Maciej Siwicki

Podstawy określenia jurysdykcji cyberprzestępstw na gruncie polskiego ustawodawstwa karnego w świetle międzynarodowych standardów normatywnych

Palestra 58/3-4(663-664), 101-108

2013

Maciej Siwicki

PODSTAWY OKREŚLENIA JURYSDYKCJI CYBERPRZESTĘPSTW NA GRUNCIE POLSKIEGO USTAWODAWSTWA KARNEGO W ŚWIETLE MIĘDZYNARODOWYCH STANDARDÓW NORMATYWNYCH

Wymiana informacji w Internecie odbywająca się z wykorzystaniem pakietów danych przebiega zazwyczaj w sposób w pełni zautomatyzowany i niezależny od użytkownika, z wykorzystaniem wielu routerów łączących niezliczoną ilość systemów informatycznych zlokalizowanych na całym świecie. Obecny poziom rozwoju i dostępności usług świadczonych drogą elektroniczną powoduje potrzebę wzmożonej ochrony prawnej, w szczególności z wykorzystaniem instrumentów prawnokarnych. Dla skutecznego ścigania sprawców cyberprzestępstw niewątpliwie duże znaczenie ma zagadnienie *locus delicti* i zakres jurysdykcji karnej w cyberprzestrzeni[1].

Jednym z najważniejszych międzynarodowych instrumentów w dziedzinie zwalczania przestępstw popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji jest Konwencja Rady Europy z 2001 r. w sprawie cyberprzestępczości, która zawiera wspólne definicje różnych rodzajów przestępstw komputerowych oraz ustanawia podstawy funkcjonowania współpracy sądowej między państwami sygnatariuszami Konwencji. Również na forum Unii Europejskiej przyjęto inne, bardziej ogólne akty prawne, dotyczące aspektów zwalczania cyberprzestępczości, takie jak decyzja ramowa Rady Unii Europejskiej 2004/68/WSiSW z 22 grudnia 2003 r. dotycząca zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej (Dz.Urz. UE L 13 z 20 stycznia 2004 r., s. 44–48; Dz.Urz., polskie wydanie specjalne, rozdz. 19, t. 7, s. 10–14), stanowiące dobry przykład możliwych do przyjęcia rozwiązań kolizyjnych. Warto również odnieść się do decyzji ramowej Rady 2008/913/WSiSW z 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych (Dz.Urz. UE L 328 z 6 grudnia 2008 r., s. 55–58) oraz decyzji ramowej Rady 2005/222/WSiSW z 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.Urz. UE L 05 z 16 marca 2005 r., s. 67–69).

Przedmiotem zainteresowania niniejszego opracowania uczyniono międzynarodowe inicjatywy i standardy normatywne określające reguły jurysdykcyjne w stosunku do

[1] Ogólnie można stwierdzić, że grupa czynów, określana jako cyberprzestępstwa, polega na posługiwaniu się systemami lub sieciami informatycznymi do naruszania jakiegokolwiek dobra prawnego chronionego przez prawo karne. W skład tak rozumianej cyberprzestępczości wchodzą zatem te typy przestępstw, które jako pierwotny przedmiot ochrony mają szeroko pojętą ochronę informacji związaną z wykorzystaniem technik informacyjnych oraz niezakłócone funkcjonowanie systemu komputerowego lub sieci teleinformatycznej, jak również ochronę innych dóbr prawnych, które mogą zostać naruszone z wykorzystaniem nowoczesnych technologii przetwarzania informacji.

cyberprzestępstw. Pozwoli to na ocenę polskiego ustawodawstwa karnego materialnego w aspekcie dostosowania zawartych w nim rozwiązań do wskazanych standardów normatywnych.

1. PODSTAWY OKREŚLENIA JURYSDYKCJI KARNEJ NA GRUNCIE POLSKIEGO USTAWODAWSTWA

Podstawą orzekania przez sądy polskie może być jedynie polskie ustawodawstwo karne. Miejsce popełnienia przestępstwa obejmuje zarówno miejsce, w którym sprawca działał lub zaniechał działania, do którego był obowiązany, jak i miejsce, gdzie nastąpił skutek stanowiący znamię czynu zabronionego lub według zamiaru sprawcy miał nastąpić (art. 6 § 2 k.k.). W myśl wskazanego przepisu wystarczy, by jeden z elementów przestępstwa dotknął terytorium danego państwa, aby mogło ono uznać, że cały czyn podlega jego jurysdykcji. Znajduje to również zastosowanie do czynów instrumentalnego wykorzystania Internetu do naruszenia dóbr prawnie chronionych pod groźbą kary.

Na gruncie obowiązującej kodyfikacji karnej z 1997 r. wyróżnić można cztery zasady odpowiedzialności za przestępstwa popełnione za granicą:

- zasada personalna (narodowości podmiotowej, obywatelstwa), wyrażona w art. 109;
- zasada ochronna (narodowości przedmiotowej) występująca w dwóch postaciach:
  - względnej (zwykłej) – art. 110 § 1 oraz
  - bezwzględnej (obostrzonej) – art. 112;
- zasada odpowiedzialności zastępczej – art. 110 § 2;
- zasada uniwersalna (represji wszechświatowej) – art. 113.

Co do zasady, warunkiem odpowiedzialności za czyn popełniony za granicą jest uznanie takiego czynu za przestępstwo również przez ustawę obowiązującą w miejscu jego popełnienia. Przedstawiona zasada sprowadza się do stwierdzenia, że zasadniczo czyn popełniony przez sprawcę za granicą musi być traktowany jako przestępstwo zarówno w polskiej ustawie karnej, jak i w ustawie obowiązującej w miejscu i w czasie jego popełnienia (*lex loci*). Ograniczenie to nie znajduje zastosowania w przypadku zasady przedmiotowej w postaci bezwzględnej. Jej zastosowanie jest bowiem zależne nie od miejsca czynu, ale od przedmiotu działania i szczególnego zagrożenia dla jakiegoś kraju. Jej działanie rozciąga się nie tylko na przestępstwa cudzoziemców, ale również obywateli Polski. Działanie zasady obostrzonej według art. 112 odnosi się do:

1) przestępstwa przeciwko bezpieczeństwu wewnętrznemu lub zewnętrznemu Rzeczypospolitej Polskiej,

2) przestępstwa przeciwko polskim urzędom lub funkcjonariuszom publicznym,

3) przestępstwa przeciwko istotnym polskim interesom gospodarczym,

4) przestępstwa fałszywych zeznań złożonych wobec urzędu polskiego.

Ostatnia z zasad to zasada represji konwencyjnej (*delicta iuris gentium*), która jest obecna we wszystkich państwach rozwiniętych, będąc wyrazem międzynarodowej solidarności w ściganiu przestępstw objętych odpowiednimi konwencjami lub umowami bilateralnymi. Uniwersalna jurysdykcja jest rozpoznawana przez prawo międzynarodowe dla zabezpieczenia interesu międzynarodowego tylko w bardzo ograniczonych

i unikalnych przypadkach, takich jak: piractwo, przestępstwa wojenne oraz inne „zachowania wystarczająco haniebne, naruszające prawa wszystkich krajów". Jeśli ściganie przestępstwa objęte jest umową międzynarodową, następuje ono niezależnie od miejsca jego popełnienia i od obywatelstwa sprawcy[2]. Chodzi tutaj zatem o sprawców przestępstw, których ściganie wykracza poza sferę zainteresowań pojedynczych państw i jest wspólnym zadaniem społeczności międzynarodowej.

2. MIĘDZYNARODOWE REGUŁY KOLIZYJNE NA OBSZARZE MIĘDZYNARODOWEJ WSPÓŁPRACY W DZIEDZINIE ZWALCZANIA CYBERPRZESTĘPCZOŚCI

Jednym z najważniejszych międzynarodowych instrumentów w dziedzinie zwalczania przestępstw popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji jest Konwencja Rady Europy z 2001 r. w sprawie cyberprzestępczości, która zawiera wspólne definicje różnych rodzajów przestępstw komputerowych oraz ustanawia podstawy funkcjonowania współpracy sądowej między państwami sygnatariuszami Konwencji.

Szczególne znaczenie dla kwestii określenia jurysdykcji w przypadku konkurencji jurysdykcji w sprawach karnych ma art. 22 Konwencji o cyberprzestępczości, według którego:

„Każda Strona przyjmie środki prawne lub inne, które mogą być potrzebne dla ustanowienia swojej jurysdykcji w odniesieniu do przestępstw określonych zgodnie z artykułami 2–11 niniejszej Konwencji, gdy przestępstwo popełnione jest:

a) na jej terytorium, lub

b) na pokładzie statku pływającego pod banderą tej Strony, lub

c) na pokładzie samolotu zarejestrowanego na podstawie prawa tej Strony, lub

d) przez jednego z jej obywateli, jeżeli przestępstwo jest karalne według prawa miejsca jego popełnienia, lub jeśli przestępstwo popełnione zostało poza jurysdykcją terytorialną jakiegokolwiek państwa"[3].

Ten artykuł wymienia zatem na pierwszym miejscu zasadę terytorialną, dalej przy określeniu jurysdykcji zaleca odnieść się do flagi statku oraz miejsca rejestracji statku powietrznego oraz wymienia zasadę narodowości podmiotowej. Jednakże pojedyncze regulacje pozostawione zostały państwom sygnatariuszom:

„Każde państwo może zastrzec sobie prawo do niestosowania lub stosowania tylko w ściśle określonych przypadkach lub warunkach zasad jurysdykcji, o jakich mowa w ustępie 1b–1d niniejszego artykułu lub w dowolnej części tego ustępu"[4].

---

[2] L. Gardocki, *Zarys prawa karnego międzynarodowego*, Warszawa 1985, s. 117–119.

[3] „Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2–11 of this Convention, when the offence is committed: a. in its territory; or b. on board a ship flying the flag; or c. on board an aircraft registered under the laws of that Party; or d. by one of its nationals, if the offence is punishable under criminal law where it was committed if the offence is committed outside the territorial jurisdiction of any State".

[4] „Each State may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b – (1) d of this article or any part thereof".

Niniejsza Konwencja nie wyłącza również jurysdykcji wykonywanej przez stronę zgodnie z jej prawem krajowym. Artykuł 22 określa także zasady postępowania w przypadku sporu:

„Jeżeli kilka Stron uznaje swoją jurysdykcję w odniesieniu do domniemanego przestępstwa określonego w niniejszej Konwencji, Strony te, o ile jest to uzasadnione, podejmują konsultacje w celu określenia, czyja jurysdykcja jest najwłaściwsza dla ścigania tego przestępstwa"[5].

W przypadku zatem, kiedy zamieszczone w Internecie nielegalne treści dostępne są dla więcej niż jednej ze stron Konwencji lub będą ogólnodostępne przy określeniu jurysdykcji, zainteresowane strony powinny podjąć konsultacje. Konsultacje te nie mają jednak charakteru obligatoryjnego i można z nich jednostronnie zrezygnować, gdyby ich wprowadzenie kolidowało z interesem wymiaru sprawiedliwości strony. Należy przy okazji podkreślić, że polski Kodeks karny daje możliwości regulacji zasad określenia jurysdykcji w umowie międzynarodowej, której Polska jest stroną (art. 5 *in fine*).

Należy jednak zauważyć, że najbardziej newralgiczna kwestia ujęcia klasycznej zasady terytorialnej, w przypadku przestępstw popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji, została pozostawiona państwom sygnatariuszom. Konwencja nie wskazuje również, jakie kryteria powinny być brane pod uwagę przy ustalaniu „najściślejszego związku" z państwem, które podejmuje się ścigania tych przestępstw.

Konwencja zawiera także rozwiązania, które mają na celu ułatwienie międzynarodowej współpracy w zakresie wykrywania i ścigania cyberprzestępstw. Według art. 22 pkt 3 Konwencji zobowiązuje się każdą ze stron do przyjęcia środków, które mogą być potrzebne dla zapewnienia swojej jurysdykcji w odniesieniu do każdego przestępstwa w przypadkach, gdy domniemany sprawca przestępstwa przebywa na jej terytorium i nie może zostać wydany innemu państwu wyłącznie ze względu na jego obywatelstwo, po otrzymaniu wniosku ekstradycyjnego.

Znamiennym rozwiązaniem, z punktu widzenia tematyki niniejszego opracowania, jest również zobligowanie państw sygnatariuszy do zbierania dowodów popełnienia przestępstw komputerowych w innych krajach, nawet jeśli w tym kraju dany czyn nie jest uznany za przestępstwo. Według bowiem art. 16 (niezwłoczne zabezpieczanie przechowywanych danych informatycznych) każda strona przyjmie środki prawne i inne, które są niezbędne do tego, by umożliwić właściwym organom nakazanie lub uzyskanie, przy użyciu podobnych metod, niezwłocznego zabezpieczenia wyspecyfikowanych danych informatycznych, w tym także danych dotyczących ruchu, przechowywanych za pomocą systemu informatycznego, w szczególności gdy istnieją podstawy do tego, by sądzić, że dane te są szczególnie podatne na ryzyko utraty lub zmodyfikowania[6].

Konwencja została przyjęta i weszła w życie w 2004 r. Podpisało ją wiele państw, m.in. Stany Zjednoczone i inne państwa pozaeuropejskie (Kanada, Japonia oraz Południowa

[5] „When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution".

[6] Zob. też art. 17 – Niezwłoczne zabezpieczenie i częściowe ujawnienie danych dotyczących ruchu, art. 18 – Nakaz dostarczenia, art. 19 – Przeszukanie i zajęcie przechowywanych danych informatycznych oraz art. 23 – Ogólne zasady współpracy międzynarodowej.

Afryka), a także wszystkie państwa członkowskie UE. Jednak wiele państw sygnatariuszy jeszcze nie ratyfikowało Konwencji lub jej dodatkowego protokołu dotyczącego czynów przestępczych o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych[7].

Bardziej zintegrowane ramy instytucjonalne UE, w szczególności brak długotrwałych procedur związanych z podpisaniem i ratyfikacją, które obowiązują w przypadku Konwencji Rady Europy, pozwalają na znacznie sprawniejsze przyjęcie wśród państw członkowskich UE wspólnych reguł kolizyjnych na obszarze międzynarodowej współpracy w dziedzinie przeciwdziałania cyberprzestępczości.

Na forum Unii Europejskiej przyjęto bardziej ogólne akty prawne dotyczące aspektów zwalczania cyberprzestępczości, takie jak: dyrektywa Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L 335/1 z 17 grudnia 2011 r.) oraz decyzja Rady 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych (Dz.Urz. UE L 328 z 6 grudnia 2008 r., s. 55–58), stanowiące dobry przykład możliwych do przyjęcia rozwiązań kolizyjnych.

Według art. 17 ust. 1 dyrektywy w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej (dotyczącego jurysdykcji i koordynowania ścigania) każde państwo członkowskie podejmuje niezbędne środki w celu ustalenia swojej jurysdykcji w odniesieniu do przestępstw określonych w dyrektywie, gdy:

a) przestępstwo zostało popełnione w całości lub w części na jego terytorium;

b) sprawca jest jednym z jego obywateli[8].

Państwo członkowskie może ustanowić jurysdykcję również jeżeli:

a) przestępstwo zostało popełnione wobec jego obywatela lub osoby mającej miejsce zamieszkania na jego terytorium;

b) przestępstwo zostało popełnione na korzyść osoby prawnej mającej swoją siedzibę na jego terytorium; lub

c) sprawca ma miejsce zwykłego pobytu na jego terytorium.

Ustanawiając jurysdykcję zgodnie z zasadą terytorialną, każde państwo członkowskie zapewnia, że jurysdykcja obejmuje przypadki, gdzie przestępstwo określone w art. 5–6 (przestępstwa związane z pornografią dziecięcą, nagabywanie dzieci do celów seksualnych – przyp. M. S.) oraz w odpowiednim zakresie, w art. 3 i 7 (przestępstwa związane z niegodziwym traktowaniem w celach seksualnych, podżeganie, pomocnictwo, usiłowanie– przyp. M. S.) zostało popełnione z wykorzystaniem systemu komputerowego dostępnego z jego terytorium, bez względu na to, czy system ten znajduje się na jego terytorium. Tym samym w stosunku do przestępstw rozpowszechniania i eksploatacji pornografii dziecięcej następuje rozszerzenie jurysdykcji karnej również na przypadki, kiedy sprawca

[7] Obecnie (stan na 15 września 2011 r.) Konwencja o cyberprzestępczości została ratyfikowana przez 22 państwa, w tym również USA (29 września 2006 r.). Zob. więcej: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=10/3/2008&CL=ENG.

[8] Przepis ten ma szczególne znaczenie dla zapewnienia skutecznego ścigania tak zwanej turystyki seksualnej.

działa z terytorium danego państwa członkowskiego Unii, ale rozpowszechnia treści za pomocą systemu komputerowego położonego w państwie trzecim[9].

Podobne do wskazanych wyżej rozwiązanie przyjęto w decyzji ramowej Rady z 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych (2008/913/WSiSW).

Według art. 9 decyzji uznanie przez państwo jurysdykcji krajowej należy uzależniać przede wszystkim od trzech przesłanek. Po pierwsze od tego, czy czyn przestępny w całości albo częściowo popełniony został na terytorium danego państwa (zasada terytorialna). Po drugie, czy czyn przestępny popełniony został przez obywatela danego państwa i przyczynił się do powstania szkody w stosunku do grupy lub pojedynczej osoby, będącej obywatelem tego państwa. Po trzecie, czy czyn został popełniony na rzecz osoby prawnej, której siedziba znajduje się na terytorium danego państwa. W przypadku zaś przestępstw popełnianych z wykorzystaniem sieci telekomunikacyjnych uznanie podległości krajowemu prawu karnemu państwa członkowskiego na podstawie zasady terytorialności zostało oparte na identycznych przesłankach, jak w decyzji ramowej dotyczącej zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej[10].

Podsumowując powyższe, można zauważyć, że przyjęte w analizowanych decyzjach ramowych rozwiązania odzwierciedlają zaangażowanie Unii Europejskiej na rzecz zwalczania cyberprzestępczości zarówno w skali globalnej, jak i w UE. Analizowane dokumenty międzynarodowe przewidują bowiem nie tylko szczególne uregulowania normatywne, zwłaszcza w odniesieniu do rodzaju i wysokości kar kryminalnych, ale również obligatoryjne przesłanki jurysdykcji. Można również wyciągnąć wniosek, że UE wymaga, aby państwa członkowskie nie ograniczały swoich działań wyłącznie do zabiegów mających na celu przeciwdziałanie cyberprzestępczości mającej miejsce na ich terytorium, lecz skoncentrowały się także na bezpieczeństwie Unii – jako całości.

Warto odnieść się przy tym do koncepcji określenia miejsca popełnienia przestępstwa na podstawie zasady terytorialności i kryterium lokalizacji systemu informatycznego. Na gruncie wskazanych decyzji ramowych zaleca się bowiem, aby ustanawiając jurysdykcję, objąć nią przypadki, w których sprawca działa, znajdując się fizycznie na terytorium danego państwa, niezależnie od miejsca lokalizacji systemu informatycznego, będącego celem lub środowiskiem zamachu, oraz miejsca lokalizacji systemu informatycznego, z wykorzystaniem którego lub przeciwko któremu skierowany jest zamach niezależnie od miejsca, w którym sprawca się fizycznie znajduje. Okoliczność, że sprawca w chwili czynu przebywał na terytorium państwa trzeciego, nie gwarantuje mu przy tym bezkarności na obszarze Unii Europejskiej. Ewentualny zarzut braku podwójnej karalności jest

[9] Zob. art. 55 Konstytucji RP. Por. P. Hofmański, A. Sakowicz, *Reguły kolizyjne w obszarze międzynarodowej współpracy w sprawach karnych*, Państwo i Prawo 2006, z. 11; E. Janczur, *Przejęcie i przekazanie ścigania karnego*, Prok. i Pr. 1999, z. 5.

[10] Według art. 9 ust. 2 jurysdykcji państwa członkowskiego na podstawie zasady terytorialnej podlega sprawca (w odpowiednim zakresie również podżegacz i pomocnik), zarówno jeżeli popełnia przestępstwo, znajdując się na terytorium państwa, niezależnie od tego, czy przestępstwo jest popełnione z wykorzystaniem systemu informatycznego znajdującego się na jego terytorium, jak również gdy popełnia przestępstwo z wykorzystaniem systemu informatycznego znajdującego się na jego terytorium, niezależnie od tego, czy popełniając przestępstwo, sprawca znajduje się na jego terytorium. Zob. też art. 9 ust. 3 decyzji.

nieskuteczny, bo czyn uznaje się za popełniony na terytorium państwa członkowskiego UE, w którym został zlokalizowany serwer.

Wskazana koncepcja budzi jednak liczne wątpliwości, głównie ze względu na możliwość wskazania przypadkowego systemu prawnego. W sytuacji, przykładowo, wykorzystania Internetu w celu nawoływania do nienawiści na tle rasowym może to być prawo kraju, w którym:

a) umiejscowiony jest system informatyczny służący podniesieniu efektywności (przyśpieszeniu) poprzez czasowe i pośrednie zapisywanie informacji pochodzących z innych serwerów;

b) umiejscowiony jest serwer, za pomocą którego informacje są rozpowszechniane z wykorzystaniem np. e-maila (lokalizacja tzw. Mailserwer);

c) umiejscowiony jest system informatyczny, za pomocą którego informacje są udostępniane np. na stronie WWW, przy czym część z nich może być umieszczona na różnych serwerach i w różnych państwach;

d) dochodzi do odczytania informacji zakazanych przez prawo.

Przyjęcie zatem miejsca położenia systemu informatycznego dla określenia jurysdykcji krajowej w sprawach karnych może prowadzić do stanu niepewności, uzależniając ją w rzeczywistości od technicznej infrastruktury usługodawcy internetowego. Należy przy tym zwrócić uwagę, że miejsce lokalizacji systemu informatycznego może być całkowicie obojętne zarówno dla poszkodowanego, jak również dla sprawcy. Nie muszą oni bowiem znać lokalizacji serwera, który wykorzystują.

Powstaje też wątpliwość, czy adekwatnym łącznikiem może być miejsce pobytu sprawcy. Istotnym argumentem przeciwko stosowaniu tej zasady może być znaczne zróżnicowanie przepisów krajowych, m.in. w zakresie standardów ochrony wolności słowa[11]. Ze względu na istniejące odmienności w praktyce pojawiać się mogą trudności z przestrzeganiem nieznanych przepisów prawa obcego.

3. WNIOSKI

Polskie przepisy określające jurysdykcję krajową są w wysokim stopniu zbieżne z wymaganiami stawianymi w przywołanych dokumentach międzynarodowych. Jednakże nie obejmują one popełnienia przez polskiego obywatela poza granicami Rzeczypospolitej Polskiej przestępstwa związanego z rozpowszechnianiem i eksploatacją pornografii dziecięcej w przypadku, gdy nie został spełniony warunek podwójnej karalności. *De lege ferenda* należałoby zatem postulować wprowadzenie stosownych zmian w art. 112 k.k., tak aby rozszerzenie jurysdykcji dotyczyło również przestępstw określonych w decyzji ramowej 2004/68/WSiSW. Ten rodzaj przestępczości bez wątpienia uzasadnia znaczne rozszerzenie jurysdykcji krajowej.

W przypadku przestępstw związanych z treścią informacji właściwa powinna być przede wszystkim ustawa karna państwa, na terytorium którego udostępniono je w sieci telekomunikacyjnej lub systemie komputerowym. Za takim rozwiązaniem przemawia wiele argumentów. Dla przestępstw popełnianych z wykorzystaniem Internetu cha-

[11] Por. M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*, Warszawa 2011.

rakterystyczna jest wielomiejscowość, polegająca na wystąpieniu ujemnych skutków działania sprawcy na różnych obszarach prawnych. Powoduje to, że miejsce działania sprawcy jest kryterium bardziej stabilnym. Od użytkownika należy oczekiwać przynajmniej zachowania zgodnego z prawem obowiązującym w miejscu jego działania. Często jest to dodatkowo zbieżne z jego prawem personalnym. Powyższe powiązanie łagodzi potencjalnie niekorzystne i trudno przewidywalne skutki zastosowania nieznanego dla sprawcy prawa obcego.

Współcześnie od zasady terytorialności tworzy się wyjątki przez posługiwanie się instytucją przekazania – przejęcia ścigania, która polega na tym, że w przypadku popełnienia pewnych określonych przestępstw przez cudzoziemców wszczyna się wprawdzie postępowanie karne, ale następnie przekazuje się dowody i ewentualnie podejrzanego do państwa, którego jest obywatelem. Jest to również korzystniejsze dla podejrzanego, który ma w swoim kraju lepsze możliwości rzeczywistego korzystania z prawa do ochrony[12]. Funkcjonowanie tej instytucji opiera się na zawartych w tym przedmiocie porozumieniach i umowach międzynarodowych, a także na przepisach prawa wewnętrznego (art. 590–592 k.p.k.).

Niezależnie od wskazanych uwag należy również podkreślić, że zasięg jurysdykcji nie powinien być określony zbyt szeroko, a sytuacje, w których dojdzie do zastosowania jurysdykcji pozaterytorialnej, należy opierać na racjonalnie uzasadnionych podstawach. Pomimo licznych komplikacji przy określeniu jurysdykcji krajowej, jakie wynikają z transgranicznego charakteru cyberprzestępczości, należy dystansować się od podejmowania prób ich rozwiązania na drodze formułowania nowego reżimu prawnego, który miałby stanowić alternatywną podstawę jurysdykcji dla mało adekwatnej w tych warunkach zasady terytorialnej, w tym także od mało realistycznych koncepcji, które postulują nadanie cyberprzestrzeni statusu suwerennej przestrzeni międzynarodowej.

[12] L. Gardocki, *Prawo karne*, Warszawa 2005, s. 39.

Summary

Maciej Siwicki
GENERAL PRINCIPLES OF CYBERCRIME JURISDICTION
IN POLISH CRIMINAL LAW IN THE LIGHT OF INTERNATIONAL
NORMATIVE STANDARDS

In this article the author describes the international law of jurisdiction in relation to cybercrime. The focus of this analysis is evaluation of Polish criminal legislation in international standards.

Key words: cybercrime, criminal jurisdiction
Pojęcia kluczowe: cyberprzestępczość, jurysdykcja karna