NOWA KODYFIKACJA PRAWA KARNEGO. Tom XLVII
AUWr No 3839 Wrocław 2018

DOI: 10.19195/2084-5065.47.7

International co-operation in combating cybercrime. Selected issues

Rafał Cieśla

Department of Forensic Sciences
Faculty of Law, Administration, and Economics
University of Wroclaw, Poland

Acquisition of evidence in cases of Internet crime within the context of online banking has changed the attitude of judicial bodies. Online declaration of will, constituting the basis of online banking, has been causing an increasing number of problems in detecting crime, and has thus resulted in the necessity to undertake new forensic measures in acquiring evidence. For years, whatever happened in banks left material traces constituting potential evidence. Both a client and a bank clerk filled in documents authorising particular activities in handwriting. Documents displayed various characteristic features, such as signatures, handwritten inscriptions, seals, etc., and were frequently secured in a secret way, specific for a bank that issued them. All of these lent themselves to forensic examination of handwriting and technical examination of documents, which might result in detecting a forgery. In a situation when doubts arose concerning the authenticity of a document, it was possible to reconstruct the circulation of banking documents drawn by bank clerks performing individual operations. To this end, samples of handwriting and seals were compared and when this did not suffice, forensic examination methods were applied. Identification was based on the basic premise

that handwriting and signatures display numerous individual characteristics, such as the shape of letters, variable pressure applied during writing, links between letters, rate, dynamics, and shading of writing as well as proportions between letters — inseparably tied with a person's individual features, which enables the determining of a connection between a document's content and its author. Proving or disproving the connection between a person and a particular document resulted in the presumption that a particular declaration of will was (or was not) drawn by a particular person.[1]

The emergence of online access to banking and electronic records of information considerably hindered acquisition of evidence enabling identification of a person responsible for a particular instance of online record. Identification of a particular electronic device used in an online transaction is usually a minor problem in forensic examination; it is the identification of a particular person who is responsible for its use that is practically impossible. Hearing of evidence may only demonstrate the connection between the consequences of an act and a device used in its execution, while it is a human being who is subject to criminal responsibility. A crucial element in the proceedings aiming at an identification of a perpetrator and proving his or her guilt is the fact that the perpetrator was not physically present in the place where the crime was committed. Perpetrators may be in another country, if not a continent, without

[1] Cf. Z. Czeczot, *Badania identyfikacyjne pisma ręcznego*, Warszawa 1977; *Zagadnienia dowodu z ekspertyzy pisma ręcznego*, ed. R. Cieśla, Wrocław 2017; R. Broadhurst, "Development in the global law enforcement of cyber-crime", *An International Journal of Police Strategies and Management* 29, 2006, issue 3, pp. 408–433; R. Jaworski, *Wykrywanie przestępstw popełnianych w bankowości elektronicznej (problematyka dowodowa)*, Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej Wydziału Prawa Administracji i Ekonomii Uniwersytetu Wrocławskiego, *e-Biuletyn* 3, 2004, p. 3; K. Archick, *CRS Report for Congress, Cybercrime: The Council of Europe Convention*, www.iwar.org.uk/news-archive/crs/10088.pdf (access: 10.03.2018); *Cybercrime Law*, ed. A. Arnes et al., www.onlinelibrary.wiley.com/doi/abs/10.1002/9781119262442.ch3 (access: 12.03.2018); M. Owoc, *Kryminalistyczna ekspertyza sfałszowanych dokumentów atramentowych*, Poznań 1968; R. Cieśla, *Technical Examination of Documents. Within the Scope of Polish Evidence Law*, Wrocław 2006; Z. Kegel, *Dowód z ekspertyzy pismoznawczej w polskim procesie karnym*, Wrocław 1973; M. Leśniak, *Wartość dowodowa opinii pismoznawczej*, Pińczów 2011; M. Goc, *Współczesny model ekspertyzy pismoznawczej — wykorzystanie nowych metod i technik badawczych*, Warszawa 2015.

physical contact with a victim, which thus does not constitute a source of evidence. A victim may only confirm that he or she never declared his or her will while executing a particular transaction. Electronic evidence is the piece of information stored or transferred online, i.e., what is stored on an electronic carrier of information, e.g., a computer's hard drive, the memory of a telephone or another mobile device. It may also be a computer-generated document employing a word processing programme, photographs and digital data confirming the history of logging in from a particular address to a particular server. The most important feature of electronic evidence is the ease with which it may be modified, stored, and duplicated, as well as its circumstantial character enabling identification of solely the perpetrator's knowledge and not his or her identity. A signature under a document or the data in the document's heading do not lead to the identification of the author; the electronic data do not indicate the person who used a device at that particular moment.[2] The specific nature of crime concerning online banking consists in a physical distance between a perpetrator and the consequences of his or her criminal act. In practice a crime may be committed in one country, which consists in breaking electronic security measures and illegal copying a magnetic strip of a card used in an ATM, thus acquiring its PIN, with the use of such devices as card readers and miniature cameras illegally fixed in an ATM or even mobile phone cameras. The data are transferred online to a recipient who resides in another country, where a crime is committed, i.e., counterfeiting of a payment card consisting in copying the content

[2] Polish law has no legal (i.e., official) definition of electronic evidence (both the Code of Penal Procedure and the Code of Civil Procedure). According to the opinion of the Ministry of Justice of 30 March 2009 no. 7857 electronic evidence may be interpreted in two ways: as documents on the basis of art. 115 § 14 Penal Code ("a document is any object or any information stored on a recording medium of legal significance or which due to its content constitutes the evidence of law, legal relation, or a circumstance of legal significance") or as "other" evidence, which due to its nature escapes the traditional division into material or personal evidence, www.infor.pl (access: 2.04.2018). Cf. G. Nauka, "Dowody elektroniczne w postępowaniu karnym (Warsaw, 12.03.2008)", *Prokuratura i Prawo* 7–8, 2008, pp. 250–255; A. Lach, "Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia praktyczne i teoretyczne", *e-biuletyn — CBKE* 2004, no. 2, www.biblitekacyfrowa.pl/dlibra/publication/16958/edition/24720/content?ref=desc (access: 2.04.2018).

of the original card's magnetic strip onto another.[3] As a result a crime is committed in the territory of another country, where physical presence of the actual perpetrator is not necessary. The perpetrator can remotely activate a programme, which will, e.g., introduce an infected programme into another user's systems with the aim of acquiring the data enabling access to bank accounts, such as passwords or authorisation codes. In such a case a perpetrator will not leave any forensic traces at the place where the crime has been committed.[4] Cybercrime is committed globally and is not restricted territorially; access to the Internet generates so-called trans-border crime, which causes additional problems for the police, resulting from differences in legal systems in various countries (this situation necessitates international co-operation between law enforcement bodies).[5]

The problem of international co-operation between the authorised bodies from various countries, comprising the introduction of special procedures of detecting and prosecuting perpetrators and collecting evidence as well as exchange of information, was partially solved in the Council of Europe's Convention on Cybercrime of 23rd November 2001.[6] This legal act aims at introducing universal measures for preventing and combating widely-understood cybercrime into the legal systems of individual countries. Theoretically, such a universal approach should facilitate international, frequently necessary, co-operation in this area, as one country on its own as a rule has no chance of effectively combating cybercrime of an inter-

[3] R. Kaszubski, Ł. Obzejta, *Karty płatnicze w Polsce*, Warszawa 2012, p. 32 ff.

[4] B. Hołyst, *Kryminalistyka*, Warszawa 2018, pp. 383–702; *Ekspertyza sądowa. Zagadnienia wybrane*, ed. M. Kała, D. Wilk, J. Wójcikiewicz, Warszawa 2017, pp. 552–598.

[5] Cf. A. Kanciak, "Problematyka cyberprzestępczości w Unii Europejskiej", *Przegląd Bezpieczeństwa Wewnętrznego* 2013, no. 8 (5), pp. 109–120; J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015; M. Macieja, *Bezpieczeństwo finansowe w bankowości elektronicznej ze szczególnym uwzględnieniem zjawiska phishingu*, Wrocław 2015, p. 20 ff.; *Bezpieczeństwo finansowe w bankowości elektronicznej*, ed. M. Górnisiewicz, M. Pstruś, R. Obczyński, Warszawa 2014; *Prawne i społeczne aspekty cyberbezpieczeństwa*, ed. S. Gwoździewicz, K. Tomaszycki, Warszawa 2017.

[6] Official Gazette (Dziennik Ustaw) of 2015, point 728 and 729; The Government Statement of 2 April 2015 on the binding power of the Council of Europe's Convention on Cybercrime drawn in Budapest on 23 November 2001; Act of 12 September 2014 on ratification of the Council of Europe's Convention on Cybercrime drawn in Budapest on 23 November 2001, point 1514.

national dimension. The convention defines the features of Internet crime and the procedures of dealing with it, which the parties to the Convention should implement in their legal systems. The convention is amended by the protocol which specifies racist and xenophobic acts committed with the use of computer systems which should be penalised by the countries — parties to the Convention. The Convention is to benefit the countries with the possibility of international co-operation in combating cybercrime and penalising the perpetrators of such crimes, independently of the fact whether it is penalised in the place where it was committed. A perpetrator committing a cybercrime leaves no traditional evidence that might help identify him or her, i.e., handwriting,[7] biological traces,[8] dactyloscopic traces,[9] DNA,[10] mechanoscopic[11] and osmological[12] traces and — consequently — the perpetrator's individual features are absent. Use of the Internet is by no means anonymous, at least in terms of identification of the device used in committing the crime or a place where the perpetrator was at that time. The device may be identified thanks to the IP address, assigned to every piece of equipment with access to the Internet; the address is not permanent, but it is assigned each time when the Internet is accessed. The individual character of the address, together with precise date and time of the access, enables identification of the device. Determining its location enables determining the place of perpetration; it is also the grounds for verifying the information concerning particular webpages accessed at a particular time or determining the content of transferred files.[13]

The modus operandi of the perpetrators of cybercrime consists in creating a bank's fake webpage and rerouting money transfers and payments

[7] Z. Czeczot, op. cit., Warszawa 1973; *Ekspertyza sądowa. Zagadnienia wybrane*, pp. 552–571; *Znaczenie aktualnych metod badań dokumentów w dowodzeniu sądowym*, ed. Z. Kegel, R. Cieśla, Wrocław 2012; *Zagadnienia dowodu z ekspertyzy dokumentów*, ed. R. Cieśla, Wrocław 2017.

[8] *Ekspertyza sądowa. Zagadnienia wybrane*, pp. 230–233, B. Hołyst, op. cit., pp. 450–511.

[9] *Ekspertyza sądowa. Zagadnienia wybrane*, pp. 46–88.

[10] Ibidem, pp. 229–258.

[11] Ibidem, pp. 318–327; B. Hołyst, op. cit., pp. 684–697.

[12] R. Zdybel, *Osmologia — Dowody zapachowe w kryminalistyce*, Przemyśl 2009; see also www.osmologia.wortale.net (access: 10.03.2018).

[13] M. Macieja, op. cit., p. 20 ff.

into other bank accounts or intercepting data of bank accounts during online sessions. It requires special knowledge and qualifications in IT, knowledge of computer programmes and — especially — their weak points, providing an opportunity to exploit their gaps and errors. These, as well as perpetrators' exceptional motivation and premises for committing cybercrime may be helpful for law enforcement bodies to profile a narrow circle of possible perpetrators. The features of electronic evidence indicated above determine the way of conducting evidence proceedings. The first essential element is the participation of experts with their specialist knowledge of equipment, computer systems, and information technology in finding and collecting electronic evidence. Any necessary action should be taken immediately because electronic evidence may be deleted at any moment. Additionally, it should be remembered that cybercrime utilises programmes with an embedded procedure of self-destruction, which sets off automatically after their destructive task has been accomplished. Apart from indicating weak points of electronic evidence, its advantages need to be emphasised, which undoubtedly includes the fact that it cannot be completely deleted without leaving any traces on an electronic date carrier. Retrieving information is possible with the use of specially dedicated computer programmes, which enable retrieving lost or deleted data, files, or folders. Routine deletion of data is not tantamount to their immediate destruction; it merely results in the loss of an access path to the data in question.[14] This is a situation contrary to what for years was characteristic of classic documents, when they were drawn on paper with the use of various pens or printing appliances. In such cases frequently crude methods of mechanical or chemical deletion of text were used to remove unwanted content. When such methods are implemented, if a document had not been completely destroyed, entirely different examination methods have been used to reveal deleted content.[15]

International co-operation of law enforcement bodies in combating cybercrime, including crime against online banking, is indispensable.[16] It is necessitated by the constantly increasing level of crime perpetrated not

[14] Ibidem.

[15] Physical-optical and physical-chemical methods.

[16] Co-operation within the EU. Combating organised crime and combating terrorism, www.mswia.gov.pl (access: 10.03.2018); Convention on cybercrime, www. bip.ms.pl (access: 10.03.2018).

only by individual persons but also by organised criminal groups. Within recent decades information and communication technology have become so significant that it constitutes the foundations of economic growth and strategic resource for the functioning of all sectors of the economy. Security of information systems is becoming a priority for financial institutions and state bodies. Due to the specific nature of the area where it occurs, an increasing number of instances of cybercrime is inseparably connected with the issue of trans-border traffic, which in turn has resulted in the need to initiate and develop co-operation in combating cybercrime at an international level. Apart from the Convention mentioned above, another important legal act of European significance regulating co-operation of law enforcement bodies in combating cybercrime is the Communication from the Commission to the European Parliament, the Council and the Committee of the Regions of 22nd May 2007.[17] The strategy's most important premises include better and more effective co-operation of law enforcement bodies, which resulted in creating a central EU contact point for information exchange about cybercrime, increasing financial support for the initiatives aimed at training law enforcement bodies in combating cybercrime, assisting public authorities in undertaking effective measures in combating the phenomenon in question and assigning appropriate means for that purpose, supporting research assisting combating cybercrime in cyberspace, participating in global international co-operation in combating cybercrime, undertaking initiatives to encourage all member states and third countries to ratify the Convention of the Council of Europe on cybercrime, initiating efforts in co-operation with member states to prevent and combat coordinated large-scale attacks against national IT infrastructure.[18]

An essential element of co-operation is the initiatives undertaken under the auspices of international institutions appointed to combat organised crime.[19] In August 2007 Europol issued a document "High Tech Crimes within the EU: Old Crimes New Tools, New Crimes New Tools.

[17] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions — Towards a general policy on the fight against cybercrime, http://eur-lex.europa.eu (access: 5.12.2017).

[18] www.eur-lex.europa.eu (access: 10.01.2018). Cf. M. Macieja, op. cit., p. 20 ff.

[19] Europol (European Police Office); Eurojust, Frontex.

Threat Assessment 2007",[20] which formulated recommendations concerning, e.g., increased information exchange in order to intensify co-operation between investigative bodies of the member states dealing with combating cybercrime, educating Internet users in the use of technology or ratifying the Council of Europe's Convention on Cybercrime of 2001 by states so that it will become the most important common legal platform for combating cybercrime. A significant achievement in combating cybercrime is the appointment of the European Cybercrime Centre at Europol,[21] whose main objective is combating organised crime in the Internet involving serious and organised cybercrime. The Centre focuses on supporting and coordinating operations and investigations carried out by law enforcement bodies of the member states in several areas. The Council of Europe's Convention on Cybercrime,[22] mentioned a few times above, constitutes a legal instrument which is to serve the purpose of combating Internet crime in its international scope. High effectiveness of the activities undertaken following the Convention's premises primarily results from the fact that it was signed by the United States, all the member states of the European Union and states from outside Europe. Another instrument of great significance in international co-operation of law enforcement bodies is the statement from the meeting of the G8 justice and interior ministers held in 1997 in Washington, which created a network of contact points in combating cyber-crime,[23] enabling quick transfer of information concerning crime in cyberspace or in cases requiring urgent assistance of law enforcement bodies.[24] On 25th June 2001 the Council of the European Union recommended that member states establish 24/7 High Tech Contact Points. The points should receive the requests from member states at any time of day and night all week and process them accordingly. Concurrently, they enable a member state to ask other states for appropriate assistance. Another institution which plays a significant international role in combating crime, including cybercrime, is Inter-

[20] www.europol.int (access: 25.02.2018).
[21] www.europa.eu (access: 10.02.2018).
[22] http://prawo.vagla.pl/node/1493 (access: 10.01.2018).
[23] G8 24/7 High Tech Contact Points.
[24] www.secure.edu.pl (access: 10.02.2018).

pol.[25] This international police organisation was established to combat all types of crime. Since 2002 its general secretariat in Lyon offers the central contact point for every national central bureau in each country with the aim of providing assistance and information concerning ongoing trans-border investigations. Interpol working parties in IT crime[26] have been formed to support the development of strategies, technologies, and data gathering on the latest methods used in cybercrime. The groups have been formed in Asia, in the Southern Pacific, in both Americas, Africa, Europe, the Middle East, and in North Africa. The European Interpol working party on IT crime has adopted the following tasks: co-operation, knowledge, and practical experience exchange, searching for solutions concerning threats present in the Internet, formulating recommendations for Interpol member states, promoting standardisation of the employed methods, procedures, training programmes and co-operation with other international organisations, establishing good practices and guidelines for the investigators of cyber-crime.[27]

A good example of a phenomenon necessitating indispensable international co-operation in combating cybercrime is phishing,[28] known for many years. Due to its complexity phishing constitutes an exceptional challenge for modern-day banking. Even though it is not a new phenomenon, it transforms continually due to the ongoing progress of IT technology. Even the very issue of defining phishing as an illegal act causes numerous doubts and problems because as such the phenomenon is not directly regulated

[25] www.interpol.int (access: 17.01.2018).

[26] www.interpol.int (access: 17.01.2018).

[27] www.secure.edu.pl (access: 2.04.2018).

[28] Phishing — fraud in which a perpetrator impersonates another person or institution to obtain information under false pretences (e.g., logging-in data, details of a credit card) or to coerce a victim into performing certain activities. It is an attack based on social engineering, www.wikipedia.org/phishing (access: 23.02.2018); Cf. L. James, *Phishing Exposed*, Rockland 2006, p. 10 ff.; *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, ed. M. Jakobsson, S. Myers, Wiley 2006, p. 2 ff.; K. Mikołajczyk, "Przestępstwa związane z wykorzystaniem bankowości elektronicznej — skimming", *Przegląd Bezpieczeństwa Wewnętrznego* 2014, no. 10, p. 108; J. Kosiński, "Phishing i ransomware", *Człowiek i Dokumenty* 2018, no. 48, pp. 21–22.

in Polish law.[29] The characteristic feature of phishing is the fact that it involves very precise and long-lasting preparation before attacking a selected victim. There are many types of phishing; beginning with its traditional form, consisting in sending e-mails from people impersonating a bank or a trustworthy institution, asking to log-in on a webpage whose address is included in the e-mail, to more sophisticated forms, such as pharming. The fact that phishing constitutes the first, albeit the most important, step in illegal acquisition of financial means is very important for the banking sector. Phishers aim at acquiring data enabling their further use to acquire financial means. Obviously, criminals resort to increasingly more effective methods, ever more difficult to identify — beginning with very simple methods of manipulation to sophisticated and highly specialised computer programmes. The specific nature of phishing consists in the fact that quite frequently it is very difficult to reach the perpetrator. Additionally, crime of this type involves specialised and organised international criminal groups. The fact mentioned earlier that the crime is perpetrated with the use of the Internet causes an additional problem in identifying a perpetrator, i.e., the international character of the crime in question, which — in turn — determines the development of international co-operation in combating cybercrime. Internet crime constitutes a continually transforming threat and combating it requires not only knowledge and experience but also exchange of information and co-operation between all the interested institutions at both national and international levels.

In view of the ubiquitous globalisation processes and the resulting interdependence of states, international co-operation is the key element in providing security of global cyberspace. Accomplishing this task at the European level, Poland should continually strive to include the aspects of cybersecurity in implementing the Common Foreign and Security Policy of the European Union. Membership of the North Atlantic Treaty Organisation is the essential element ensuring Polish and Euro-Atlantic security. Intensifying hybrid warfare necessitates investment in deterrence and de-

[29] It is most frequently interpreted as fraud, according to art. 286–287, Penal Code (Penal Code of 6 June 1997, Dz.U. — Official Gazette 1997 No. 88, point 553 with subsequent amendments).

fence, including quick and effective reaction to cyber attacks.[30] Co-operating in the United Nations, Poland should support the debate on the effective system of global Web network management and the issues involving legal assessment of cyber attacks in order to formulate coherent solutions providing security of the international exchange of information on the Internet. It should also participate in strengthening the means of promoting trust and security within the existing international forums, e.g., Organisation for Security and Co-operation in Europe.[31] Equally essential is the co-operation with the countries of the region, including co-operation within the Visegrád Group and with the countries of the Baltic Sea Region.

Strengthening the Polish international position will only be possible in close co-operation between the Polish institutions and agencies responsible for providing cybersecurity, especially the minister responsible for digitisation and the minister of foreign affairs responsible for the general directions of Polish foreign policy.[32]

References

Literature

Archick K., *CRS Report for Congress. Cybercrime: The Council of Europe Convention,* www.iwar.org.uk/news-archive/crs/10088.pdf.

Bezpieczeństwo finansowe w bankowości elektronicznej, ed. M. Górnisiewicz, M. Pstruś, R. Obczyński, Warszawa 2014.

Broadhurst R., "Development in the global law enforcement of cyber-crime", *An International Journal of Police Strategies and Managment* 29, 2006, issue 3.

Cieśla R., *Technical Examination of Documents. Within the Scope of Polish Evidence Law*, Wrocław 2006.

Convention on Cybercrime, www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

[30] National Cybersecurity Policy Framework of the Republic of Poland for 2017–2022, www.gov.pl (access: 20.03.2018).

[31] Organization for Security and Co-operation in Europe, www.osce.org (access: 20.04.2018).

[32] National Cybersecurity Policy Framework of the Republic of Poland for 2017–2022, www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf (access: 20.03.2018).

Cybercrime Law, ed. A. Arnes et al., www.onlinelibrary.wiley.com/doi/abs/10.1002/9781119262442.ch3.

Czeczot Z., *Badania identyfikacyjne pisma ręcznego*, Warsaw 1977.

Ekspertyza sądowa. Zagadnienia wybrane, ed. M. Kała, D. Wilk, J. Wójcikiewicz, Warszawa 2017.

Goc M., *Współczesny model ekspertyzy pismoznawczej — wykorzystanie nowych metod i technik badawczych*, Warszawa 2015.

Hołyst B., *Kryminalistyka*, Warszawa 2018.

Jaworski R., "Wykrywanie przestępstw popełnianych w bankowości elektronicznej (problematyka dowodowa)", Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej Wydziału Prawa Administracji i Ekonomii Uniwersytetu Wrocławskiego, *e-Biuletyn* 3, 2004.

Kanciak A., "Problematyka cyberprzestępczości w Unii Europejskiej", *Przegląd Bezpieczeństwa Wewnętrznego* 2013, no. 8 (5).

Kaszubski R., Obzejta Ł., *Karty płatnicze w Polsce*, Warszawa 2012.

Kegel Z., *Dowód z ekspertyzy pismoznawczej w polskim procesie karnym*, Wrocław 1973.

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Kosiński J., "Phishing i ransomware", *Człowiek i Dokumenty* 2018, no. 48.

Lach A., "Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia praktyczne i teoretyczne", *e-biuletyn CBKE* 2004, no. 2, www.biblitekacyfrowa.pl/dlibra/publication/16958/edition/24720/content?ref=desc.

Leśniak M., *Wartość dowodowa opinii pismoznawczej*, Pińczów 2011.

Macieja M., *Bezpieczeństwo finansowe w bankowości elektronicznej ze szczególnym uwzględnieniem zjawiska phishingu*, Wrocław 2015.

Mikołajczyk K., "Przestępstwa związane z wykorzystaniem bankowości elektronicznej — *skimming*", *Przegląd Bezpieczeństwa Wewnętrznego* 2014, no. 10.

National Cybersecurity Policy Framework of the Republic of Poland for 2017–2022, www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf.

Nauka G., "Dowody elektroniczne w postępowaniu karnym", *Prokuratura i Prawo* 2008, no. 7–8.

Owoc M., *Kryminalistyczna ekspertyza sfałszowanych dokumentów atramentowych*, Poznań 1968.

Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft, ed. M. Jakobsson, S. Myers, Wiley 2006.

Polish Penal Code (Penal Code of 6 June 1997, Dz.U. — Official Gazette — 1997 no. 88, point 553 with subsequent amendments).

Prawne i społeczne aspekty cyberbezpieczeństwa, ed. S. Gwoździewicz, K. Tomaszycki, Warszawa 2017.

Zagadnienia dowodu z ekspertyzy pisma ręcznego, ed. R. Cieśla, Wrocław 2017.

Zdybel R., *Osmologia — dowody zapachowe w kryminalistyce*, Przemyśl 2009.

Znaczenie aktualnych metod badań dokumentów w dowodzeniu sądowym, ed. Z. Kegel, R. Cieśla, Wrocław 2012.

Internet sources

www.eur-lex.europa.eu.
www.europa.eu.
www.europol.int.
www.infor.pl.
www.mswia.gov.pl.
www.osce.org.
www.osmologia.wortale.net.
www.secure.edu.pl.
www.wikipedia.org/phishing.

Summary

The article discusses selected aspects of international co-operation in combating selected types of cybercrime. The complex character of criminal activity besetting contemporary banking causes numerous difficulties and poses many challenges, such as detecting and apprehending perpetrators. Online banking crime constitutes a specific category, comprising cashless transactions and electronic data processing. The specific environment of online banking, where crime is committed, determines the nature of traces left by perpetrators; it also necessitates creation of new forensic methods based on modern technology. The more sophisticated the crime, the more difficult it is to identify the perpetrators. Therefore, international co-operation in combating cybercrime is essential.

Keywords: cybercrime, international co-operation, document, electronic document, phishing.