Konwencja o Cyberprzestępczości - konieczność ratyfikacji, potrzeba rewizji

Dorota Głowacka

I. Wstęp

Konwencja Rady Europy o Cyberprzestępczości (dalej: „Konwencja", „Traktat", „Porozumienie") jest pierwszym międzynarodowym aktem prawnym poświęconym przeciwdziałaniu przestępstwom związanym z wykorzystaniem Internetu. Powstała w kontekście rosnącego znaczenia wspólnych działań państw podejmowanych na rzecz poprawy bezpieczeństwa w przestrzeni wirtualnej, która stała się narzędziem coraz powszechniej wykorzystywanym przez cyberprzestępców. Wobec globalnego charakteru Internetu, zjawisku temu można przeciwdziałać jedynie w drodze wprowadzenia transgranicznych mechanizmów współpracy. Podstawowym celem Konwencji było zatem wprowadzenie jednolitego katalogu czynów karalnych popełnianych przez użytkowników sieci informatycznych, ustanowienie szczególnych procedur dotyczących wykrywania i ścigania cyberprzestępczości, a także określenie standardów współpracy międzynarodowej w tej dziedzinie.

Konwencja ma również ogromny wpływ na realizację praw podstawowych w Internecie, w szczególności na sferę prawa do prywatności oraz ochronę danych osobowych. Z tego względu niektóre jej postanowienia wzbudzają zastrzeżenia ze strony przedstawicieli społeczeństwa obywatelskiego. W dodatku, pomimo upływu niemal dekady od wejścia Konwencji w życie, poziom je implementacji do krajowych porządków prawnych jest wciąż niesatysfakcjonujący. Wiele państw, które początkowo wyraziły wolę przystąpienia do Konwencji - wciąż nie podpisało lub - jak np. Polska - ostatecznie nie ratyfikowało Traktatu.

Obecnie Rada Europy (dalej „RE") zintensyfikowała działania na rzecz szerszego wdrożenia Konwencji wśród swoich członków. Ostatnio do jej ratyfikacji wezwało ponownie Zgromadzenie Parlamentarne RE w Rezolucji ws. ochrony swobody wypowiedzi i swobodnego przepływu informacji w Internecie i mediach elektronicznych z 25 kwietnia 2012 r.[1]. Z drugiej strony, Ministerstwo Sprawiedliwości wznowiło niedawno zawieszoną w 2008 r. procedurę ratyfikacyjną w Polsce[2]. Jednocześnie coraz częściej zgłaszane są postulaty nawołujące nie tylko do pełnego związania się postanowieniami Konwencji, ale także do reformy i modernizacji jej aktualnej treści. Rewizja Konwencji została zapowiedziana zresztą w Strategii Regulacyjnej RE dotyczącej Internetu na lata 2012 – 2015[3].

---

1 Rezolucja nr 1877 (2012), http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=18323&Language=EN#footnote-1385588

2 31 maja 2012 r. odbędzie się spotkanie inaugurujące proces konsultacji społecznych w tej sprawie.

3 https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282011%29175&Language=lanEnglish&Ver=final&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

Przedmiotem niniejszego opracowania będzie próba zidentyfikowania najbardziej problematycznych obszarów związanych w funkcjonowaniem Konwencji, ze szczególnym uwzględnieniem analizy zagrożeń, jakie może ona stwarzać dla praw podstawowych oraz postanowień mogących wpływać na osłabienie jej skuteczności. Ponadto, celem opracowania będzie podsumowanie kwestii ratyfikacji Konwencji w Polsce oraz sformułowanie zaleceń dotyczących dalszych etapów tego procesu.

II. Geneza oraz główne założenia Konwencji

Prace nad tekstem Konwencji rozpoczęły się w 1997 r. W jej powstanie oprócz państw członkowskich RE, zaangażowane były również takie kraje jak Stany Zjednoczone, Kanada, Japonia, czy Republika Południowej Afryki. Konwencja została uchwalona i otwarta do podpisu 23 listopada 2001 r. w Budapeszcie i weszła w życie 1 lipca 2004 r. (warunkiem nadania jej mocy obowiązującej była ratyfikacja w pięciu państwach, w tym trzech należących do RE).

Niewątpliwym osiągnięciem autorów Konwencji jest wprowadzenie do niej katalogu typów przestępstw popełnianych z wykorzystaniem systemów informatycznych. Należą do nich m. in. oszustwo komputerowe, fałszerstwo komputerowe, przestępstwo *hackingu* (m. in. nielegalny dostęp do systemu komputerowego, a także wytwarzanie czy sprzedaż „narzędzi hackerskich"), rozpowszechnianie, posiadanie pornografii dziecięcej, czy też kopiowanie i rozpowszechnianie utworów chronionych prawami własności intelektualnej.

Konwencja o cyberprzestępczości nakłada ponadto na strony obowiązek przyjęcia odpowiednich rozwiązań proceduralnych, które są niezbędne dla celów prowadzonych postępowań karnych w sprawach o przestępstwa określone w Konwencji i mają pomóc uprawnionym organom krajowym w identyfikacji sprawców oraz w gromadzeniu dowodów popełnionych przez nich czynów. Traktat wprowadza m. in. zasady i gwarancje dotyczące przeszukania zasobów komputerowych czy przekazywania, udostępniania oraz zabezpieczenia danych informatycznych. Konwencja obliguje również strony do wprowadzenia odpowiednich środków prawnych mających na celu wzmocnienie współpracy międzynarodowej w zakresie zwalczania cyberprzestępczości m. in. poprzez udzielanie pomocy prawnej (w tym wymianę danych) czy ekstradycję sprawców.

Uzupełnieniem Konwencji jest **Protokół w sprawie kryminalizacji aktów o naturze rasistowskiej lub ksenofobicznej popełnianych z wykorzystaniem systemów komputerowych.** Został on otwarty do podpisu 28 stycznia 2003 r. i wszedł w życie 1 marca 2006 r. Protokół definiuje czym są materiały o charakterze rasistowskim i ksenofobicznym w cyberprzestrzeni, wzywa państwa strony do ich kryminalizacji oraz rozszerza w stosunku do nich zakres stosowania Konwencji. Na włączenie problematyki rasistowskich czy ksenofobicznych treści do samej Konwencji nie zgodziły się niektóre państwa uczestniczące w procesie negocjacji, w szczególności Stany Zjednoczone powołując się na obowiązujące tam szerokie granice swobody wypowiedzi zagwarantowane przez pierwszą poprawkę do Konstytucji. Na rzecz Stanów Zjednoczonych poczyniono także inne „ustępstwa" w procesie tworzenia Konwencji, m. in. w dziedzinie ochrony danych osobowych, co sprowokowało zastrzeżenia, że Konwencja jest efektem zbyt daleko idącego politycznego kompromisu.

Warto zaznaczyć w tym miejscu, że już sam sposób procedowania nad tekstem Konwencji został oceniony przez liczne instytucje reprezentujące społeczeństwo obywatelskie jako nietransparentny i mało otwarty. Pełny projekt postanowień Porozumienia został przedstawiony opinii publicznej po raz pierwszy dopiero w kwietniu 2000 r. Uwagi zgłaszane

w toku zorganizowanych konsultacji społecznych, m. in. przez organizacje pozarządowe, nie zostały w większości uwzględnione[4]. Sposób zredagowania postanowień Konwencji, w szczególności w odniesieniu do gwarancji bezpieczeństwa danych osobowych, skrytykowała także unijna Grupa Robocza Art. 29 (zrzeszająca organy kontrolne ds. ochrony danych osobowych państw członkowskich UE), podkreślając, iż Traktat zawiera wiele niezrozumiałych zapisów, które powinny zostać doprecyzowane. Jak stwierdzono w opinii Grupy Roboczej, „Wskazówki interpretacyjne sformułowane następnie w memorandum wyjaśniającym nie mogą zastąpić bowiem wymogu jasności tekstu samej Konwencji"[5].

III. Problemy związane z funkcjonowaniem Konwencji

A) Niski poziom ratyfikacji

Zasadniczym problemem, jaki dostrzega się na gruncie obowiązywania Konwencji jest przede wszystkim ograniczony zakres terytorialny jej stosowania (choć jest ona otwarta do podpisu także przez kraje niebędące członkami RE). Pomimo szerokiego kręgu państw zainteresowanych przystąpieniem do Konwencji, wiele z nich wciąż nie związało się w pełni jej postanowieniami, co w kontekście ponadgranicznej natury Internetu, znacząco osłabia skuteczność tej umowy międzynarodowej. Państwa, w których ochrona przed bezprawnymi działaniami popełnianymi z wykorzystaniem sieci informatycznych jest niewystarczająca, podważają istotę walki z cybeprzestępczością, która musi mieć charakter globalny. Wśród krajów, które nie podpisały Konwencji znajduje się m. in. Rosja, w której - jak wskazują międzynarodowe raporty - skala cyberprzestępczości należy do najwyższych na świecie[6] (prezydent Wladimir Putin oficjalnie odmówił przystąpienia do Konwencji wskazując, iż porozumienie „uderza w suwerenność Rosji"[7]).

Istnieje także liczna grupa państw, wśród nich m. in. Polska, Szwecja, Irlandia czy Belgia, które podpisały porozumienie, ale wciąż go nie ratyfikowały. W rezultacie, Konwencja obowiązuje jedynie w 19 z 27 państw członkowskich UE. Z państw spoza RE, Konwencję podpisały tylko Stany Zjednoczone, Kanada, Republika Południowej Afryki i Japonia. W tym, jedynie Stany Zjednoczone ostatecznie ratyfikowały Traktat. W sumie Konwencję ratyfikowały 33 państwa, 14 państw podpisało nie dopełniając procedury ratyfikacji, a w 12 krajach, w których planowane było przystąpienie do Porozumienia, wciąż nie podjęto decyzji o złożeniu podpisu. Oznacza to, że niemal w połowie krajów, które wyraziły wolę związania się postanowieniami Konwencji, wciąż nie weszły one w pełni w życie[8].

B) Kwestia ratyfikacji Konwencji w Polsce

Jak już wspomniano, wśród krajów, które nie implementowały w pełni Konwencji znajduje się

---

4 Zob. więcej na temat zarzutów dotyczących przejrzystości i efektywności konsulatcji społecznych Konwencji: „An Advocacy Handbook for the Non Governmental Organisations. The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems", str. 8, http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf

5 Opinia 4/2001 w sprawie projektu konwencji Rady Europy w sprawie cyberprzestępczości, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp41en.pdf

6 Zob. „Raport o zagrożeniach bezpieczeństwa pochodzących z Internetu 2011", http://ssl.certum.pl/certyfikaty/certy,informacje_ciekawostki_certyfikaty_SSL.dxml?MEDIA=pdf ; Zob. także „Global Security Map", http://globalsecuritymap.com/ .

7 „Putin defies Convetion on Cybercrime", http://eng.cnews.ru/news/top/indexEn.shtml?2008/03/27/293913

8 Aktualny stan implementacji: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

Polska, która podpisała Porozumienie już 23 listopada 2001 r. Powody, dla których polskie władze do tej pory nie dopełniły procedury ratyfikacji są niejasne. Ministerstwo Sprawiedliwości podaje, że „na ten stan rzeczy wpływa niewątpliwie to, że materia konwencyjna ma charakter skomplikowany, związany ze stałym rozwojem technologicznym oraz ewolucją stosownych zobowiązań międzynarodowych, zwłaszcza wiążących się z członkostwem Polski w Unii Europejskiej”[9]. Jak pisze A. Adamski (jeden z członków Komitetu Ekspertów Rady Europy ds. Cyberprzestrzeni), „zaniechanie Polski w tym względzie nie jest w pełni zrozumiałe. Można je oczywiście uznać za wyraz suwerennej decyzji państwowej, podejmowanej wszakże w sposób mało transparentny i motywowanej bliżej nieznanymi racjami politycznymi”[10].

Przedstawiciele Ministerstwa Sprawiedliwości podkreślają jednocześnie, że prace legislacyjne, podjęte w Polsce po podpisaniu Konwencji, doprowadziły do zgodności prawa krajowego z większością jej przepisów[11]. Postanowienia Konwencji, pomimo braku jej ratyfikacji, znalazły bowiem odzwierciedlenie w kolejnych nowelizacjach prawa karnego. Ustawodawca wprowadził przede wszystkim do k. k. typy przestępstw określone w Traktacie (zob. art. 115 § 14, 202 § 4a i 4b 268a, 269b, 287 k.k.), a także pewne instrumenty karnoprocesowe (zob. art. 218a czy 236a k.p.k.).

Mimo to, dotychczasowa implementacja postanowień Konwencji jest niepełna oraz wzbudza szereg zastrzeżeń co do niezgodności z normami konwencyjnymi. Zdaniem A. Adamskiego, nieprawidłowości związane z wdrożeniem części zapisów Konwencji dotyczą zarówno sfery regulacji materialnoprawnej, jak i karnoprocesowej[12]. A. Adamski na prośbę Ministerstwa Sprawiedliwości przygotował krytyczną analizę stanu transpozycji Konwencji do polskiego porządku prawnego[13]. Najpoważniejsze zarzuty dotyczą wadliwej transpozycji niektórych typów przestępstw określonych w Konwencji, nieprawidłowego określenia definicji pojęć (takich jak np. definicja dokumentu z art 115 § 14 k.k), czy nieujednoliconej terminologii. A. Adamski zwraca również uwagę, iż nie powołano choćby tzw. „punktu kontaktowego 24/7” o którym mowa w art. 35 Konwencji. Punkty kontaktowy ma wpierać pracę organów powołanych do ścigania cyberprzestępczości, m. in. przez doradztwo techniczne, czy gromadzenie i zabezpieczanie dowodów elektronicznych, udzielanie informacji o prawie i lokalizowanie osób podejrzanych. Konwencja zakłada, iż odpowiednie jednostki mają docelowo powstać we wszystkich krajach, które podpisały Porozumienie.

Jeszcze więcej wątpliwości wzbudza implementacja środków przymusu procesowego. Główny zarzut pod adresem przepisów transponujących postanowienia Konwencji w tym zakresie dotyczy tego, iż opierają się one na analogicznym stosowaniu do rzeczywistości cyfrowej tradycyjnych instytucji k.p.k. Zastrzeżenia dotyczą przede wszystkim wprowadzenia do k.p.k. art. 236a, który zakłada odpowiednie stosowanie przepisów dotyczących zatrzymania rzeczy (217 k.p.k) i przeszukania pomieszczeń (219 k.p.k) do danych przechowywanych w systemie informatycznym. Takiego rozwiązania przyjętego przez polskiego ustawodawcę nie można uznać jednak za wdrożenie przepisów art. 18 (nakaz dostarczenia danych organom uprawnionym) i 19 Konwencji (przeszukanie i zajęcie przechowywanych danych

9 Zob. Materiał informacyjny dotyczący ratyfikacji Konwencji rozesłany przez Ministerstwo Sprawiedliwości 27 kwietnia 2012 r. do instytucji zaproszonych do uczestnictwa w konsultacjach społecznych dotyczących ratyfikacji. http://www.isoc.org.pl/201204/cyberprzestepczosc

10 A. Adamski, „Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę” [w] G. Szpor, „Internet. Ochrona wolności, własności i bezpieczeństwo”, C.H. Beck, 2011.

11 Zob. Materiał informacyjny dotyczący ratyfikacji Konwencji..., *op. cit.*

12 A. Adamski, *op. cit.*

13 Pełne podsumowanie analizy można znaleźć w zaproszeniu do ww. konsultacji społecznych dotyczących ratyfikacji Konwencji przez Polskę, http://www.isoc.org.pl/201204/cyberprzestepczosc

informatycznych).

Obecny stan prawny nie przyznaje także wyraźnego uprawnienia organom powołanym do ścigania przestępstw w cyberprzestrzeni do dokonywania tzw. „przeszukania na odległość" (czynności polegającej na przeszukaniu zasobów systemu komputerowego znajdującego się w odległym miejscu za pośrednictwem sieci). Organy ścigania prowadzące tego typu działania, głęboko ingerujące w sferę prywatną jednostki, narażają się więc obecnie na zarzut działania bez wystarczającej podstawy prawnej. Należy podkreślić jednocześnie, iż obok zastrzeżeń przedstawionych powyżej, zarzutów dotyczących właściwej implementacji przepisów Konwencji jest znacznie więcej[14].

C) Praktyczne problemy związane ze ściganiem przestępstw internetowych

Wątpliwości związane z prawidłową i zgodną z duchem Konwencji transpozycją jej postanowień do polskiego porządku prawnego potęguje **praktyka prokuratorska i sądowa w zakresie ścigania przestępstw popełnianych z wykorzystaniem Internetu.** Praktykę tę Helsińska Fundacja Praw Człowieka monitoruje głównie w ramach programu Obserwatorium Wolności Mediów w Polsce, przede wszystkim w dziedzinie zwalczania przestępstw przeciwko czci popełnianych w sieci. O trudnościach z prawidłowym stosowaniem art. 236a w związku z 217 k.p. k., świadczy chociażby zgłoszony „Obserwatorium" przypadek portalu „Nasze Dziemiany" (portal jest jednocześnie zarejestrowanym tytułem prasowym). W siedzibie redakcji „Naszych Dziemian" zjawiła się policja z żądaniem wydania kilku adresów IP należących do internautów, którzy umieszczali swoje komentarze na portalu. Policjanci nie przedstawili żadnego dokumentu, na podstawie którego zażądali udostępniania wskazanych danych. Dopiero na prośbę redaktor naczelnej okazali do wglądu postanowienie sądu nakazujące policji ustalenie adresów IP w ramach „dokonania czynności dowodowych na podstawie art. 30 § 1 k.p.k., art. 488 § 2 k.p.k.". Postanowienie zostało wydane w ramach procesu z art. 216 kk (zniewaga) toczącego się z oskarżenia prywatnego. Redaktor naczelna przekazała policjantom numery IP, obawiając się zajęcia przez policję sprzętu komputerowego. Należy jednak zaznaczyć, że w sprawie nie dochowano gwarancji procesowych wynikających z ww. przepisów k.p.k. Nie wydano bowiem postanowienia o wydaniu rzeczy (ewentualnie postanowienia zatwierdzającego tę czynność, jeśli byłby to przypadek niecierpiący zwłoki), nie wydano postanowienia o zwolnieniu z tajemnicy służbowej (adresy IP są objęte tajemnicą telekomunikacyjną), a nawet nie spisano protokołu z przeprowadzonej czynności. W konsekwencji redakcja nie miała żadnej możliwości zaskarżenia decyzji o przekazaniu danych. Wydaje się ponadto, iż bardziej proporcjonalnym rozwiązaniem w takich przypadkach byłoby pisemne zwrócenie się do władz portalu o udostępnienie żądanych adresów IP. Więcej o sprawie można przeczytać na stronie internetowej www.obserwatorium.org[15].

W tym miejscu warto podkreślić, że w polskim porządku prawnym z przyczyn proceduralnych brakuje efektywnych mechanizmów dochodzenia odpowiedzialności za przestępstwa internetowe ścigane z oskarżenia prywatnego (takie jak np. zniewaga czy zniesławienie), z uwagi na trudności z identyfikacją personaliów sprawcy i wskazaniem go w prywatnym akcie oskarżenia. Jeszcze bardziej skomplikowane wydaje się obecnie pociągnięcie autora zniesławiającego komentarza internetowego do odpowiedzialności cywilnoprawnej (problem oznaczenia pozwanego w pozwie). Tymczasem warto

14 W nieniejszym opracowaniu nie ma miejsca na bla bla bla Odesłanie do bardziej kompleksowych analiz.

15 http://www.obserwatorium.org/index.php?option=com_content&view=article&id=4169:gdy-policja-przychodzi-do-gazety-po-adresy-ip-przypadek-portalu-nasze-dziemiany&catid=42:z-kraju-polska&Itemid=64

przypomnieć, że zgodnie ze standardem sformułowanym przez Europejski Trybunał Praw Człowieka w wyroku *K.U. p. Finlandii*[16], regulacje krajowe powinny umożliwiać ofiarom naruszeń w Internecie dochodzenie odpowiedzialności od bezpośrednich sprawców.

D) Najważniejsze problemy związane z potrzebą rewizji postanowień Konwencji

- **Niesatysfakcjonujący kompromis między ochroną praw człowieka i walką z cyberprzestępczością**

Pomimo, że Konwencja powstała jako element dorobku prawnego Rady Europy, organizacji o niezaprzeczalnym wkładzie w kształtowanie i promocję standardów praw człowieka, Konwencja zawiera wyłącznie symboliczne odniesienie do praw podstawowych w preambule oraz w klauzuli ogólnej wyrażonej w art. 15. Jej tekst nie odnosi się szczegółowo do przestrzegania praw, których znaczenie jest kluczowe dla komunikacji internetowej, takich jak chociażby swoboda wypowiedzi czy prawo do prywatności, w tym do standardów ochrony danych osobowych. Jeśli chodzi o ostatni aspekt, należy zauważyć, że Konwencja nie nawiązuje w żadnym ze swoich postanowień do zasad zawartych w innej, mającej bardzo istotne znaczenie dla tego obszaru umowie międzynarodowej stworzonej w ramach RE, tj. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (tzw. „Konwencja 108"). Innym problemem jest kwestia inkorporacji do treści Konwencji zasad przyjętych w Rekomendacji (1999) 5 Komitetu Ministrów Rady Europy dla państw członkowskich w sprawie ochrony prywatności w Internecie.

W efekcie przestrzeganie ww. standardów nie jest warunkiem przystąpienia do Konwencji. Jest ona zatem otwarta do podpisu przez państwa, które nie mają skodyfikowanych zasad ochrony danych osobowych lub prowadzą znacznie mniej rygorystyczną politykę w tym zakresie (jak np. Stany Zjednoczone) w stosunku do krajów UE, w których poziom ochrony jednostki reguluje w tej dziedzinie dyrektywa o ochronie danych osobowych[17]. Z punktu wiedzenia państw członkowskich UE taka sytuacja może być szczególnie problematyczna, gdyż Konwencja w ramach wzajemnej pomocy może obligować je do udostępnienia danych do państw trzecich, które nie zapewniają gwarancji przestrzegania zasad przetwarzania danych osobowych na tym samym poziomie. Takie działanie byłoby jednak sprzeczne z art. 25 dyrektywy o ochronie danych osobowych, który zakazuje przekazywania danych do krajów nieczłonkowskich, które nie zapewniają „odpowiedniego stopnia ochrony" (co najmniej na tym samym poziomie). Dlatego też, projekt Konwencji został krytycznie oceniony przez unijną Grupę Roboczą Art. 29 ds. ochrony danych osobowych, która podkreśliła, jak wielki wpływ mają postanowienia Konwencji na ochronę prywatności oraz zasygnalizowała, iż problematyka standardów dotyczących danych osobowych nie została w dostatecznym stopniu przeanalizowana i uwzględniona przez twórców Traktatu[18].

- **Brak efektywnych zasad jurysdykcyjnych**

Zasady jurysdykcyjne określone w Konwencji opierają się głównie na jurysdykcji terytorialnej (w odniesieniu do przestępstw popełnionych na terytorium państwa uznającego się za właściwe do osądzenia sprawcy). Należy jednak pamiętać, że choć zasada ta ma podstawowe znaczenie w świecie niewirtualnym, znajduje ona ograniczone zastosowanie do cyberprzestrzeni, w kontekście jej transgranicznej natury. Inne zasady jurysdykcyjne (np.

16 Orzeczenie ETPC z 2 grudnia 2008 r., nr skargi 2872/02
17 Zob. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r.
18 Opinia 4/2001 w sprawie projektu konwencji Rady Europy w sprawie cyberprzestępczości , http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp41en.pdf

zasada jurysdykcji personalnej) zostały wprowadzone jedynie fakultatywnie bądź w stosunku do ograniczonego kręgu przestępstw. Nie przewidziano natomiast wprowadzenia innego rodzaju jurysdykcji, np. skutkowej (jurysdykcję wykonuje państwo, na terenie którego odczuwalny jest szkodliwy skutek danego zachowania[19]) bądź jurysdykcji ochronnej (uprawnione do wykonywania jurysdykcji są państwa, dla których działania prowadzone w cyberprzestrzeni stanowią bezpośrednie zagrożenie czy w które bezpośrednio wymierzone są treści stron internetowych[20]).

W Konwencji brakuje ponadto skutecznego mechanizmu rozstrzygania sporów międzypaństwowych co do sprawowanie jurysdykcji. Konwencja przewiduje jedynie, że wątpliwości w tym zakresie mają być rozwiązywane w drodze „konsultacji" (art. 22 ust. 5). W konsekwencji, na gruncie Konwencji państwa mogą mieć problem z ustaleniem właściwej jurysdykcji, a co się z tym wiąże – ze skutecznym pociągnięciem do odpowiedzialności sprawców przestępstw.

- **Inne postanowienia osłabiające efektywność współpracy międzynarodowej**

Konwencja zawiera nieprecyzyjny katalog przesłanek pozwalających jej stronom odmówić współpracy międzynarodowej, która jest warunkiem skutecznego zwalczania przestępczości w sieci. W szczególności należy w tym kontekście zwrócić uwagę na **art. 24 ust. 4b**, który stanowi, że państwo może odmówić „pomocy wzajemnej", zawsze gdy „uważa, że realizacja wniosku [innego państwa] może stanowić zagrożenie dla jej suwerenności, bezpieczeństwa, porządku publicznego lub innych podstawowych interesów".

- **Brak mechanizmu nadzoru nad wykonywaniem jej postanowień**

W Konwencji nie przewidziano utworzenia żadnej instytucji pomocniczej, która pomogłaby stronom interpretować jej zapisy, a także monitorowałaby wprowadzenie w życie i wykonywanie jej postanowień, czy umożliwiałaby wymianę dobrych praktyk. Nie przewidziano także obowiązku okresowego raportowania przez strony poziomu i skutków implementacji Konwencji (na wzór mechanizmów, na których opiera się skuteczność innych traktatów międzynarodowych, np. tych dotyczących praw człowieka).

IV. Rekomendacje

Podsumowując rozważania przedstawione powyżej, należy stwierdzić, że Konwencja może stać się instrumentem, który odegra bardzo istotną rolę przeciwdziałaniu przestępczości w środowisku cyfrowym. Aby jednak zapewnić przewidzianym w niej mechanizmom większą skuteczność należy rozważyć podjęcie działań w dwóch obszarach: 1) pełniejszej jej implementacji w krajowych systemach prawnych oraz 2) rewizji niektórych jej postanowień, tak aby odpowiadały aktualnym wyzwaniom związanym ze zwalczaniem cyberprzestępczości.

Działania na rzecz pełniejszej implementacji Konwencji:

- Niezbędne jest dopełnienie ratyfikacji przez kraje, które wciąż nie związały się w pełni postanowieniami Konwencji. Działania na rzecz sfinalizowania procedury ratyfikacji powinien podjąć w szczególności polski rząd, który po raz pierwszy podjął inicjatywę

19 Zob. więcej na temat zasad jurysdykcyjnych stosowanych w cyberprzestrzeni w: J. Kulesza, „Ius Internet. Między prawem a etyką", wyd. WaiP, 2010

20 *Ibidem*

w tym kierunku jeszcze w 2008 r. W kontekście zapowiadanych konsultacji społecznych poświęconych „wypracowaniu stanowiska w przedmiocie ratyfikacji Konwencji przez Polskę", należy mieć nadzieję, że proces ten zostanie obecnie zintensyfikowany. Na marginesie warto podkreślić, że do przystąpienia Polski do Konwencji wzywały liczne instytucje krajowe i międzynarodowe, w tym Rzecznik Praw Obywatelskich[21], Minister Spraw Zagranicznych[22], Generalny Inspektor Ochrony Danych Osobowych[23], Zgromadzenie Parlamentarne oraz Komitet Ministrów Rady Europy, czy Rada Europejska w tzw. Programie sztokholmskim[24].

- Niezbędna jest również ratyfikacja protokołu dodatkowego do Konwencji dotyczącego zwalczania aktów o wydźwięku rasistowskim i ksenofobicznym w Internecie. O jego implementację apelowały m. in. Europejska Komisja Przeciwko Rasizmowi i Nietolerancji (ECRI); a na gruncie polskim – m. in. organizacja „Nigdy Więcej".

- Konieczne jest jednocześnie podjęcie działań na rzecz pełniejszej harmonizacji polskich regulacji prawnych z normami Konwencji, w szczególności w obszarach problemowych wskazanych w części III niniejszego opracowania. Istniejące obecnie rozbieżności nie powinny jednak przeszkodzić w procesie ratyfikacji Konwencji, choć jednocześnie ustawodawca powinien jak najszybciej dążyć do dostosowania prawa krajowego do wymogów konwencyjnych. Jeszcze przed ratyfikacją ustawodawca powinien wskazać środki prawne, jakie należy podjąć w przyszłości w celu najpełniejszego wdrożenia postanowień Konwencji.

- Przygotowanie do ratyfikacji Konwencji stwarza także dogodną okazję do tego, aby rozważyć reformę istniejących na gruncie prawa polskiego instrumentów prawnych umożliwiających pociągnięcie do odpowiedzialności sprawców przestępstw prywatnoskargowych, w których ściganiu nie uczestniczy policja czy prokuratura. Obecnie pokrzywdzeni nie dysponują efektywnymi narzędziami w tym zakresie.

- Po ratyfikacji Konwencji, Polska powinna włączyć się działania podejmowane na arenie międzynarodowej zmierzające do promocji przystąpienia do niej innych państw, które wciąż nie stały się jego stroną.

Działanie na rzecz rewizji postanowień Konwencji:

- Konwencja powinna zapewniać w większym stopniu równowagę pomiędzy zwalczaniem cyberprzestępczości oraz poszanowaniem praw i wolności chronionych na mocy Europejskiej Konwencji Praw Człowieka oraz na mocy orzecznictwa Europejskiego Trybunału Praw Człowieka. Konieczne jest wprowadzenie do niej bardziej precyzyjnych gwarancji poszanowania praw podstawowych w stosunku do aktualnej treści traktatu.

- W szczególności Konwencja powinna uwzględniać dorobek Rady Europy w dziedzinie ochrony danych osobowych, przede wszystkim Konwencję 108. Przestrzeganie zasad ochrony danych osobowych określonych w Konwencji 108 powinno być standardem

21 Zob. Wystąpienie RPO do Ministra Sprawiedliwości w sprawie pełnej implementacji do polskiego porządku prawnego postanowień Konwencji Rady Europy o cyberprzestępczości oraz Protokołu dodatkowego do tej Konwencji - 26 stycznia 2010 r., http://www.rpo.gov.pl/pliki/12645972580.pdf

22 http://www.radeksikorski.pl/dokumenty/konwencja_o_cyberprzestepczosci.pdf

23 http://tech.wp.pl/kat,1009785,wid,14337896,martykul.html?ticaid=1e873

24 Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli 2010/C

dla stron Konwencji. Dlatego też, przystąpienie do Konwencji 108 powinno być warunkiem podpisania i ratyfikowania Traktatu.

- Należy przeanalizować katalog przesłanek pozwalających państwom – stronom odmówić współpracy międzynarodowej wymaganej przez Konwencję. W szczególności warto rozważyć wyeliminowanie zbyt ogólnikowej przesłanki uprawniającej do odstąpienie od stosowania norm konwencyjnych z uwagi na istnienie „innych podstawowych interesów państwa" (art. 24 ust. 4b) i wprowadzić w jej miejsce przesłankę nakazującą odmówienia współpracy, w przypadku gdy druga strona podejmuje działania sprzecznie z poszanowaniem podstawowych praw i wolności.

- Należy wprowadzić efektywne zasady jurysdykcyjne. Propozycje w tym zakresie zostały sformułowane chociażby w alternatywnym do Konwencji tzw. stanfordzkim projekcie międzynarodowego traktatu o cyberprzestępczości[25]. Obok jurysdykcji terytorialnej, przewiduje on wachlarz innych zasad jurysdykcyjnych (m. in. jurysdykcję skutkową), opierając się na zasadzie *aut dedere aut iudicare* („osądź albo wydaj"). Ponadto projekt wprowadza odpowiednią hierarchię stosowania powyższych zasad, która pozwala uniknąć konfliktów między państwami co do wykonywania jurysdykcji (zob. art. 5 projektu stanfordzkiego). Taka konstrukcja zwiększa szansę pociągnięcia do odpowiedzialności sprawców przestępstw popełnionych w sieci, gdy mają one charakter transgraniczny.

- Projekt stanfordzki przewiduje ponadto mechanizm nadzoru nad wykonywaniem postanowień Konwencji, przede wszystkim poprzez utworzenie Agencji, czuwającej nad wdrażaniem i przestrzeganiem jego zapisów w oparciu o raporty składane raz w roku przez państwa strony. Zgodnie z projektem, w ramach Agencji, miałby również zostać utworzony Komitet, którego zadaniem byłoby nadzorowanie wykonywania postanowień traktatu z punktu widzenia podstawowych praw i wolności, ze szczególnych uwzględnieniem zasad ochrony danych osobowych.

- Zaleca się ponadto wprowadzenie do Konwencji ugruntowanych w prawie międzynarodowych pokojowych metod rozwiązywania sporów między stronami w postaci negocjacji, mediacji lub arbitrażu.

- Trzeba jednocześnie podkreślić że mechanizmy proponowane w Konwencji, w tym instrumenty procesowe powinny być wspierane przez działania edukacyjne podejmowane przez rządy państw członkowskich, skierowane zarówno do użytkowników sieci, jak i do organów uprawnionych do ścigania przestępczości w cyberprzestrzeni (przykładem dobrej praktyki jest w tym zakresie podręcznik Interpolu dla policjantów zajmujących się ściganiem cyberprzestępstw[26], czy ośrodek badawczy przy Sądzie Apelacyjnym w Hadze, którego zadaniem jest szkolenie sędziów z prawnych aspektów funkcjonowania Internetu).

- Wreszcie, należy dodać, że walka z cyberprzestępczością nie może opierać się wyłącznie na współpracy międzyrządowej, czy sądowej, ale powinna zakładać również kooperację sektora publicznego z podmiotami prywatnymi działającymi w środowisku cyfrowym, w szczególności takimi jak dostawcy usług internetowych.

---

25 Zob. Proposal for an International Convention on Cyber Crime and Terrorism, **http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf**

26 Zob. https://www.interpol.int/Public/Icpo/Publications/default.asp.