PANOPTYKON
FUNDACJA

Zarząd: Katarzyna Szymielewicz, Małgorzata Szumańska
Rada programowa: Adam Bodnar, Ewa Charkiewicz, Dominika Dörre-Nowak, Józef Halbersztadt, Joanna Kamiol, Monika Płatek, Maciej Ślusarek, Piotr Waglowski, Roman Wieruszewski

Warszawa, 30 maja 2012 r.

Wydział Koordynacji Polityki Europejskiej
Departament Prawa Karnego
Ministerstwo Sprawiedliwości

Szanowni Państwo,

W odpowiedzi na zaproszenie do zabrania głosu w sprawie zainicjowania procesu ratyfikacji Konwencji Rady Europy z 23 listopada 2001 r. o cyberprzestępczości (dalej: „Konwencja") oraz wypracowania stanowiska dotyczącego zakresu zmian w polskim prawie koniecznych do dostosowania go do przepisów Konwencji, Fundacja Panoptykon przekazuje następujące uwagi:

1) Uwagi ogólne

W naszym rozumieniu decyzja polityczna o przystąpieniu do Konwencji zasadniczo została już przez rząd polski podjęta i wyrażona na forum międzynarodowym w momencie jej podpisania (tj. 23 listopada 2001 r.). Zgodnie z zasadami obowiązującymi w prawie międzynarodowym, podpisanie traktatu międzynarodowego jest jednoznaczne z podjęciem przez państwo zobowiązania do dążenia do jego ratyfikacji. Ponadto, mamy świadomość, że rząd polski podjął już szereg działań mających na celu dostosowanie prawa polskiego do postanowień Konwencji. W tym kontekście wydaje się, że decyzja o ratyfikowaniu bądź nie Konwencji jest wtórna wobec decyzji politycznej rządu co do kierunków oraz szczegółowych zasad regulacji obszaru objętego przedmiotem zastosowania Konwencji.

W opinii Fundacji Panoptykon istnieje potrzeba stworzenia spójnych ram prawnych umożliwiających skuteczną walkę z cyberprzestępczością na poziomie międzynarodowym. Jednocześnie, dostrzegamy jednak szereg zagrożeń z perspektywy praw człowieka, które mogą wyniknąć ze zbyt represyjnego lub błędnie zaprojektowanego reżimu prawnego w tym obszarze. Tekst Konwencji pozostawia poszczególnym państwom-sygnatariuszom duże pole do interpretacji jej szczegółowych postanowień w procesie wdrażania do prawa krajowego. W tym kontekście sygnalizujemy potencjalne zagrożenia związane z wdrożeniem wybranych (pod kątem zakresu kompetencji Fundacji Panoptykon) postanowień Konwencji.

Sposób, w jaki zredagowane są postanowienia Konwencji był przedmiotem krytyki między innymi ze strony unijnej Grupy Roboczej Art. 29, która podkreślała, że dokument zawiera wiele niejasnych sformułowań, które należałoby doprecyzować. Zwrócono również uwagę na fakt, iż mimo wielkiego wpływu, jaki na ochronę prywatności i danych osobowych mają postanowienia Konwencji, problematyka ta nie została w wystarczający sposób uwzględniona przez jej twórców. Warto w tym kontekście odnotować również brak jakichkolwiek nawiązań do zasad ochrony danych osobowych z tzw. Konwencji 108 (tj. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, stworzonej w ramach Rady Europy), których przestrzeganie powinno być standardem dla stron Konwencji o cyberprzestępczości.

Doświadczenia państw, które już ratyfikowały i wdrożyły Konwencję pokazują, że nie są to obawy bezpodstawne. W opinii organizacji pozarządowych monitorujących wdrożenie

Konwencji w USA i krajach Ameryki Łacińskiej (EDRi, EFF), doprowadziło do poważnego zaostrzenia prawa, w wyniku którego niektóre czynności i zachowania podejmowane on-line zostały obwarowane większymi sankcjami (lub w ogóle objęte kryminalizacją) w przeciwieństwie do ich odpowiedników w świecie off-line. Ponadto, obywatele podejmujący aktywność w sferze on-line korzystają ze słabszych gwarancji ochrony swoich praw podstawowych, w porównaniu z gwarancjami, jakimi cieszą się off-line. Taka sytuacja, dysproporcji w zakresie kryminalizacji z jednej strony i dostępności niezbędnych gwarancji ochrony praw podstawowych z drugiej, nie powinna mieć miejsca w demokratycznym porządku prawnym, jako sprzeczna m.in. z zasadą proporcjonalności ograniczenia praw człowieka. W tym kontekście liczne organizacje pozarządowe, które wcześniej krytykowały kształt poszczególnych postanowień Konwencji, apelowały o zrewidowanie Konwencji i jej narodowych implementacji z perspektywy praw człowieka oraz zasady rządów prawa przed dopuszczeniem innych państw do jej sygnowania i ratyfikacji.

Mamy nadzieję, że poniższe uwagi zostaną przez Ministerstwo Sprawiedliwości uwzględnione podczas prac nad ratyfikacją Konwencji w Polsce oraz, potencjalnie, prac nad nową dyrektywą Komisji Europejskiej dotyczącą cyberprzestępczości. W szczególności, aby zmitygować sygnalizowane przez nas zagrożenia, rząd polski powinien rozważyć złożenie odpowiednich zastrzeżeń zgodnie z art. 42 Konwencji.

2) Uwagi szczegółowe

a) Definicja cyberprzestępczości w kontekście działań haktywistycznych

Niezwykle istotną kwestią, w kontekście wdrożenia przepisów Konwencji do polskiego porządku prawnego, jest określenie granic ogólnego pojęcia "cyberprzestępczość" oraz zakresu definicji poszczególnych przestępstw, jakie mieszczą się w tej ogólnej kategorii. W szczególności, uważamy, że polskie prawo powinno wyraźnie wyłączać z tych zakresów znaczeniowych działania hakerskie i haktywistyczne, które z definicji są podejmowane w interesie społecznym.

Przykładem złego rozwiązania w tym obszarze jest funkcjonujący w polskim prawie od 2005 roku przepis art. 269b kodeksu karnego:

> *§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.*

Ten przepis jest sformułowany w sposób na tyle ogólny, że nawet osoba testująca bezpieczeństwo systemów teleinformatycznych za zgodą jego właścicieli może być narażona na odpowiedzialność karną, ponieważ w pewnym sensie „wytwarza" lub „pozyskuje" narzędzia programowe „przystosowane do popełnienia przestępstw" wymienionych w tym rozdziale kodeksu karnego.

Ustęp 2 artykułu 6 Konwencji wyłącza jednak spod karalności narzędzia stosowane podczas „autoryzowanych testów i zabezpieczania systemów komputerowych":

> *This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.*

Oczekujemy, że wyłączenie przewidziane w artykule 6 Konwencji znajdzie swoje

odzwierciedlenie w polskim porządku prawnym. Nie rozwiąże ono jednak wszystkich problemów związanych z potencjalnie szerokim zakresem oddziaływania definicji cyberprzestępczości. W szczególności, prawo powinno chronić działania mające na celu wytwarzanie narzędzi hakerskich, które nie mają na celu popełnienia przestępstwa w rozumieniu Konwencji, ale mogą służyć np. omijaniu blokad w dostępie do informacji w Internecie lub ukrywaniu tożsamości osób obawiających się represji politycznych.

W tym kontekście postulujemy również:

(i) Wyraźne wyłączenie karalności działań o charakterze haktywistycznym, tj. manifestacji o charakterze społecznym lub politycznym, polegających np. na modyfikowaniu zawartości stron www, ich podmianie, masowych „odwiedzinach" serwerów w celu ich przeciążenia (DDoS), atakach blokujących lub spowalniających pracę systemów. Działania haktywistyczne od cyberprzestępczości odróżnia ich wymiar symboliczny: wywołują one skutki jedynie w rzeczywistości wirtualnej; nie prowadzą do poważnych szkód majątkowych ani nie stwarzają zagrożenia życia lub zdrowia;

(ii) Powiązanie definicji penalizowanych narzędzi z czynnością przestępczą, a nie samym faktem ich wytwarzania, posiadania lub przesyłania. Mając świadomość, że w wielu przypadkach narzędzia takie są jednym z kluczowych dowodów materialnych w sprawach przeciwko cyberprzestępcom, uważamy, że penalizowane powinno być wyłącznie narzędzie spersonalizowane i przystosowane do konkretnego ataku na konkretną ofiarę, a nie ogólnie "narzędzia przystosowane do popełnienia przestępstw".

b) Proporcjonalność środków zabezpieczających

W kontekście sygnalizowanych powyżej zastrzeżeń z perspektywy zasady proporcjonalności ograniczenia praw podstawowych użytkowników Internetu, na szczególną uwagę zasługuje artykuł 19 Konwencji, dotyczący przeszukania i zajęcia przechowywanych danych informatycznych. Artykuł ten zobowiązuje państwa-strony Konwencji do wdrożenia środków prawnych pozwalających na:

„(...) niezwłoczne rozszerzenie przeszukania lub podobnych metod uzyskiwania dostępu na inny system, jeżeli podczas dokonywania przez nie przeszukania lub uzyskiwania dostępu przy użyciu podobnych metod do konkretnego systemu informatycznego lub jego części (...), organy te mają uzasadnione podstawy by sądzić, że poszukiwane dane przechowywane są w innym systemie informatycznym lub w jego części na ich terytorium i że do danych tych można legalnie uzyskać dostęp z systemu pierwotnego lub są one dostępne dla tego systemu".

W naszej ocenie cytowany powyżej przepis oraz dalsze postanowienia artykułu 19 Konwencji mogą stanowić podstawę daleko idących ograniczeń zarówno prawa do prywatności jak i prawa własności. W przypadku przyjęcia interpretacji niekorzystnej dla obywateli, państwa-strony Konwencji mogą korzystać z możliwości przeszukania i zajęcia przechowywanych danych w sposób dość arbitralny, także w odniesieniu do osób trzecich - czyli osób nieobjętych zakresem podejrzenia.

Warto podkreślić, że już istniejące w polskim prawie przepisy nie gwarantują zachowania zasady proporcjonalności w toku czynności zabezpieczających: nierzadko okazuje się, że osoby podejrzane o dokonanie naruszeń prawa o znikomej społecznej szkodliwości (np. drobne naruszenia prawa własności intelektualnej) są poddawane niezwykle uciążliwym procedurom przeszukania i konfiskaty mienia, co prowadzi do pozbawienia ich narzędzi niezbędnych do normalnego funkcjonowania w społeczeństwie cyfrowym (w tym świadczenia pracy).

W tym kontekście postulujemy obwarowanie artykułu 19 odpowiednimi zastrzeżeniami na etapie ratyfikacji albo (gdyby takie rozwiązanie okazało się niemożliwe) zapewnienie

odpowiednich gwarancji poszanowania podstawowych praw użytkowników na etapie wdrażania tego przepisu do prawa krajowego.

c) Przekazywanie danych osobowych pomiędzy państwami-stronami Konwencji

W naszej opinii na szczególną uwagę zasługują artykuły od 23 do 35 Konwencji, które przewidują daleko idącą współpracę międzynarodową pomiędzy organami egzekwowania prawa państw-stron Konwencji. Na mocy tych postanowień każde państwo-strona Konwencji może zażądać przekazania danych, które inne państwo-strona Konwencji zebrało zgodnie z postanowieniami artykułów od 16 do 21. Konieczność realizacji takiego żądania nie jest uzależniona od spełnienia wymogu podwójnej karalności czynu, którego dotyczy prowadzone dochodzenie (chyba, że państwo uczyniło odpowiednie zastrzeżenie przy ratyfikacji Konwencji).

W przypadku ratyfikowania Konwencji bez zastrzeżeń, państwo-strona ma niezwykle ograniczone możliwości odmowy przekazania danych w przypadku otrzymania takiego żądania. Należy mieć przy tym na uwadze, że pomiędzy państwami-stronami Konwencji już dziś występują istotne rozbieżności zarówno co do zakresu kryminalizacji różnych aktywności podejmowanych przez użytkowników Internetu (np. w sferze ochrony własności intelektualnej), jak i co do standardów ochrony danych osobowych (np. w USA).

W tym kontekście uważamy, że wdrożenie artykułów od 23 do 35 Konwencji do polskiego porządku prawnego może stworzyć poważne zagrożenia na gruncie prawa do prywatności i ochrony danych osobowych, podobne do sygnalizowanych w debacie na temat porozumienia ACTA. Postulujemy zatem dokonanie niezbędnych zastrzeżeń na etapie ratyfikacji Konwencji, które zapewnią maksymalne gwarancje poszanowania polskich standardów ochrony danych osobowych w sytuacji przekazania danych do krajów trzecich oraz uzależnią samą możliwość takiego transferu od spełnienia warunku podwójnej karalności czynu.

Co więcej, gwarancje i obwarowania poszanowania praw użytkowników zawarte w artykule 15 Konwencji ani nie są wystarczające, ani nie gwarantują jednolitej implementacji przez poszczególne państwa-strony Konwencji. Warto również podkreślić, że poważne zastrzeżenia pod adresem reżimu przekazywania danych osobowych na gruncie Konwencji zgłaszała także Grupa Robocza Art. 29. Niestety, ani te uwagi ani krytyczne głosy organizacji pozarządowych nie zostały uwzględnione na etapie prac nad Konwencją.

Z poważaniem,

W imieniu Fundacji Panoptykon,

Katarzyna Szymielewicz

Dyrektorka