Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.09

Received: 10.01.2021
Accepted: 11.04.2021

Wojciech Filipkowski
University of Bialystok, Poland
w.filipkowski@uwb.edu.pl
ORCID ID: https://orcid.org/0000–0001-6248–0888

Lorenzo Picarella
University of Milan, Italy
lorenzo.picarella@unimi.it
ORCID ID: https://orcid.org/0000–0002-5281–3017

Criminalizing Cybercrimes: Italian and Polish Experiences

Abstract: The rapidly advancing development of technology has both positive and negative effects on society and its members. Moreover, legislation can be slow to catch up with reality. This also applies to any reaction of society to new forms of social deviance. There is typically a delay in the introduction of legislation which tries to give a legal framework to new technological developments. The authors have taken an exploratory approach, analysing changes in Italian and Polish penal law relating to cybercrime that have occurred in Italy and Poland so far. The timeline, pace, and scope of the processes of criminalization are presented for each country. Even though both legislators had and have the same goal, differences in the approach to achieving it are visible. The conclusions may lead to changes in the penal policies of both countries.
Keywords: cybercrime, Italy, penal law, penal policy, Poland

Introduction

The Council of Europe Convention on Cybercrime, which was drawn up in Budapest on 23 November 2001 (entering into force in 2004), is of key importance in the fight against cybercrime. It was the first, and currently remains the only, act of international criminal law directly regulating the issue. This Convention was an effort to address the challenges posed by the development of information technology at global, regional, and local levels. Despite more than 20 years having passed since

its adoption, there are still asymmetries between countries in the criminalization of behaviour related to computers and their networks. From a scientific point of view, it is worth exploring these dissimilarities, as they may contribute to the search for the best legislative solutions in this area.

The main objective of this study is to examine the legislative actions taken by Italian and Polish legislators in the field of the criminalization of behaviour related to the functioning of computers and their networks. We have chosen two European countries which are members of the European Union, whose legal systems grew out of Roman law, belonging to one legal family and which have also ratified the Budapest Convention. At the same time, these are two countries which developed technologically in different ways, mainly due to the fact that Poland was an Eastern bloc country behind the Iron Curtain. Technological innovations arrived with a delay, which was then quickly compensated for in the period of political transition from the early 1990s.

The main research problem addressed in the study is to examine how the processes of the criminalization of pathological behaviour related to computers and their networks in both countries have developed in terms of time, pace, and scope. The hypothesis is that despite the above-mentioned similarities or dissimilarities, we are dealing with different approaches. In order to verify this hypothesis, the following research methods were used: dogmatic in relation to the regulations of both countries, desk research on Italian and Polish legal literature, and historical analysis.

1. Technological Evolution and its Impact on Penal Law

Technological advances have been characterized by the spread of computers (and subsequently other similar devices) throughout society in the last three decades. This evolution can be summed up in the following steps:[1]

- the first automatic data-processing devices (computers) – around and after the Second World War;
- the steady increase in the computing power and memory of these devices[2];
- the miniaturization of devices and falling prices per unit (microprocessors, microcomputers) – from the 1970s;
- increasingly widespread use in the public and private sectors, the connection of computers to local and wide area networks, exchanging data or information

1 P. Grabosky, Electronic Crime, Upper Saddle River 2007, p. 5ff.

2 M. Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice 2015, pp. 31ff.

and collecting it in databases (the development of telecommunications) – from the 1970s;[3]
- the emergence of mobile devices (from the 1970s) and wireless access to networks;[4]
- the commercialization of the Internet (broad public access to online services, i.e. via the web) and the progressive expansion of cyberspace (electronic mail, websites, search engines, instant messaging, social networks, forums, blogs) – in the mid-1990s;[5]
- the emergence of social deviance associated with access to the network (e.g. addiction to information, games, smartphones)[6] – at the beginning of the 21st century, as well as the phenomenon of the dark web (around 2009);[7]
- the concept of the internet of things (IoT):[8] devices connected to the network (of varying complexity, with their own computing power) can communicate with each other autonomously without human intervention – since 2008; they generate most of the traffic in networks.[9]

The list presented above is not strictly chronological since some of the elements occurred across a wide time frame and did not occur in all countries at the same pace. Another future milestone in technological development will be the spread of information technology (IT) solutions with a high degree of automation in the processes of acquiring and processing data and information, and consequently the implementation of artificial intelligence.

3 In 1957, the United States Department of Defense began the ARPA project, which was designed to create a unbreakable system for information exchange. Initially a military, and later an academic, network, ARPA (ARPANet) made their creators realize the development potential inherent in interconnected computers. The first two-way connection in ARPANet between computers took place in 1969. See M. Pudełko, Prawdziwa Historia Internetu, Piekary Śląskie 2013, p. 91.

4 M. Grzelak and K. Liedel, Bezpieczeństwo w cyberprzestrzeni: Zagrożenia i wyzwania dla Polski – zarys problemu, „Bezpieczeństwo Narodowe" 2012, no. 22, p. 125.

5 The Transmission Control Protocol/Internet Protocol (TCP/IP) was developed as early as the 1970s and 1980s, and contributed to the creation of a single and effective standard for the exchange of information; an e-mail program, the prototype of today's File Transfer Protocol (FTP); and the Domain Name System (DNS). The first Internet domain, symbolics.com, was registered as early as 1995 and WWW (World Wide Web) technology was created in 1989.

6 W.A. Kasprzak, Ślady cyfrowe. Studium prawno-kryminalistyczne, Warsaw 2015, p. 50.

7 V. Benjamin, S. Samtani and H. Chen, Conducting Large-Scale Analyses of Underground Hacker Communities, (in:) T.J. Holt (ed.), Cybercrime Through an Interdisciplinary Lens, Abingdon 2017, p. 62ff.

8 E.M. Kwiatkowska, Development of the Internet of Things: Opportunities and Threats, "Internet Kwartalnik Antymonopolowy i Regulacyjny" 2014, vol. 3, no. 8, p. 4.

9 2020 Global Networking Trends Report, CISCO, https://www.cisco.com/c/dam/m/en_us/solutions/enterprise-networks/networking-report/files/GLBL-ENG_NB-06_0_NA_RPT_PDF_MOFU-no-NetworkingTrendsReport-NB_rpten018612_5.pdf (accessed on 05.04.2021).

This technological evolution, and specifically the rise of cyberspace, has produced a change in the nature of human activities, criminal ones included. They now present new characteristics, including:[10]

- dematerialization (the resources/goods on the Internet do not possess physical components, but mainly consist in data and information);
- automation (technological progress has significantly reduced both the need for human intervention in IT operations and the minimum skill level needed to be competent in using IT);
- increased speed (the ever-increasing network speed has enhanced the pace of human activities);
- deterritorialization (the Internet is a space potentially limitless and without borders);
- ubiquity (computer users can carry out online activities from different virtual places at the same time);
- detemporalization (computer activities can be carried out without the direct intervention of the user by using automated software that will start operating at a specific time decided by the user themselves);
- overlapping between private and public dimensions (e.g the great amount of personal data uploaded to the web, especially to social networks).

These characteristics differ significantly from 'traditional' human physical activities, and they have inevitably made a significant impact on penal law, challenging its traditional principles and doctrines concerning:[11]

- the *actus reus*, the *mens rea*, and the nexus of causality (e.g. the act of the offender in cyberspace often loses importance in favour of the automated operations of software, because it is the latter which directly harms the victim; the role of the internet service provider is paradigmatic of these new challenges);
- the *locus commissi delicti* (considering that online activities are not subject to traditional borders, it may be challenging to determine the competent jurisdiction, e.g. in the case of international cyberattacks);
- harm and legally protected goods (e.g. the emergence of IT confidentiality and IT security as new potential legal goods that needs autonomous protection).

10 R. Flor, Lotta alla 'criminalità informatica' e tutela di 'tradizionali' e 'nuovi' diritti fondamentali nell'era di internet, 'Diritto penale contemporaneo' 20 September 2012; R. Flor, La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative, (in:) A. Cadoppi, S. Canestrari, A. Manna and M. Papa (eds.), Trattato di Diritto penale – Cybercrime, Milan 2019, p. 141ff.

11 L. Picotti, Diritto penale e tecnologie informatiche: una visione d'insieme, (in:) A. Cadoppi et al. (eds.), Trattato di Diritto penale, *op. cit.*, p. 34ff.

Even if most cybercrimes simply consist of a new way of committing traditional offences,[12] legislators have been forced to make changes in penal law through amendments or the introduction of new offences, because cybercrimes evade the scope of traditional offences due to the aforementioned characteristics.[13]

At the international level, the Council of Europe Convention on Cybercrime, which was drawn up in Budapest on 23 November 2001 (entering into force on 1 June 2004), was the first act of international penal law of the information-society era directly regulating the above matters, and is still the most influential.[14] The Convention, which aimed to harmonize substantial penal law and improve judicial cooperation between Member States, has greatly influenced national legislation on cybercrime, including that of Italy and Poland.

2. National Experiences

A. The Italian Penal Law System

In this section, we summarize the evolution of penal law legislation against cybercrime in Italy, highlighting its timeline and main features.[15] The first law that introduced a cybercrime offence in the Penal Code was enacted in 1978. In the following years, the legislator's activity was characterized by two systematic interventions, in 1993 and 2008, with the latter constituting the transposition of the Budapest Convention. Italian legislation against cybercrime has also been characterized by several narrow-scope interventions since the mid-1990s.

Regarding the criminalization of cybercrime behaviours, the legislation adopted two different approaches:[16]

1) the extension of the scope of 'traditional' offences, introducing new ways to commit the crime, or cyber goods as the target of the *actus reus*;
2) the creation of new offences.

12 P. Grabosky, Virtual Criminality: Old Wine in New Bottles? "Social & Legal Studies" 2001, no. 2, p. 243ff.

13 C. Pecorella, Reati informatici, (in:) Enciclopedia del diritto – annali, Milan 2017, p. 707ff.

14 For a specific analysis, see R. Flor, Cyber-criminality: le fonti internazionali ed europee, (in:) A. Cadoppi A. Cadoppi, S. Canestrari, A. Manna and M. Papa (eds.), Trattato di Diritto penale, *op. cit.*, p. 97ff. and A. Adamski, Przestępczość w cyberprzestrzeni. Prawne środki przeciw działania zjawisku w Polsce na tle projektu konwencji Rady Europy, Toruń 2001, p. 17.

15 Concerning the scope of the research, we take into consideration only 'cybercrimes and computer crimes *in a strict sense*' (for these definitions, see L. Picotti, Diritto penale, *op. cit.*, p. 77ff) or as covered by the Budapest Convention as far as the scope of criminalization is concerned. These definitions, which embody all the offences, make explicit reference to the computer or cyber dimension present in the Penal Code.

16 C. Pecorella, Reati informatici, *op. cit.*, p. 712ff.

In both cases, the new cybercrime offences were placed in the Penal Code next to their traditional counterparts, in that way avoiding the creation of an ad hoc section. This legislative choice was aimed at assimilating, as far as possible, the *ratio puniendi* and the structure of the old offences with the new ones.[17] Although this approach has been praised by the literature, it might lead to the transfer of the old offences' interpretation schemes to the new offences, increasing the risk of limiting their application.[18]

In general, the legislation has introduced and amended several offences to counter cybercrime through the years, trying to cover any possible gaps in the substantive penal law legislation. Even if the legislation's activity has mainly achieved its target, at the same time it has received a fair dose of criticism from the academic literature. The most recurrent issue that has been highlighted concerns the lack of technical accuracy in the creation of new offences or the amendment of 'old' ones, showing little attention to and/or knowledge of penal law and information and communications technology (ICT).[19] For example, the cyberfraud offence (Article 640-ter), due to the choice to distance it from the traditional fraud offence model, has not been a useful tool for prosecutors to counter cyberfraud; instead, its scope was more centred towards damage to computer systems and data.[20] The expansion of the definition of 'correspondence' in Article 616, without an explicit reference to the 'open' or 'closed' nature of it, has caused problems in the interpretation of the offence and has produced a loophole in the protection of the secrecy of correspondence, for example, in the case of the employer who reads the messages that employees receive on the company's e-mail accounts.[21] Article 392 does not make explicit reference to 'data' and 'programs' as possible objects of damage, therefore it has not been frequently applied in case law.[22] The element of 'belonging to another' in Article 635-bis (damage to computer data, information, or programs), which reflects the structure of the offence of vandalism on which Article 635-bis was based, makes it difficult to identify the victim of the crime, because data, information, and programs, due to their immaterial nature, cannot be owned or possessed in the same way as things.[23] It is also important to underline that there are very limited cases of damage to computer data and systems (Article 635 from -bis to -quinquies) in Italian jurisprudence.[24]

17 L. Picotti, Diritto penale, *op. cit.*, pp. 58–59.
18 *Ibidem*.
19 The legislator was only able to partially fix this general issue in 2008; L. Picotti, La ratifica della Convenzione Cybercrime del Consiglio d'Europa: Profili di diritto penale sostanziale, 'Diritto penale e processo' 2008, no. 6, p. 700ff.
20 C. Pecorella, Reati informatici, *op. cit.*, pp. 721–722.
21 *Ibidem*, p. 714.
22 *Ibidem*, p. 716.
23 L. Picotti, La ratifica della Convenzione Cybercrime, *op. cit.*, p. 711.
24 C. Pecorella, Reati informatici, *op. cit.*, p. 720.

Moreover, in some offences, particularly those concerning the actions that precede illegal access to a computer system (Article 615-quater and -quinquies), criminal liability is expanded to behaviours that are not harmful.[25] In other cases, specifically Article 635-ter and -quinquies, the offences are vague, and from their penalties and collocation in the Penal Code it is not clear which penal law policy the legislator has pursued.[26] (See Table 1.)

B. The Polish Penal Law System

There are three milestones in the history of Polish legislation regarding offences connected with computers or their networks – in 1997, 2004, and in 2017. Twelve types of behaviour were criminalized for the first time in the 1997 Polish Penal Code[27] (see Table 2). They included behaviours aimed not only against confidentiality, integrity, and availability of computer data, but also state interest, public safety, sexual freedom and decency, credibility of documents, and property. The introduction of computer offences to the penal code might be considered as a 'revolution' in the Polish penal law system in those times.

Table 1. The timetable of changes to the Italian Penal Code (IPC) regarding cybercrimes

Article of IPC	L. 191/78	L. 547/1993	L. 269/1998	L. 48/2008	L. 172/2012	D.L. 93/2013	D.L. 7/2015	D.LGS. 7/2016	L. 69/2019
270-quinquies, § 2[1]							C		
392, § 3[2]		E							
420[3]	N	A		AB					
491-bis[4]		N		A				A	
495-bis[5]				N					
600-ter[6]			N						
600-quater[7]			N						
600-undecies[8]					N				
612-bis, co. 2[9]						C			
612-ter[10]									N
615-ter[11]		N							
615-quater[12]		N							
615-quinquies[13]		N		A					
616, § 4[14]		E							
617-quater[15]		N							

25 *Ibidem*, p. 710.

26 *Ibidem*, p. 714ff.

27 This has been in force since 1 September 1998 (Official Journal of the Republic of Poland (OJ) 1997.88.553).

617-quinquies[16]		N							
617-sexies[17]		N							
621, § 2[18]		E							
635-bis[19]		N		A				A	
635-ter[20]				N				A	
635-quater[21]				N				A	
635-quinquies[22]				N				A	
640-ter[23]		N				A			
640-quinquies[24]				N					

Key: N (new offence); A (amended); C (new aggravating circumstance added to an existing offence); E (expanding the scope of a 'traditional' offence); AB (abolished).

Source: Authors' own study.

1. 'Training for terrorism-oriented activities', Offences against the State.
2. 'Arbitrary exercise of one's rights with violence to objects', Offences against justice.
3. 'Attack against public utility structures', Offences against public order.
4. 'Forgery of digital documents', Offences against public faith.
5. 'False communication of information about one's or another's identity of personal qualities to the certifier of digital signatures', Offences against public faith.
6. 'Child-abuse pornography', Offences against the person.
7. 'Disposal of child-abuse contents', Offences against the person.
8. 'Child grooming', Offences against the person.
9. 'Stalking', Offences against the person.
10. 'Revenge porn', Offences against the person.
11. 'Illegal access to a cyber system', Offences against the person.
12. 'Unlawful disposal or provision of access codes', Offences against the person.
13. 'Unlawful provision of malicious computer programs', Offences against the person.
14. 'Violation, theft and destruction of correspondence', Offences against the person.
15. 'Unlawful interception, obstruction or interruption of cyber communication', Offences against the person.
16. 'Installment of devices aimed at intercepting, obstructing or interrupting cyber communication', Offences against the person.
17. 'Falsification, forgery or destruction of cyber communication contents', Offences against the person.
18. 'Disclosure of secret documents' contents', Offences against the person.
19. 'Damage to computer information, data and programs', Offences against property.
20. 'Damage to computer information, data and programs used by the State or a public utility', Offences against property.
21. 'Damage to computer systems', Offences against property.
22. 'Damage to computer systems of a public utility', Offences against property.
23. 'Cyberfraud', Offences against property.
24. 'Cyberfraud committed by a person who gives electronic signature certification services', Offences against property.

This brief description indicates that the development of Polish computer criminal law has not evolved in line with the progress of technology and its dissemination worldwide. Polish legislation had to catch up relatively quickly in terms of its legal

penal response to manifestations of the pathological use of computers and, later on, networks. This is different from the Italian legislation described earlier, which has a much longer history in this respect.

For this reason, so far there are only cases of creating new types of offences or updating the descriptions of the constituent elements of an offence in the Polish Penal Code. These are described in Table 2 as N (new offences) or A (amended). There are no cases described above in relation to changes in Italian penal law, such as a new aggravating circumstance added to an existing offence, expanding the scope of a 'traditional' offence, or abolished offences.

More types of offences were then introduced to the Polish penal law system: two in 2004 and one in 2008. The second milestone was not only about introducing new types of offences; the changes introduced lead to the conclusion that criminalization went beyond computer offences to encompass the already-developing Internet and the pathological behaviours emerging along with it. The following examples of the 2004 amendments to the constituent elements of offences can be pointed out:

- 'entering a computer network' was changed to 'entering an information system';
- 'transmission of information' was changed to 'transmission of computer data';
- 'change of record' or 'change of information' was changed to 'computer data';
- 'transmission of information' was changed to 'transfer of computer data';
- 'recording on a computer storage medium' was changed to 'recording of computer data'.

There is an evident shift away from computers strictly as devices towards broadening the scope of criminalization to include behaviour related to their networks: local or wide area networks. This process has also affected the information entered, processed, and accessed in these systems This change in the constituent elements of the offences was intended to broaden the concept of computer data.. This trend was confirmed with the subsequent 2008 amendments. Attention was drawn to security breaches (also in the sense of software, not merely hardware) in telecommunications networks, and the computer storage medium was changed to a recording of computer data.

Table 2. The timetable of changes to the Polish Penal Code (PPC) regarding cybercrimes

Article of PPC	1998	2004[25]	2005	2008	2014	2017
130 § 3[26]	N	A				
165 § 1, item 4[27]	N	A				
202 § 3[28]	N	A	A		A	

267[29]	N			A		
268[30]	N			A		
268a[31]		N				
269[32]	N	A		A		
269a[33]		N				A
269b[34]		N				A
270 § 1[35]	N					
278 § 2[36]	N					
278 § 5[37]	N					
285 § 1[38]	N					
287[39]	N	A				
293[40]	N					

Key: N (new offence); A (amended).
Source: Authors' own study.

25. OJ 2004.69.626.
26. 'Computer espionage', Offences against the Republic of Poland.
27. 'Causing danger by interfering with, obstructing or otherwise affecting automatic processing, storage or transmission of computer data', Offences against public safety.
28. 'Production, recording or importing, storing or possessing with a view to distribution, or distribution or presentation of pornographic content with the participation of a minor, or pornographic content involving the display of violence or the use of an animal', Offences against sexual freedom and decency.
29. 'Obtaining information unlawfully', Offences against information protection.
30. 'Obstructing access to information', Offences against information protection.
31. 'Destruction of information in databases', Offences against information protection.
32. 'Damaging computer data of special importance to the country', Offences against information protection.
33. 'Interference with the operation of an IT or data communications system or network', Offences against information protection.
34. 'Unlawful production, acquisition, disposal or provision of malicious computer programs', Offences against information protection.
35. 'Forgery of digital documents', Offences against the credibility of documents.
36. 'Theft of a computer program', Offences against property.
37. 'Theft of an ATM card', Offences against property.
38. 'Telecommunication fraud', Offences against property.
39. 'Computer fraud', Offences against property.
40. 'Obtaining stolen software', Offences against property.

The most recent amendments, of 2017, are the separation of systems from 'computer' to 'IT' and 'ICT'. In the explanatory memorandum to this amendment, we can find the explicit statement that 'the term "computer system" does not correspond to modern IT or ICT reality and raises interpretation doubts'. However, the amendments introduced have led to more interpretation problems. The concepts of telecommunication networks and systems are semantically similar. Although they have not been defined in the Penal Code, this has been done in other laws. According to the principles of interpretation, the same meaning should be given to the concepts, especially since they are legal definitions in such legal acts as the Act of 2002 on the provision of electronic services,[28] the Act of 2005 on the computerization of the activities of entities performing public tasks,[29] and the Act of 2004 – Telecommunications Law.[30] This renders some articles unnecessary, for example Article 268(a) of the PPC, which falls within the scope of Article 269(a) of the PPC.[31]

There are two basic problems in the case of Polish penal regulations, and they both concern the issue of assigning meaning to the constituent elements of the offences. The first relates to their 'extension' to new behaviours. The second problem is the issue of ensuring the consistency of their meaning in the context of the entire Polish legal system.

3. Final notes

The changes relating to the adaptation of penal law to developing IT technologies started much earlier in Italy than in Poland. In the former case, the first intervention dated back to 1978, in the latter case to 1997. The gradual evolution of Italian legislation has gone in two directions: expanding the scope of 'traditional' offences and creating entirely new ones. The latter direction was the one that was taken up by Polish legislation. It has taken advantage of a new penal code to introduce completely new types of offence, instead of updating or amending the traditional ones. Another consequence is that the types of offences in Italian law are far more numerous and have a more dispersed and detailed character. In the case of Polish law, the offences related to cybercrime are fewer, and they have been constructed using descriptions

28 OJ 2020.344.

29 OJ 2020.346

30 OJ 2019.2460.

31 A. Lach, Komentarz do art. 269a (in:) V. Konarska-Wrzosek (ed.), Kodeks karny. Komentarz, wyd. III, Warsaw 2020 – https://sip.lex.pl/#/commentary/587715949/630826/konarska-wrzosek-violetta-red-kodeks-karny-komentarz-wyd-iii?cm=URELATIONS; W. Wróbel and D. Zając, Komentarz do art. 269a (in:), W. Wróbel and A. Zoll (eds.), Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. 212–277d, Warsaw 2017 – https://sip.lex.pl/#/commentary/587746553/543993/wrobel-wlodzimierz-red-zoll-andrzej-red-kodeks-karny-czesc-szczegolna-tom-ii-czesc-ii-komentarz...?cm=URELATIONS.

which are more general in semantical scope. Nevertheless, both legislative bodies have problems in adjusting the descriptions of offences to the ongoing IT revolution. This is an example of the common perception that the law has not kept up with technological progress, which criminals are attempting to abuse.

Considering the constant evolution of IT and the experience of these two countries in criminalizing cybercrime, in our opinion the legislative bodies should pay attention to some elements for future amendments to the law: firstly, it is necessary to better understand cyberspace and its nature; secondly, it would be useful to rethink some of the traditional categories of penal law in the light of the new technologies; finally, it would be wise to adopt a more international approach in order to harmonize different legislations and foster international cooperation.

REFERENCES

2020 Global Networking Trends Report, CISCO – https://www.cisco.com/c/dam/m/en_us/solutions/enterprise-networks/networking-report/files/GLBL-ENG_NB-06_0_NA_RPT_PDF_MOFU-no-NetworkingTrendsReport-NB_rpten018612_5.pdf.

Adamski A., Przestępczość w cyberprzestrzeni. Prawne środki przeciw działania zjawisku w Polsce na tle projektu konwencji Rady Europy, Toruń 2001.

Benjamin V., Samtani S. and Chen H., Conducting large-scale analyses of underground hacker communities, (in:) T.J. Holt (ed.), Cybercrime Through an Interdisciplinary Lens, Abingdon 2017.

Flor R., Cyber-criminality: le fonti internazionali ed europee, (in:) A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), Trattato di Diritto penale – Cybercrime, Milan 2019.

Flor R., La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative, (in:) A. Cadoppi, S. Canestrari, A. Manna and M. Papa (eds.), Trattato di Diritto penale – Cybercrime, Milan 2019.

Flor R., Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet, (in:) Diritto penale contemporaneo, 20 settembre 2012.

Grabosky P., Electronic crime, New Jersey 2007.

Grabosky P., Virtual Criminality: Old Wine in New Bottles? „Social & Legal Studies" 2001, no. 2.

Grzelak M. and Liedel K., Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, „Bezpieczeństwo Narodowe" 2012, no. 22.

Kasprzak W.A., Ślady cyfrowe. Studium prawno-kryminalistyczne, Warsaw 2015.

Kwiatkowska E.M., Development of the Internet of Things - opportunities and threats, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, vol. 3, no. 8.

Lach A., Komentarz do art. 269a, (in:) V. Konarska-Wrzosek (ed.), Kodeks karny. Komentarz, wyd. III, Warsaw 2020 – https://sip.lex.pl/#/commentary/587715949/630826/konarska-wrzosek-violetta-red-kodeks-karny-komentarz-wyd-iii?cm=URELATIONS.

Lakomy M., Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice 2015.

Pecorella C., Reati informatici, (in:) Enciclopedia del diritto - annali, Milan 2017.

Picotti L., Diritto penale e tecnologie informatiche: una visione d'insieme, (in:) A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), Trattato di Diritto penale – Cybercrime, Milan 2019.

Picotti L., La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale, "Diritto penale e processo" 2008, no. 6.

Pudełko M., Prawdziwa Historia Internetu, Piekary Śląskie 2013.

Wróbel W. and Zając D., Komentarz do art. 269a, (in:), W. Wróbel and A. Zoll (eds.), Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. 212–277d, Warsaw 2017 – https://sip.lex.pl/#/commentary/587746553/543993/wrobel-wlodzimierz-red-zoll-andrzej-red-kodeks-karny-czesc-szczegolna-tom-ii-czesc-ii-komentarz...?cm=URELATIONS.