PRAWO W DZIAŁANIU
LAW IN ACTION
36/2018
DOI: 10.32041/pwd.3607

Mariusz Nawrocki*

Cybercrime *locus* as defined now and in amendments suggested

The question of *locus delicti* is regulated in the Criminal Code[1], Art. 6(2), under which an offence is believed to be committed in the place where the perpetrator acted or failed to act or where the result – being the distinguishing characteristic of an offence – occurred or was to occur according to the perpetrator's intent. The question is rather a complex one as it is related to the institutions of substantive criminal law, as for instance the principle of territoriality (Art. 5), or a number of offence types defined in the Special Section of the Criminal Code[2]. The determination of *locus delicti* is crucial for procedural criminal law as well, because it is a major criterion for establishing the jurisdiction of the Polish State in criminal matters and designating a competent authority to conduct criminal proceedings[3].

The question of *locus delicti,* although of paramount importance, enjoys moderate interest among the authoritative juristic literature[4] and is almost non-existent in judicial decisions[5]. It appears that criminal law practice will have to deal increasingly often with offences committed with the help of the Internet and in the Internet on account of its ever greater availability and a consequently increasing social role. The Internet is no longer a mere network for exchanging information. Over the last decades, it has become a trading place (e.g. auction sites), working

* Chair of Criminal Law, Faculty of Law and Administration, Szczecin University, Poland, E-Mail: mariusz.nawrocki@usz.edu.pl

[1] Act of 6 June 1997 (consolidated text: Journal of Laws 2018, Item 1600 as amended).

[2] See: M. Nawrocki, *Miejsce popełnienia czynu zabronionego*, Warszawa 2016, pp. 45–113.

[3] M. Nawrocki, *Miejsce popełnienia*…, pp. 153–179.

[4] See: M. Nawrocki, *Miejsce popełnienia*…, *passim*; M. Nawrocki, *Przestępstwa dystansowe i tranzytowe*, *Acta Iuris Stetinensis* 2016, No. 2(14), pp. 89–104; A. Światłowski, *Miejsce popełnienia przestępstwa a odpowiedzialność karna – zarys problematyki*, „Monitor Prawniczy" 1993, No. 4, pp. 103–105; J. Warylewski, *Pornografia w Internecie – wybrane zagadnienia karnoprawne*, „Prokuratura i Prawo" 2002, No. 4, pp. 52–61; M. Sowa, *Odpowiedzialność karna sprawców przestępstw internetowych*, „Prokuratura i Prawo" 2002, No. 4, pp. 62–79; A. Błachnio, *Miejsce popełnienia czynu zabronionego przed podżegacza i pomocnika – zarys problematyki*, „Palestra" 2006, No. 7–8, pp. 82–91; B. Hołyst, *Internet jako miejsce zdarzenia*, „Prokuratura i Prawo" 2009, No. 4, pp. 5–20; R.A. Stefański, *Miejsce popełnienia przestępstwa. Problemy materialno-karne i procesowe* [in:] *Problemy wymiaru sprawiedliwości karnej. Księga Jubileuszowa Profesora Jana Skupińskiego*, A. Błachnio-Parzych, J. Jakubowska-Hara, J. Kosonoga, H. Kuczyńska (eds.), Warszawa 2013, pp. 515–526; D. Zając, *Odpowiedzialność karna za czyny popełnione za granicą*, Kraków 2017, pp. 332–345.

[5] See: judgment of CoA in Łódź of 24 January 2001, II AKa 240/01, LEX No. 84224; SC decision of 29 September 2010, IV KO 99/10, OSNwSK 2010, No. 1, Item 1827; decision of CoA in Katowice of 6 September 2017, II AKz 582/17, LEX No. 2440802 and SC decision of 17 April 2018, IV KK 296/17, LEX No. 2481975.

place (e.g. for professional computer-game players or bloggers), space for doing business (today, almost any branch of the economy is present on the Internet, if only for advertising its services or products). On the Internet, you can carry out the largest financial transactions (accessing bank accounts, exchanging traditional currencies and so-called crypto-currencies, trading in securities, immovables, collector's items or antiques). There are also huge spaces on the Internet that are used as social networking sites (e.g. Facebook, Twitter, and *Nasza Klasa,* a school-based social networking service functioning in Poland some years ago) or applications for professional data exchange (electronic mail known already for a long time, but also such applications as Messenger or WhatsApp, and *GaduGadu,* a communication app which was very popular in Poland some years ago).

The broad availability of the Internet and its widespread use in society and the economy must necessarily make it a virtual space where and with the help of which ever more often a number of offence types are committed. This, in turn, must inevitably raise legal questions. Recently, one of such questions has appeared before the Supreme Court that has ruled the Internet to be a public place[6]. The Supreme Court, in its own words, has fully agreed with the view that the Internet, although it is a virtual space, has the nature of a public place. Specifically, it ruled that in the event the Internet is used to publish an indecent announcement, inscription and/or a drawing or foul language is used on the Internet, publicly available website services, that is to say, not protected by a login and password[7], should be considered a public place within the meaning of Art. 141 of the Code of Petty Offences. The Supreme Court narrowed its arguments down to teleological considerations. It maintained

that the Code of Petty Offences has been in force for almost half a century and its provisions, including Article 141, entered into force as of 1 January 1972 when the Internet was not there yet. Of course, successive amendments made over the last one or two decades aimed at adjusting these provisions to evolving socio-economic changes. However, in the context of behaviour on the Internet, the process is not over yet due to its special character and continuing advances of computer technology. For these reasons, in the opinion of the Supreme Court, when interpreting the Code of Petty Offences, Art. 141, which has not been amended since the day it entered into force, teleological interpretation should be used to discern if it is possible to establish the meaning of specific legislative provisions, taking into account technological and civilization advances and today's needs (dynamic interpretation). The purport of the Code of Petty Offences, Art. 141, changes thus with time together with a change of the situation. Since the legislator has not amended the provision in question so far, it must be assumed that the legislator wishes it to continue in force but under new conditions, i.e. after taking into account computer science advances. In the context of Internet use, it must be noted that it certainly is a space for both doing business and presenting artistic performances, that it has its own currency and leaves no doubt as to being a space

[6] SC decision of 17 April 2018, IV KK 296/17, LEX No. 2481975; Legalis No. 1766222. The decision is also available in the database of decisions on the Supreme Court webpage: www. sn.pl

[7] See: opinion to the SC decision of 17 April 2018, IV KK 296/17.

suitable for committing an offence or a petty offence as attested actually by various acts classified in the Criminal Code and Code of Petty Offences, as appropriate.

Although this article is not devoted to the detailed discussion of the above-mentioned Supreme Court decision, it must be stressed that the position taken by the Court is not correct and its opinion is unconvincing. Suffice it to say that the Supreme Court, relying solely on reasons of a teleological nature, has completely ignored the linguistic and systemic meaning of the distinguishing characteristic 'public place', leaving it out of the discussion[8]. Nevertheless, the added value of the decision is the undeniable fact that it shows how necessary it is to regulate legally the question of the place of the commission of acts done on the Internet.

The question is in principle uncontroversial when it comes to the establishing of the place of commission of offences characterized by result, that is, acts that can be located in both the place where the perpetrator acted or the place where the criminal result occurred or – according to the perpetrator's intent – was to occur. As uncontroversial can be considered also formal (resultless) offences, the distinguishing characteristics of the causative act of which can be located in a perceivable space. Controversies do arise, however, when the act is not materially perceivable or its consequences do not share such a character either. It is here that acts committed in the virtual world, above all on the Internet, come into play.

The first thing that ought to be preliminarily decided is the meaning of the term 'Internet offences'. The task is by no means simple, because to denote this category of offences various terms are used such as computer offences, digital offences, offences perpetrated with the use of advanced technologies or cybercrimes[9]. As Hołyst writes, in the past, there were attempts made to classify cybercrimes, applying the criteria of the techniques used by offenders and the nature of committed acts. Six categories of cybercrimes were proposed:

(1) Offences made easier to commit by a computer,
(2) Offences the commission of which is made possible by a computer,
(3) Offences that cannot be committed without computer technology,
(4) Offences that can be committed in a conventional way but also with the use of the Internet,
(5) Offences that are easier to commit using the Internet, and
(6) Offences the commission of which is possible only using the Internet[10].

In the opinion of Hołyst, Internet offences include only such offences in the commission of which the Internet is used or which directly influence the provision of specific Internet services[11].

[8] The Supreme Court has offered only the linguistic interpretation of the distinguishing characteristic 'publicly' and only in relation to it did the Court refer to (very briefly as a matter of fact) a public place. It said that 'In the purely semantic sense, the word "public" means one that is happening in the place that is accessible to all, done in front of witnesses, visibly and openly (…). It follows from these senses without doubt that the public character of some action does not depend solely on the place where it happens but can follow also from certain situations'.

[9] For a broader treatment see: M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, pp. 9–21, M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, No. 7a–8, pp. 241–252; B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo" 2011, No. 1, pp. 17–19 and C. Nowak, *Wpływ procesów globalizacyjnych na polskie prawo karne*, Warszawa 2014, p. 329.

[10] B. Hołyst, *Internet*…, p. 19.

[11] B. Hołyst, *Internet*…, p. 19.

Speaking of Internet offences, the position of Adamski who suggested a definition of the term 'computer offences' is worth noting. Regarding it from the substantive law perspective, he held it to mean attacks on computer systems, data and software, as well as offences involving the use of electronic information processing systems to infringe legal interests traditionally protected by criminal law. From the procedural perspective, in turn, he defined computer offences as prohibited acts the prosecution of which requires the administration of justice authorities to gain access to information processed in computer or data-communications systems[12].

Treating of Internet offences, the Council of Europe's Convention on Cybercrime[13] undertaken in Budapest on 23 November 2001 is worth taking a closer look at. Under its Article 1, giving definitions of terms used therein, 'computer system' means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data, while 'computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function. 'Information system' has been defined in a similar way in EU law. There it means a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance[14].

Taking into account suggestions made in the authoritative juristic literature and in acts of international law, it can be assumed that cybercrimes encompass all these acts that are committed through the (broadly understood) use of an information system.

The clarifying of terminological issues does not settle the question of possible loci for committing cybercrimes. Typically, at least two solutions are possible. One, dominant in the European legal orders, has the *locus delicti,* including that of computer offences (Internet offences, cybercrimes), determined in the traditional way, i.e. following the formula that the Polish legislator employed in the Criminal Code, Art. 6(2). The other, prevailing in other legal orders, mostly in the US and in some Asian countries, refers to the location of a computer system affected by the perpetrator from abroad through a telecommunications network[15].

The question of cybercrimes is additionally complicated on account of the fact that the commission of this type of offences is not fully dependent on the perpetrator him-/herself. Hence, it falls outside the places, mentioned in the Criminal Code, Art. 6(2), where the perpetrator acted or failed to act or where the result materialized or was to materialize according to the perpetrator's intent. After all, when the perpetrator uses information systems, the transport and recording of

[12] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, pp. 30–35.
[13] Journal of Laws f 2005, Item 728; https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[14] Directive 2013/40/EU of the European Parliament and of the Counsil of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Art. 2(a) (EU Official Journal L of 14 August 2013, No. 218, p. 8).
[15] A. Adamski, *Podstawy jurysdykcji cyberprzestępstw w prawie porównawczym* [in:] *Księga pamiątkowa ku czci Profesora Jana Białocerkiewicza*, T. Jasudowicz, M. Balcerzak (eds.), Vol. II, Toruń 2009, pp. 940–941.

data is done automatically. Sometimes, the perpetrator is not even aware that the computer data he/she uses may be recorded in many unconnected places. This is so because website fragments (i.e. computer data) may be stored on various servers located anywhere in the world[16].

Moreover, it is necessary to bear in mind how illegal content is disseminated on the Internet or, in more general terms, how information is spread on the Internet. There are two technologies: push and pull. The push technology involves sending information to receivers or making it available to them (e.g. sending e-mails or posting messages on social networking sites), whereas the pull technology assumes that the web user, to access this information, must make an effort to look for it (e.g. web browsing or searching blogs)[17]. Polish criminal law theoreticians, relying on the opinions propounded in the German authoritative juristic literature, claim that only in the former case can the territory of a foreign country be considered a *locus delicti*[18]. This follows from the fact that as a *locus delicti* is also considered the place the perpetrator intended to affect – the place where he/she expected specific content to be presented. Furthermore, it seems right to maintain, at least in the light of the Criminal Code, Art. 6(2), thatpull technology may not serve as the reason for extending the concept of *locus delicti* to include the place where a web user accessed on his/her own information posted there, since the perpetrator has not disseminated the information in that place, nor made it available there. It has come into the possession of the web user only because of his/her own activity[19].

A universal access to the Internet makes illegal content easily accessible almost around the world. A universal and territorially unlimited availability of the Internet makes the location of the producer(s) and addressee(s) of this content irrelevant. Given these circumstances, the traditional connecting factor joining a territory with the perpetrator's behaviour does not work as it should. Allowing for the specific nature of cybercrimes, one can distinguish four potential types of behaviour by the perpetrator:

(1) The perpetrator is located outside Poland and affects an information system located outside Poland,
(2) The perpetrator is located outside Poland and affects an information system located inside Poland,
(3) The perpetrator is located inside Poland and affects an information system located outside Poland,
(4) The perpetrator and information system he/she affects are located inside Poland.

The Polish authoritative juristic literature has already discussed the possibility of classifying the above behaviour types in compliance with the principles of criminal liability laid down in the Criminal Code currently in force. As Sowa

[16] M. Siwicki, *Podstawy określenia jurysdykcji karnej przestępstw prasowych w Internecie*, „Przegląd Sądowy" 2013, No. 11–12, pp. 45–46. See also J. Czekalska, *Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych*, „Państwo i Prawo" 2004, Vol. 11, pp. 73–81.
[17] For a broader treatment of *push* & *pull* technology see: A. Adamski, *Podstawy jurysdykcji*..., pp. 947–948; M. Siwicki, *Podstawy określenia jurysdykcji*..., pp. 41–42.
[18] A. Adamski, *Podstawy jurysdykcji*..., p. 947; M. Siwicki, *Podstawy określenia jurysdykcji*..., p. 42.
[19] A. Adamski, *Podstawy jurysdykcji*..., p. 947.

rightly observed, the situations listed under (1) and (4) above pose no problem, because the principle of universal jurisdiction may be applied under the Criminal Code (Art. 113) in respect of the perpetrator who committed an offence outside the country by affecting an information system located outside the country as well (provided the conditions stipulated in the Code are met). The perpetrator, on the other hand, located in the country and affecting an information system located inside the country as well, will be subject to the classic grounds of criminal liability under the Criminal Code, Art. 5 and Art. 6(2)[20].

The legal situation of the perpetrator is somewhat different if he/she is located outside Poland and affects an information system located inside Poland or vice versa. In these cases, the division of offences into result-producing and resultless is crucial. The latter, with the perpetrator acting outside Poland but affecting an information system located inside the country, rule out Polish criminal jurisdiction[21]. The reason being in the opinion of Sowa that resultless (formal) Internet offences consist mostly in only recording specific content on a server supporting a given network. The recording in itself is not a result, being a distinguishing characteristic of an offence type, hence it falls outside the Criminal Code, Art. 6(2) in connection with Art. 5 thereof[22]. Sowa further suggests that the phrase 'place where the perpetrator acted', used in the Criminal Code, Art. 6(2), should be subject to an appropriate interpretation. The phrase should encompass not only the place where the perpetrator acted but also the place where the information system affected by the perpetrator is located[23]. It appears that continental criminal law rules out such a possibility on account of the breach of the principle *nullum crimen sine lege stricta* and the ban on extensive interpretation to the disadvantage of the perpetrator following from it.

It must be remembered, however, such a solution is employed in other jurisdictions, e.g. English or American. In English criminal law, offences involving tampering with information systems may also be committed by persons not holding UK citizenship and located outside the UK. The British law enforcement and administration of justice authorities have jurisdiction over such matters inasmuch as there is a 'significant link' between the committed act and the territories of England, Wales, Scotland or Northern Ireland[24]. The Anglo-American authoritative juristic literature and judicial decisions maintain that a 'significant link' is present when at the moment of offending, the perpetrator stays in his/her native country and uses a computer for specific purposes or when at the moment of offending he /she is in his/her native country and attempts to gain or gains unauthorized access to any computer containing any program or data[25]. As far as the American system is concerned, it is worth noting that US courts, with respect to offences committed through the use of a computer, refer to the location of the information system made use of for a criminal purpose. Counter-terrorist legislation is a case in point.

[20] M. Sowa, *Odpowiedzialność karna*..., pp. 73, 75.
[21] M. Sowa, *Odpowiedzialność karna*..., p. 75.
[22] M. Sowa, *Odpowiedzialność karna*..., p. 75. See also R.A. Stefański, *Miejsce*..., pp. 519–520.
[23] M. Sowa, *Odpowiedzialność karna*..., pp. 75–76.
[24] M. Siwicki, *Pojęcie locus delicti i zasady jurysdykcji karnej w ujęciu prawnoporównawczym* (part II), „Europejski Przegląd Sądowy" 2011, No. 10, pp. 27–28.
[25] M. Siwicki, *Pojęcie locus delicti*..., p. 28.

Where the perpetrator of a terrorist offence acts inside the US and where a telecommunication system or a computer system located inside the US is used to commit an offence in another country, American courts usurp the right to try the case[26].

In order to introduce a similar solution to the Polish legal system, new legislation would be necessary. The authoritative juristic literature has already offered suggestions of amending the Criminal Code, Art. 6, by adding para. 3, worded as follows: 'a prohibited act committed through the use of or against a computer system shall be considered committed in the place specified in para. 2 and also in the place where the computer system was located'[27].

A problem of this kind does not arise with result-producing offenses where the perpetrator acts abroad but affects an information system located at home. For the result, as long as it has occurred inside Poland, by virtue of the Criminal Code, Art. 6 (2) and Art. 5, locates the act at home[28].

A still different situation occurs when the perpetrator acts at home, but affects an information system located outside Poland. Under the Criminal Code, Art. 6 (2), there is no doubt that the *locus* of such an act is the place where the perpetrator acted, i.e. Poland[29]. For the same reason, the place where the information system affected by the perpetrator is located, if it is located outside Poland, is not covered by the Criminal Code, Art. 6 (2). Thus, it is inadmissible to invoke it as grounds for the jurisdiction of the Polish State in criminal matters, unless the committed act can be prosecuted under the Criminal Code, Art. 113.

To recapitulate, the law as it stands now, namely the Criminal Code, Art. 6 (2), does not fully regulate the *locus* of cybercrimes as it leaves out all the situations where the perpetrator commits a resultless Internet offence, acting from outside the country but affecting an information system located inside it. To the fact that this category of offences is a serious one attest the following examples from the Criminal Code: displaying and disseminating pornographic content (obscenity offences) (Art. 200(3), Art. 200(5), Art. 202(1)), sexually accosting a minor (Art. 200a(1 & 2)), publicly promoting or approving of paedophile behaviour (Art. 200b), libelling (Art. 212(2)), abusing in mass media (Art. 216(2)), publicly abetting a fiscal misdemeanour and/or offence (Art. 255(1)), publicly abetting a felony (Art. 255(2)), disseminating and/or publicly presenting content that may facilitate the commission of a terrorist offence (Art. 255a(1)), participating intraining that may enable a person to commit a terrorist offence for the purpose of committing such an offence (Art. 255a(2)), publicly promoting a totalitarian political system and/or inciting national, ethnic, racial or denominational hatred or one on

[26] M. Siwicki, *Pojęcie locus delicti*…, p. 30. See also A. Adamski, *Podstawy jurysdykcji*…, p. 956.
[27] M. Sowa, *Odpowiedzialność karna*…, p. 76.
[28] M. Nawrocki, *Miejsce popełnienia*…, p. 103.
[29] A similar opinion is expressed by Siwicki, who writes: 'In the case of offences related to the information content, the criminal statute of the country where it has been posted in a telecommunication network or a computer system should be given precedence in terms of applicability. (…) Internet users should be expected to comply at least with the law of the place where they act'. M. Siwicki, *Podstawy określenia jurysdykcji cyberprzestępstw na gruncie polskiego ustawodawstwa karnego w świetle międzynarodowych standardów normatywnych*, "Palestra" 2013, No. 3–4, pp. 107–108. Not without reason, either, is the view that a result-producing computer offence is (if only potentially) committed in all places where the result of a given prohibited act occurred or was to occur according to the perpetrator's intent – see J. Giezek [in:] *Kodeks karny. Część ogólna. Komentarz*, J. Giezek, N. Kłączyńska, G. Łabuda (eds.), Warszawa 2012, p. 50; R.A. Stefański, *Miejsce*…, p. 520.

account of a non-denominational status (Art. 256(1)), publicly abusing a group of people or a person on account of their national, ethnic, racial and denominational affiliation or on account of their non-denominational status (Art. 257), making available to other people computer programs or devices adapted to the commission of offences specified in Art. 165 (1)(4), Art. 267(3), Art. 268a(1) or (2) in connection with para. 1, Art. 269(1) or (2),or Art. 269a, as well computer passwords, access codes or other data enabling unauthorized access to information stored in an information system, data communication system or a data communication network (Art. 269b(1)).

The above considerations prompt this author to formulate at least one suggestion for an amendment to the law. This involves the extension of the Criminal Code formula of *locus delicti* used in Art. 6(2). The technological progress of today calls for such a definition of *corpus delicti* that would cover Internet offences (cybercrimes).

In reliance on the above discussion, Art. 6(2) may be amended as appropriate or Art. 6(3) may be added to the Criminal Code. An amended wording of Art. 6(2) could read as follows: 'An offence is believed to be committed in the place where the perpetrator acted or failed to act or where the result being the distinguishing characteristic of an offence occurred or was to occur according to the perpetrator's intent. As the place of offence commission shall be also considered the place where the information system affected by the perpetrator or one that served the perpetrator to commit an offence was located'. Alternatively, the second sentence of this provision could be placed in a separate textual unit as Art. 6(3): 'As the place of offence commission shall be also considered the place where the information system affected by the perpetrator or one that served the perpetrator to commit an offence was located'.

It is also possible to apply an analogous solution to that used in Art. 115(15), namely: 'As defined herein, as the place of offence commission shall be also considered the place where the information system affected by the perpetrator or one that served the perpetrator to commit an offence was located'. This provision could be introduced to the Criminal Code either as Art. 6(3) or one of the definitions in Art. 115 thereof. It seems that it would be necessary to have the Criminal Code define the concept of 'computer/information system', following the model of the Council of Europe Convention on Cybercrime or the DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. It also appears that to avoid interpretation problems it would be necessary to reformulate the distinguishing characteristics of several types of prohibited acts in which the legislator has alternatively used such terms as: information system, data communication system, data communication network (Criminal Code, Art. 269a, Art. 269b, Art. 269c).

The suggested extension of the *locus delicti* definition describes another two locations that determine the place of commission of cybercrimes. One is the place where the information system affected by the perpetrator was located, while the other is the place where the information system used by the perpetrator to commit a prohibited act was located. It appears that both locations ought to be covered by the new definition, because only jointly can they ensure that it will cover all

possible places where a prohibited act can be potentially committed. This is seen in the above list of offence types that can be committed through the use of the Internet (understood as an information system), which may be the object of a causative act (e.g. in Art. 269b(1)) or – far more often – the implement of an offence.

The above suggestions for regulating the *loci* of cybercrimes are a response meant to fill the gap in the Criminal Code in this respect. The discussion shows that the current wording of its Art. 6(2) does not cover all the possible locations where the offences of this category may be committed. Consequently, there is a risk that at least some criminal acts may fall outside the jurisdiction of the Polish criminal justice authorities. Bearing in mind the continual development of technology, one may expect an increase in cybercrime. This situation, in turn, calls on the legislator to take appropriate measures to ensure that the legal order will be always capable of responding to the commission of an offence. One may only hope that the suggestions will improve the law as it stands now or at least provoke a constructive discussion in this respect.

Summary

Mariusz Nawrocki, *Cybercrime locus as defined now and in amendments suggested*

The article deals with the issue of how to determine the place where cybercrimes are committed. This is a problematic issue, as the Criminal Code, Art. 6(2), regulating the place of committing a prohibited act, does not fully cover all the possible locations of this category of offences. The article proposes amendments to the provisions that aim to extend the definition of a prohibited act so as to include also those locations in which there is an IT system (including the Internet) used to commit an offense or one which the perpetrator has affected, committing the act.

Keywords: *criminal liability, place of committing offence, cybercrime*

(przekład na język angielski: Tomasz Żebrowski)

Streszczenie

Mariusz Nawrocki, *Miejsce popełnienia przestępstw internetowych de lege lata i de lege ferenda*

Artykuł dotyczy zagadnienia sposobu określania miejsca popełnienia przestępstw internetowych. Jest to zagadnienie problematyczne, gdyż przepis art. 6 § 2 Kodeksu karnego, regulujący miejsce popełnienia czynu zabronionego, nie obejmuje w pełni wszystkich możliwych lokalizacji tej kategorii przestępstw. W artykule zaproponowano zmiany przepisów, które zmierzają do rozszerzenia definicji miejsca popełnienia czynu zabronionego tak, aby objąć tym pojęciem również te lokalizacje, w których znajduje się system informatyczny (obejmujący również Internet) służący do popełnienia czynu zabronionego lub na który sprawca oddziaływał, popełniając ten czyn.

Słowa kluczowe: *odpowiedzialność karna, miejsce popełnienia przestępstwa, przestępstwo internetowe*

Literatura

1. A. Adamski, *Prawo karne komputerowe*, Warszawa 2000;
2. A. Adamski, *Podstawy jurysdykcji cyberprzestępstw w prawie porównawczym* [w:] *Księga pamiątkowa ku czci Profesora Jana Białocerkiewicza*, red. T. Jasudowicz, M. Balcerzak, t. II, Toruń 2009;
3. A. Błachnio, *Miejsce popełnienia czynu zabronionego przed podżegacza i pomocnika – zarys problematyki*, „Palestra" 2006, nr 7–8;
4. J. Czekalska, *Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych*, Państwo i Prawo 2004, nr 11;
5. J. Giezek [red.] *Kodeks karny. Część ogólna. Komentarz*, red. N. Kłączyńska, G. Łabuda, Warszawa 2012;
6. B. Hołyst, *Internet jako miejsce zdarzenia*, Prokuratura i Prawo 2009, nr 4;
7. B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, Prokuratura i Prawo 2011, nr 1;
8. M. Nawrocki, *Miejsce popełnienia czynu zabronionego*, Warszawa 2016
9. M. Nawrocki, *Przestępstwa dystansowe i tranzytowe*, Acta Iuris Stetinensis 2016, nr 2(14);
10. C. Nowak, *Wpływ procesów globalizacyjnych na polskie prawo karne*, Warszawa 2014;
11. M. Siwicki, *Pojęcie locus delicti i zasady jurysdykcji karnej w ujęciu prawnoporównawczym (cz. II)*, Europejski Przegląd Sądowy 2011, nr 10;
12. M. Siwicki, *Podział i definicja cyberprzestępstw*, Prokuratura i Prawo 2012, nr 7–8;
13. M. Siwicki, *Cyberprzestępczość*, Warszawa 2013;
14. M. Siwicki, *Podstawy określenia jurysdykcji cyberprzestępstw na gruncie polskiego ustawodawstwa karnego w świetle międzynarodowych standardów normatywnych*, Palestra 2013, nr 3–4;
15. M. Siwicki, *Podstawy określenia jurysdykcji karnej przestępstw prasowych w Internecie*, Przegląd Sądowy 2013, nr 11–12;
16. M. Sowa, *Odpowiedzialność karna sprawców przestępstw internetowych*, Prokuratura i Prawo 2002, nr 4;
17. R.A. Stefański, *Miejsce popełnienia przestępstwa. Problemy materialno-karne i procesowe* [w:] *Problemy wymiaru sprawiedliwości karnej. Księga Jubileuszowa Profesora Jana Skupińskiego*, red. A. Błachnio-Parzych, J. Jakubowska-Hara, J. Kosonoga, H. Kuczyńska, Warszawa 2013;
18. A. Światłowski, *Miejsce popełnienia przestępstwa a odpowiedzialność karna – zarys problematyki*, Monitor Prawniczy 1993, nr 4;
19. J. Warylewski, *Pornografia w Internecie – wybrane zagadnienia karnoprawne*, Prokuratura i Prawo 2002, nr 4;
20. D. Zając, *Odpowiedzialność karna za czyny popełnione za granicą*, Kraków 2017.