was noted, as well as their lowest level (Bulgaria, Rumania, and Italy). EU citizens more often admit to being victims of cybercrime of a technological nature (37.7%) than of a humanistic one (15.3%). Significant disproportions are noticed. In the years 2014–2019, nearly every four out of ten examined were victims of infection by malicious software, while as

regards content propagating racial hatred or religious extremism, less than two out of ten were affected. A considerably greater decline in the case of cybercrime of a technological nature (19 pp), than of a humanistic one (1 pp) was noted. With the exception of Sweden, both in the case of cybercriminal action of a technological nature (more than twice), as in that of a humanistic kind (more than thrice), the level of fear surpasses the level of frequency of its experience. In addition, falling tendencies of frequency of being a victim of both kinds of cybercrime are accompanied by a constant level of fear of becoming a victim of cybercrime action of a technological nature (66%), and an increase in the level of fear of becoming a victim of cybercrime of a humanistic nature (from 41% in 2012 to 53% in 2019). The data obtained testify to an ignorance of EU citizens as regards the level of actually experienced cybercrimes – a factor that intensifies the level of fear and results above all from a lack of sound knowledge concerning safety and protection measures. Only a proper level of humanistic competences may solve the problem of anxiety/fear of contemporary society.

Bibliography

Bogunia-Borowska M., Łuczaj K., *Kompetencje medialne młodzieży w wieku gimnazjalnym. Co i w jaki sposób badać?*, "Państwo i Społeczeństwo" 2017, vol. 17, no. 3, pp. 135–150.

Center for Media Literacy, *About CML*, https://www.medialit.org/about-cml (accessed 11.05.2022).

Council of the European Union, Council Recommendation of 22 May 2017 on the European Qualifications Framework for Lifelong Learning and Repealing the Recommendation of the European Parliament and of the Council of 23 April 2008 on the Establishment of the European Qualifications Framework for Lifelong Learning (2017/C 189/03), OJ C 189, 15.06.2017, pp. 15–28.

European Commission, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 464a, Brussels 2017.

European Commission, *Media Use in the European Union*, Standard Eurobarometer 76, Brussels 2011.

European Commission, *Media Use in the European Union*, Standard Eurobarometer 78, Brussels 2012.

European Commission, *Media Use in the European Union*, Standard Eurobarometer 88, Brussels 2017.

European Parliament and the Council, Recommendation of the European Parliament and of the Council of 18 December 2006 on Key Competences for Lifelong Learning (2006/962/EC), OJ L 394, 30.12.2006, pp. 10–18.

European Schoolnet, http://www.eun.org (accessed 15.02.2022).

European Union, *Attitudes Towards the Impact of Digitalization on Daily Lives*, Special Eurobarometer 503, Brussels 2020.

European Union, *Attitudes Towards the Impact of Digitization and Automation on Daily Life*, Special Eurobarometer 460, Brussels 2017.

European Union, *Cyber Security*, Special Eurobarometer 390, Brussels 2012.

European Union, *Cyber Security*, Special Eurobarometer 404, Brussels 2013.

European Union, *Cyber Security*, Special Eurobarometer 423, Brussels 2015.

European Union, *Europeans' Attitudes Towards Cyber Security*, Special Eurobarometer 499, Brussels 2020.

European Union, *Europeans' Attitudes Towards Internet Security*, Special Eurobarometer 480, Brussels 2019.

European Union, *Media Use in the European Union*, Standard Eurobarometer 90, Brussels 2018.
European Union, *Media Use in the European Union*, Standard Eurobarometer 86, Brussels 2016.
Ferrari A., *DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe*, Report EUR 26035 EN, Luxembourg 2013.
Foucault M., *Power/Knowledge. Selected Interviews and Other Writings 1972–1977*, Harvester Wheatsheaf, New York 1980.
Gordon S., Ford R., *On the Definition and Classification of Cybercrime*, "I Comput Virol" 2006, no. 20, pp. 13–20.
Grabosky P., *Cybercrime. Keynotes in Criminology and Criminal Justice Series*, Oxford University Press, Oxford 2016.
Gruchoła M., *Kompetencje medialne nauczycieli w dobie nowych technologii. Kilka refleksji socjologa i kulturoznawcy*, "Lubelski Rocznik Pedagogiczny" 2019, vol. 38, no. 3, pp. 95–116. DOI: 10.17951/lrp.2019.38.3.95-116.
Gruchoła M., *Polityka Unii Europejskiej w zakresie cyberprzestępczości*, in: *Patologie w cyberświecie,* eds. S. Bębas, J. Plis, J. Bednarek, Wyższa Szkoła Handlowa, Radom 2012, pp. 147-165.
Gruchoła M., *W pajęczynie globalnej sieci*, "Społeczeństwo i Rodzina" 2016, vol. 47, no. 2, pp. 94–116.
Gruchoła M., Szulich-Kałuża J., *Kompetencje medialne w komunikacji wizualnej*, Wydawnictwo KUL, Lublin 2020.
Hoechsmann M., Poyntz S., *Media Literacies: A Critical Introduction*, Wiley-Blackwell, Malden 2012.
Jasiewicz J., Filiciak M., Mierzecka A. et al., *Framework Directory of Digital Skills*, Centrum Cyfrowe Projekt Polska, Warszawa 2015.
Johnson D., Post D., *Law and Borders: The Rise of Law in Cyberspace*, "Stanford Law Review" 1996, vol. 48, no. 5, pp. 1367-1402.
Livingstone S., *The Changing Nature and Uses of Media Literacy*, Media@LSE Electronic Working Papers 4, London School of Economics and Political Science, London 2003.
Shinder D.L., Tilttel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, trans. J. Dobrzański, K. Masłowski, Wydawnictwo Helion, Gliwice 2006.
Siadak G., *Kompetencje cyfrowe polskich uczniów i nauczycieli – kierunek zmian*, "Ogrody Nauk i Sztuk" 2016, vol. 6, pp. 368–381.
Społeczeństwo informacyjne w liczbach 2014, ed. V. Szymanek, Ministerstwo Administracji i Cyfryzacji, Warszawa 2014.
Wall D.S., *Cyberrime, Media and Insecurity. The Shaping of Public Perceptions of Cybecrime*, "International Review of Law, Computers & Technology" 2008, vol. 22, nos. 1–2, pp. 45–63.

Summary

The purpose of the article is a study of components of digital competence (technological and humanistic) in cybercrime behaviours, based on the example of internet levels (technical, social and informative) as well as the confrontation of theoretical assumptions with the frequency of their experience by the citizens of the European Union. Subject to analysis were fourteen reports of Eurobarometer, carried out in twenty-eight countries of the EU in the years 2011–2019. The method applied is a quantitative and qualitative analysis of data available, comparative, historical as well as analytical-synthetic. Two research hypotheses were accepted: 1) A catalogue formulation of digital competences focusing on social-demographic traits should be replaced by a relational formulation taking into account the skills, knowledge and attitude of internet users. 2) EU citizens possess greater digital competences of a technological character and more often admit being affected by cybercrime behaviours of a technological kind than of a humanistic one. The first hypothesis was confirmed, whereas the second was only partially confirmed. In basing ourselves on a typology of three layers of the internet, we proposed two areas of digital competence: technological competence and humanistic competence (social and informative). These were subordinated to particular layers of the internet

and in this context an analysis was carried out of the social opinion of EU citizens on the subject of cybercrime behaviours. The low level of humanistic competence (52%) reported by EU citizens determines a high degree of fear which does not show a causal-effective connection in the actual level of noted experiences of being a victim of criminal behaviour.

Keywords: competence components, cybercrime, digital competence, Eurobarometer, humanistic competence, technological competence

Kompetencje cyfrowe użytkowników internetu w zachowaniach cyberprzestępczych. Studium na podstawie badań Eurobarometru

Streszczenie

Celem artykułu było uporządkowanie i określenie w ujęciu relacyjnym zakresu komponentów kompetencji cyfrowych w zachowaniach cyberprzestępczych oraz skonfrontowanie teoretycznych założeń z częstotliwością ich doświadczania przez mieszkańców Unii Europejskiej. Analizie poddano 16 raportów Eurobarometer obejmujących wszystkie państwa Unii Europejskiej w latach 2010–2019. Zastosowano metody ilościowej i jakościowej analizy danych zastanych, porównawczą, historyczną oraz analityczno-syntetyczną. Jako hipotezy badawcze przyjęto, że: 1) ujęcie katalogowe kompetencji cyfrowych koncentrujące się na cechach społeczno-demograficznych powinno być zastąpione ujęciem relacyjnym uwzględniającym także inne komponenty kompetencji cyfrowych, czyli wiedzę, umiejętności i postawy; 2) mieszkańcy Unii Europejskiej mają większe kompetencje cyfrowe o charakterze technologicznym i częściej przyznają się do bycia ofiarą cyberprzestępczości o charakterze technicznym niż humanistycznym. Pierwsza hipoteza została potwierdzona całkowicie. Ujęcie relacyjne – w odróżnieniu od katalogowego – uwzględnienia wiedzę, umiejętności i postawy jako komponenty kompetencji cyfrowych, a obok kompetencji technologicznych – także humanistyczne, czyli informacyjne, kulturowe i społeczne. Druga hipoteza została potwierdzona częściowo. Chociaż uśredniony wynik dla państw Unii Europejskiej wskazuje na większe kompetencje cyfrowe o charakterze technologicznym niż humanistycznym (w 2017 roku o 20 punktów procentowych, a w 2019 roku o 18 punktów procentowych) to istnieją wyjątki od tej prawidłowości (Niemcy w 2017 roku i Malta w 2019 roku). Zauważa się również grupę państw, w których odnotowano zarówno najwyższy poziom kompetencji technologicznych i humanistycznych (Dania, Holandia, Niemcy, Szwecja), jak i najniższy (Bułgaria, Rumunia, Włochy). Mieszkańcy Unii Europejskiej częściej przyznają się do bycia ofiarą cyberprzestępczości o charakterze technologicznym niż humanistycznym (uśredniony wynik to odpowiednio 37,7 i 15,3% w ciągu roku). Zmniejsza się zatem różnica pomiędzy liczbą ofiar, które przynajmniej raz doświadczyły cyberprzestępczości o charakterze technologicznym i humanistycznym. Bazując na typologii trzech warstw internetu, tj. technicznej, społecznej i informacyjnej, zaproponowano nowe obszary kompetencji cyfrowych: technologiczną, społeczną oraz informacyjną. Podstawowe komponenty kompetencji przyporządkowano poszczególnym warstwom internetu i w tym kontekście dokonano analizy opinii społecznej mieszkańców Unii Europejskiej dotyczącej zachowań cyberprzestępczych i podstawowych typów cyberprzestępczości, wymagających kompetencji zarówno z obszaru technologicznego, jak i humanistycznego.

Słowa kluczowe: komponenty kompetencji, cyberprzestępczość, kompetencje cyfrowe, Eurobarometr, kompetencje humanistyczne, kompetencje technologiczne