KOMISJA EUROPEJSKA

Bruksela, dnia 30.9.2010
KOM(2010) 517 wersja ostateczna

2010/0273 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WsiSW

{SEC(2010) 1122 final}
{SEC(2010) 1123 final}

UZASADNIENIE

1. PODSTAWA I CELE WNIOSKU

Wniosek ma na celu zastąpienie decyzji ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[1]. Decyzja ramowa stanowiła, jak czytamy w jej motywach, odpowiedź na potrzebę usprawnienia współpracy między organami sądowymi i innymi właściwymi organami, włącznie z policją i innymi wyspecjalizowanymi organami ścigania państw członkowskich, poprzez zbliżanie w państwach członkowskich przepisów prawa karnego w dziedzinie ataków na systemy informatyczne. Wprowadziła ona przepisy UE dotyczące postępowania z takimi przestępstwami jak nielegalne uzyskiwanie dostępu do systemów informatycznych, nielegalne ingerowanie w te systemy oraz nielegalne ingerowanie w dane, jak również szczególne przepisy dotyczące odpowiedzialności osób prawnych, jurysdykcji i wymiany informacji. Państwa członkowskie zobowiązane były podjąć środki niezbędne w celu wypełnienia przepisów decyzji ramowej do dnia 16 marca 2007 r.

W dniu 14 lipca 2008 r. Komisja opublikowała sprawozdanie z wykonania decyzji ramowej[2]. W konkluzjach sprawozdania odnotowano, że w większości państw członkowskich osiągnięto znaczące postępy, oraz że stopień wdrożenia aktu był stosunkowo dobry, jednak w niektórych państwach członkowskich proces ten nie został jeszcze zakończony. W sprawozdaniu zaznaczono także, że liczne „ataki, jakie miały miejsce w całej Europie od czasu przyjęcia decyzji ramowej, uświadamiają wiele rodzących się zagrożeń, a w szczególności pojawienie się zjawiska masowych jednoczesnych ataków na systemy informatyczne oraz wzrost przestępczego wykorzystania tzw. botnetów". Ataki te nie znajdowały się w centrum uwagi w momencie przyjmowania decyzji ramowej. W odpowiedzi na taki rozwój sytuacji Komisja rozważy działania służące opracowaniu lepszych środków przeciwdziałania temu zagrożeniu (zob. wyjaśnienia dotyczące botnetów w kolejnej części).

Znaczenie podjęcia dalszych działań w celu intensyfikacji walki z cyberprzestępczością zostało podkreślone w programie haskim z 2004 r. dotyczącym wzmacniania wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej, jak również w programie sztokholmskim z 2009 r. i powiązanym z nim planem działania[3]. Ponadto w niedawno zaprezentowanej Europejskiej agendzie cyfrowej[4], pierwszej inicjatywie przewodniej przyjętej w ramach strategii „Europa 2020", uznano potrzebę podjęcia na szczeblu europejskim działań w odpowiedzi na nowe formy przestępczości, w szczególności cyberprzestępczości. W obszarze działań skoncentrowanym na zaufaniu i bezpieczeństwie Komisja zdecydowana jest podejmować środki na rzecz zwalczania cyberataków na systemy informatyczne.

Na szczeblu międzynarodowym za aktualnie najbardziej kompletny zbiór norm międzynarodowych, uznawana jest Konwencja Rady Europy o cyberprzestępczości („Konwencja o cyberprzestępczości") podpisana w dniu 23 listopada 2001 r. , ponieważ przewiduje ona kompleksowe i spójne ramy prawne obejmujące różne aspekty związane z

---

1 Dz.U. L 69 z 16.3.2005, s. 68.

2 Sprawozdanie Komisji dla Rady na podstawie art. 12 decyzji ramowej Rady z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne, COM (2008) 448.

3 Dz.U. C 198 z 12.8.2005, Dz.U. C 115 z 4.5.2010 , COM (2010) 171 z 20.4.2010.

4 Komunikat Komisji COM(2010) 245 z 19.5.2010 r.

cyberprzestępczością[5]. Konwencję podpisały jak dotychczas wszystkie 27 państwa członkowskie, ale tylko 15 z nich ratyfikowało ją[6]. Konwencja weszła w życie w dniu 1 lipca 2004 r. UE nie jest jej sygnatariuszką. Ze względu na znaczenie tego instrumentu Komisja aktywnie zachęca pozostałe państwa członkowskie UE do możliwie najszybszego ratyfikowania konwencji.

- **Kontekst ogólny**

Jeżeli chodzi o cyberprzestępczość, główną przyczyną tego zjawiska jest podatność na zagrożenie wynikająca z szeregu czynników. Do utrzymywania się tego zjawiska i pogłębiania związanych z nim trudności przyczyniają się niewystarczające działania ze strony organów ścigania, ponieważ pewne rodzaje przestępstw mają charakter transgraniczny. Przestępstwa tego rodzaju często nie są właściwie zgłaszane, po części dlatego, że niektóre z nich nie są zauważane, a po części dlatego, że pokrzywdzeni (spółki i inne podmioty gospodarcze) nie zawiadamiają o przestępstwach z obawy o pogorszenie ich wizerunku oraz perspektyw biznesowych w wyniku upublicznienia stopnia ich narażenia na te zagrożenia.

Ponadto zróżnicowanie krajowego prawa i procedur karnych może powodować różnice w sposobie prowadzenia dochodzeń i ścigania przestępstw, co prowadzi z kolei do odmiennego traktowania tych przestępstw w poszczególnych państwach członkowskich. Rozwój technologii informatycznych przyczynił się do zaostrzenia tych problemów, ponieważ obecnie łatwiej jest produkować i rozpowszechniać narzędzia (złośliwe oprogramowanie i botnety) przy zachowaniu anonimowości przestępców i rozłożeniu odpowiedzialności pomiędzy różnymi jurysdykcjami. Ze względu na trudności w ściganiu tych przestępstw, przestępczość zorganizowana może przynosić w tej dziedzinie znaczne zyski przy niewielkim ryzyku.

W niniejszym wniosku uwzględniono nowe metody popełniania cyberprzestępstw, w szczególności wykorzystanie botnetów. Pojęcie botnetu oznacza sieć komputerów zarażonych złośliwym oprogramowaniem (wirusami komputerowymi). Taka sieć zainfekowanych komputerów (tzw. zombie) może zostać aktywowana do wykonywania szczególnych zadań, takich jak ataki na systemy informatyczne (cyberataki). Owe komputery „zombie" można kontrolować – często bez wiedzy użytkowników zainfekowanych komputerów – z innego komputera. Taki komputer kontrolujący nazywany jest również „centrum dowodzenia i kontroli" (ang. *command-and-control centre*). Osoby kontrolujące to centrum zaliczane są do przestępców, ponieważ używają zainfekowanych komputerów do atakowania systemów informatycznych. Bardzo trudno jest namierzać sprawców, ponieważ komputery składające się na botnet i wykorzystywane do ataku mogą znajdować się w innymi miejscu niż sam przestępca.

Ataki przeprowadzane za pośrednictwem botnetu wykonywane są często na wielką skalę. Ataki na wielką skalę to ataki przeprowadzane z wykorzystaniem narzędzi oddziałujących na znaczną liczbę systemów informatycznych (komputerów), bądź ataki powodujące znaczne szkody, np. polegające na zakłóceniu świadczenia usług realizowanych przez system, powodujące koszty finansowe, utratę danych osobowych etc. Szkody powodowane atakami na wielką skalę mają istotny wpływ na funkcjonowanie samego celu tych ataków lub negatywnie oddziałują na jego środowisko pracy. W tym kontekście „duży botnet" należy

---

[5] Konwencja Rady Europy o cyberprzestępczości, Budapeszt 23.11.2001 r., CETS nr 185.

[6] Zestawienie informacji dotyczących ratyfikacji konwencji (CETS nr 185) - zob.: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

rozumieć jako sieć zdolną do wyrządzenia poważnych szkód. Trudno jest zdefiniować botnety pod względem wielkości, jednak największe odnotowane wśród nich szacowano na od 40 do 100 tys. połączeń (tzn. zainfekowanych komputerów) w okresie 24 godzin[7].

- **Obowiązujące przepisy w dziedzinie, której dotyczy wniosek**

Na szczeblu UE decyzja ramowa wprowadza minimalny poziom zbliżenia przepisów państw członkowskich w celu kryminalizacji licznych cyberprzestępstw, w tym nielegalnego uzyskiwania dostępu do systemów informatycznych, nielegalnego ingerowania w system, nielegalnego ingerowania w dane oraz podżeganie do tych przestępstw, pomocnictwo w nich, jak i usiłowanie ich popełnienia.

Chociaż przepisy decyzji ramowej zostały ogólnie wdrożone przez państwa członkowskie, akt ten ma szereg braków, biorąc pod uwagę tendencje w zakresie skali i liczby przestępstw (cyberataków). Zbliża on przepisy wyłącznie w odniesieniu do ograniczonej liczby przestępstw, równocześnie nie zaradzając w pełni potencjalnemu zagrożeniu, jakie stwarzają dla społeczeństwa ataki na wielką skalę. Nie uwzględnia również wystarczająco powagi tych przestępstw i kar za nie nakładanych.

Pozostałe realizowane lub planowane inicjatywy i programy UE pozwalają w pewnym stopniu zaradzić problemom związanym z cyberatakami lub cyberprzestrzenią, takim jak bezpieczeństwo sieciowe oraz bezpieczeństwo użytkowników Internetu. Należą do nich działania wspierane w ramach programów „Zapobieganie i walka z przestępczością”[8], „Wymiar sprawiedliwości w sprawach karnych”[9], „Bezpieczniejszy Internet”[10] oraz inicjatywa w zakresie krytycznej infrastruktury informatycznej[11]. Obok decyzji ramowej kolejnym istotnym obowiązującym instrumentem prawnym jest decyzja ramowa 2004/68/WSiSW dotycząca zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej.

Na szczeblu administracyjnym, praktyka polegająca na infekowaniu komputerów i włączania ich do botnetów jest już zakazana przepisami UE dotyczącymi prywatności i ochrony danych[12]. Zwłaszcza agencje administracji krajowej współpracują już w ramach europejskiej sieci kontaktowej krajowych organów odpowiedzialnych za walkę ze spamem. Na podstawie wspomnianych przepisów UE państwa członkowskie zobowiązane są do zakazania przechwytywania komunikatów przesyłanych za pośrednictwem publicznych sieci komunikacyjnych i publicznie dostępnych elektronicznych usług komunikacyjnych bez zgody zainteresowanych użytkowników lub zezwolenia prawnego.

Wniosek jest zgodny z tymi przepisami. Państwa członkowskie powinny zwrócić uwagę na kwestię poprawy współpracy między administracją i organami ścigania w przypadkach, które podlegają zarówno sankcjom administracyjnym, jak i karom kryminalnym.

---

7 Jednostką pomiaru używaną powszechnie do szacowania wielkości botnetów jest liczba połączeń w okresie 24 godzin.

8 Zob. http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

9 Zob. http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm

10 Zob. http://ec.europa.eu/information_society/activities/sip/index_en.htm

11 Zob. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

12 Dyrektywa o prywatności i komunikacji elektronicznej (Dz.U. L 201 z 31.7.2002), zmieniona dyrektywą 2009/136/WE (Dz.U. L 337 z 18.12.2009).

- **Spójność z pozostałymi obszarami polityki i celami Unii**

Cele są w zgodne z politykami UE w dziedzinie zwalczania przestępczości zorganizowanej, zwiększenia odporności sieci komputerowych, ochrony krytycznej infrastruktury informatycznej oraz ochrony danych. Cele te są także spójne z programem na rzecz bezpieczniejszego Internetu, ustanowionym w celu promowania bezpieczniejszego korzystania z Internetu i nowych technologii internetowych oraz w celu zwalczania nielegalnych treści.

Niniejszy wniosek został poddany dogłębnej analizie w celu zagwarantowania, by jego przepisy były w pełni zgodne z prawami podstawowymi oraz, w szczególności, z ochroną danych osobowych, swobodą wypowiedzi i informacji, prawem do rzetelnego procesu, domniemaniem niewinności oraz prawem do obrony, jak również zasadą legalizmu i proporcjonalności przestępstw i kar kryminalnych.

2. KONSULTACJE Z ZAINTERESOWANYMI STRONAMI I OCENA SKUTKÓW

- **Konsultacje z zainteresowanymi stronami**

Przeprowadzono konsultacje z szerokim kręgiem ekspertów w rozpatrywanej dziedzinie podczas szeregu różnych spotkań, na których omawiano różne aspekty walki z cyberprzestępczością, w tym działania podejmowane w ich następstwie przez organy wymiaru sprawiedliwości (ściganie). W spotkaniach uczestniczyli w szczególności przedstawiciele rządów państw członkowskich i sektora prywatnego, wyspecjalizowani sędziowie i prokuratorzy, organizacje międzynarodowe, agencje europejskie i organy eksperckie. Wielu ekspertów i wiele organizacji przesłało następnie swoje opinie oraz dostarczyło informacji.

Najważniejsze wnioski wynikające z konsultacji to:

– potrzeba podjęcia przez UE działania w tej dziedzinie;

– potrzeba kryminalizacji form przestępstw nieujętych w obecnej decyzji ramowej, w tym w szczególności nowych form cyberataków (botnetów);

– potrzeba wyeliminowania czynników utrudniających dochodzenie i ściganie w sprawach transgranicznych.

Opinie zebrane w trakcie konsultacji zostały uwzględnione w ocenie skutków.

Gromadzenie i wykorzystanie wiedzy specjalistycznej

Konsultacje z ekspertami zewnętrznymi przeprowadzono podczas różnych spotkań z zainteresowanymi podmiotami.

Ocena skutków

Przeanalizowane zostały różne warianty strategiczne, mające służyć osiągnięciu zakładanego celu.

- Wariant strategiczny nr 1: *status quo*/brak nowych działań ze strony UE

Wariant ten oznacza, że UE nie podejmie żadnych dalszych działań w celu zwalczania tego szczególnego rodzaju cyberprzestępczości, tzn. ataków na systemy informatyczne. Trwające już działania byłyby kontynuowane, w szczególności programy na rzecz wzmocnienia ochrony krytycznej infrastruktury informatycznej oraz poprawy współpracy publiczno-prywatnej w zwalczaniu cyberprzestępczości.

- Wariant strategiczny nr 2: stworzenie programu mającego zintensyfikować wysiłki na rzecz przeciwdziałania atakom na systemy informatyczne środkami nielegislacyjnymi.

Środki nielegislacyjne zostałyby zastosowane obok programu na rzecz ochrony krytycznej infrastruktury informatycznej i skoncentrowałyby się na egzekwowaniu prawa w wymiarze transgranicznym oraz współpracy publiczno-prywatnej. Te instrumenty „miękkiego" prawa powinny zmierzać do wspierania dalszych skoordynowanych działań na szczeblu UE, w tym udoskonalenia istniejącej całodobowej sieci punktów kontaktowych dla organów ścigania; ustanowienia unijnej sieci publiczno-prywatnych punktów kontaktowych, z udziałem ekspertów w dziedzinie cyberprzestępczości i organów ścigania; opracowania standardowej unijnej umowy o gwarantowanym poziomie świadczonych usług na potrzeby współpracy organów ścigania z operatorami z sektora prywatnego; oraz wspierania organizacji programów szkoleniowych dla organów ścigania dotyczących dochodzeń w sprawach cyberprzestępczości.

- Wariant strategiczny nr 3: specjalnie ukierunkowana aktualizacja przepisów decyzji ramowej (nowa dyrektywa zastępująca obecną decyzję ramową) mająca stanowić odpowiedź na zagrożenie wynikające z ataków na wielką skalę na systemy informatyczne (botnety) oraz, w przypadku ataków popełnianych przez sprawców ukrywających swoją prawdziwą tożsamość i stawiających w cieniu podejrzeń prawowitych właścicieli tożsamości, na problem skuteczności punktów kontaktowych organów ścigania państw członkowskich oraz braku danych statystycznych na temat cyberataków.

Wariant ten przewiduje wprowadzenie specjalnie ukierunkowanych (tzn. o ograniczonym zakresie) przepisów mających zapobiegać atakom na wielką skalę, których celem są systemy informatyczne. Takim udoskonalonym przepisom towarzyszyłyby środki nielegislacyjne służące zacieśnieniu operacyjnej współpracy transgranicznej w zwalczaniu takich ataków, która z kolei ułatwiałaby wykonywanie środków legislacyjnych. Środki te miałyby na celu zwiększenie gotowości, bezpieczeństwa i odporności krytycznej infrastruktury informatycznej oraz wymianę najlepszych praktyk.

- Wariant strategiczny nr 4: wprowadzenie kompleksowych unijnych przepisów przeciwko cyberprzestępczości

Wariant ten pociągałby za sobą ustanowienie nowych kompleksowych przepisów UE. Obok wprowadzenia środków „miękkiego" prawa z wariantu strategicznego nr 2 oraz aktualizacji z wariantu nr 3, służyłaby on rozwiązaniu także innych problemów prawnych związanych z wykorzystaniem Internetu. Środki te dotyczyłyby nie tylko ataków na systemy informatyczne, lecz także takich kwestii jak cyberprzestępstwa finansowe, nielegalne treści w Internecie, gromadzenie/przechowywanie/przekazywanie dowodów elektronicznych oraz bardziej szczegółowe normy jurysdykcyjne. Przepisy funkcjonowałyby obok Konwencji Rady Europy o cyberprzestępczości oraz obejmowałyby towarzyszące środki nielegislacyjne wspomniane powyżej.

- Wariant strategiczny nr 5: aktualizacji Konwencji Rady Europy o cyberprzestępczości.

Wariant ten wymagałby istotnej renegocjacji obecnej konwencji, co jest procesem długotrwałym i wykraczającym poza ramy czasowe działania zaproponowanego w ocenie skutków. Jak się wydaje, na szczeblu międzynarodowym brakuje woli do renegocjacji konwencji. Dlatego też nie można uznać aktualizacji konwencji za opcję realną, ponieważ jej przeprowadzenie nie byłoby możliwe w wyznaczonym terminie działania.

Preferowany wariant strategiczny połączenie środków nielegislacyjnych (wariant nr 2) ze specjalnie ukierunkowaną aktualizacją decyzji ramowej (wariant nr 3)

Analiza skutków gospodarczych i społecznych oraz wpływu na prawa podstawowe wskazuje, że warianty nr 2 i 3 stanowią najlepsze podejście do omawianych problemów i najlepiej umożliwiają osiągnięcie celów niniejszego wniosku.

W toku przygotowywania wniosku Komisja przeprowadziła ocenę skutków.

3. ASPEKTY PRAWNE WNIOSKU

- **Krótki opis proponowanych działań**

Dyrektywa uchyli wprawdzie decyzję ramową 2005/222/WSiSW, jednak zachowa jej obecne przepisy z dodaniem następujących nowych elementów:

– w zakresie prawa karnego materialnego w ujęciu ogólnym dyrektywa:

A. penalizuje wytwarzanie, sprzedaż, dostarczanie w celu używania, przywóz, dystrybucję oraz inne sposoby udostępniania urządzeń/narzędzi służących do popełniania rozpatrywanych przestępstw.

B. zawiera okoliczności obciążające:

- przeprowadzanie ataków na wielką skalę – problem botnetów lub podobnych narzędzi zostałby uwzględniony poprzez wprowadzenie nowej okoliczności obciążającej, czyli czyn polegający na stworzeniu botnetu lub innego podobnego narzędzia stanowiłby okoliczność obciążającą przy popełnianiu przestępstw wyszczególnionych w obecnej decyzji ramowej;

- jeśli ataki te popełniane są przez sprawcę ukrywającego swoją prawdziwą tożsamość, a podejrzenia spadają na prawowitego właściciela tożsamości. Wszelkie takie przepisy musiałyby odpowiadać zasadom legalizmu oraz proporcjonalności przestępstw i kar kryminalnych oraz być zgodne z obowiązującymi przepisami dotyczącymi ochrony danych osobowych[13].

C. wprowadza nowe przestępstwo „nielegalnego przechwytywania”

[13] Takimi jak dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002, s. 37 (obecnie poddawana rewizji), oraz takich jak ogólna dyrektywa o ochronie danych nr 95/46/WE.

D. wprowadza środki mające poprawić współpracę europejskich wymiarów sprawiedliwości w sprawach karnych poprzez udoskonalenie obecnej struktury całodobowych punktów kontaktowych[14];

- proponuje się wprowadzić obowiązek realizacji wniosku o pomoc złożonego przez operacyjne punkty kontaktowe (określone w art. 14 dyrektywy) w wyznaczonym terminie; Konwencja o cyberprzestępczości nie zawiera wiążącego postanowienia tego rodzaju. Ma to zagwarantować, by punkty kontaktowe wskazały w wyznaczonym czasie, czy będą w stanie zrealizować wniosek o pomoc, oraz kiedy punkt kontaktowy, który o nią wystąpił, może tego oczekiwać. Nie określono natomiast, na czym ta realizacja ma konkretnie polegać.

E. stanowi odpowiedź na potrzebę dostarczania danych statystycznych dotyczących cyberprzestępczości nakładając na państwa członkowskie obowiązek zagwarantowania istnienia odpowiedniego systemu umożliwiającego rejestrowanie, sporządzanie i dostarczanie danych statystycznych dotyczących przestępstw, o których mowa w obowiązującej decyzji ramowej, oraz nowo dodanego „nielegalnego przechwytywania".

W definicjach przestępstw wyszczególnionych w art. 3, 4 i 5 (nielegalny dostęp do systemów informatycznych, nielegalne ingerowanie w system oraz nielegalne przechwytywanie) dyrektywa zawiera przepis umożliwiający kryminalizację wyłącznie tych „przypadków, które nie są przypadkami mniejszej wagi" w procesie transpozycji dyrektywy do prawa krajowego. Ten element elastyczności ma umożliwić państwom członkowskim pozostawienie poza obrębem regulacji przypadków, które *in abstracto* objęte byłyby podstawową definicją, ale nie są uznawane za szkodliwe dla chronionych interesów prawnych; dotyczy to np. czynów młodych ludzi, którzy próbują wykazać się specjalistycznymi umiejętnościami w zakresie technologii informatycznych. Możliwość ograniczenia zakresu kryminalizacji nie powinna jednak prowadzić do wprowadzenia dodatkowych znamion przestępstwa obok tych, które zostały już wprowadzone w dyrektywie, ponieważ prowadziłoby to do sytuacji, w której zakresem regulacji objęte byłyby wyłącznie przestępstwa, przy których popełnieniu wystąpiły okoliczności obciążające. W procesie transpozycji państwa członkowskie powinny w szczególności powstrzymać się od uzupełniania opisu podstawowych przestępstw o nowe znamiona, takie jak np. szczególny zamiar uzyskania nielegalnych dochodów z przestępstwa lub wystąpienie szczególnego efektu, takiego jak spowodowanie znacznych szkód.

- **Podstawa prawna**

Artykuł 83 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej[15].

- **Zasada pomocniczości**

Zasada pomocniczości dotyczy działań Unii Europejskiej. Cele wniosku nie mogą być osiągnięte w sposób wystarczający przez państwa członkowskie z następujących względów:

cyberprzestępczość, a dokładniej mówiąc ataki na systemy informatyczne, mają istotny wymiar transgraniczny, najbardziej ewidentny przypadku ataków na wielką skalę, ponieważ

---

[14] Wprowadzonej konwencją oraz decyzją ramową 2005/222/WSiSW o atakach na systemy informatyczne.

[15] Dz.U. C 83 z 30.3.2010, s. 49.

elementy służące łącznie do ataku znajdują się często w różnych miejscach, w różnych państwach. Wymaga to działań ze strony UE, w szczególności w celu dotrzymania kroku obecnym tendencjom do ataków na dużą skalę w Europie i na świecie. Do działań na szczeblu UE i aktualizacji decyzji ramowej 2005/222/WSiSW wezwano także w konkluzjach Rady z listopada 2008 r.[16], ponieważ cel, jakim jest skuteczna ochrona obywateli przed cyberprzestępczością nie może być dostatecznie osiągnięty przez same państwa członkowskie.

Cele przedstawione w niniejszym wniosku można zrealizować lepiej poprzez działania na szczeblu Unii Europejskiej z poniższych przyczyn:

wniosek jeszcze bardziej zbliży prawo karne materialne państw członkowskich i przepisy proceduralne, co będzie miało pozytywny wpływ na zwalczanie tych przestępstw. Po pierwsze, jest to sposób zapobieżenia przemieszczaniu się przestępców do państw członkowskich, w których przepisy przeciwko cyberatakom są łagodniejsze. Po drugie, wspólne definicje umożliwiają wymianę informacji oraz gromadzenie i porównywanie właściwych danych. Po trzecie, zwiększa się także efektywność środków prewencyjnych podejmowanych w całej UE oraz współpracy międzynarodowej.

W związku z powyższym niniejszy wniosek jest zgodny z zasadą pomocniczości.

- **Zasada proporcjonalności**

Wniosek jest zgodny z zasadą proporcjonalności z następujących względów:

niniejsza decyzja ramowa ogranicza się do minimum koniecznego dla osiągnięcia tych celów na poziomie europejskim i nie wykracza poza to, co jest do tego niezbędne biorąc pod uwagę potrzebę stanowienia precyzyjnych przepisów prawnokarnych.

- **Wybór instrumentów**

Proponowany instrument: dyrektywa.

Inne środki byłyby niewłaściwe z następujących względów:

podstawa prawna wymaga dyrektywy.

Środki nielegislacyjne i samoregulacja poprawiłyby sytuację w niektórych dziedzinach, w których zasadnicze znaczenie ma wprowadzenie w życie już obowiązujących przepisów. Jednak w innych dziedzinach, gdzie niezbędne są nowe przepisy, korzyści byłyby umiarkowane.

4. WPŁYW NA BUDŻET

Wniosek ma niewielki wpływ na unijny budżet. Ponad 90 % szacunkowych kosztów wynoszących 5 913 000 EUR poniosłyby państwa członkowskie, przy czym istnieje możliwość wystąpienia o finansowanie z UE w celu obniżenia tych kosztów.

---

[16] „Uzgodniona strategia pracy i konkretnych środków służących zwalczaniu cyberprzestępczości", 2987. posiedzenie RADY DS. WYMIARU SPRAWIEDLIWOŚCI I SPRAW WEWNĘTRZNYCH, Bruksela, 27-28 listopada 2008 r.

5. INFORMACJE DODATKOWE

- **Uchylenie obowiązującego prawodawstwa**

Przyjęcie niniejszego wniosku doprowadzi do uchylenia obowiązującego prawodawstwa.

- **Zakres terytorialny**

Niniejsza dyrektywa skierowana jest do państw członkowskich zgodnie z Traktatami.

2010/0273 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności

jego art. 83 ust. 1,

uwzględniając wniosek Komisji Europejskiej[17],

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego,

uwzględniając opinię Komitetu Regionów,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Niniejsza dyrektywa ma na celu zbliżenie przepisów prawa karnego w państwach członkowskich w dziedzinie ataków na systemy informatyczne oraz poprawę współpracy między organami sądowymi i innymi właściwymi organami, w tym policją i pozostałymi wyspecjalizowanymi organami ścigania państw członkowskich.

(2) Ataki na systemy informatyczne, w szczególności ze względu na zagrożenie ze strony przestępczości zorganizowanej, są coraz bardziej niebezpieczne, narastają również obawy o możliwość ataków o charakterze terrorystycznym lub mających podłoże polityczne ukierunkowanych na systemy informatyczne stanowiące element infrastruktury krytycznej państw członkowskich i Unii. Zagraża to dążeniom do zapewnienia bezpieczniejszego społeczeństwa informacyjnego oraz przestrzeni wolności, bezpieczeństwa i sprawiedliwości, dlatego też wymaga reakcji na szczeblu Unii Europejskiej.

(3) Istnieją dowody wskazujące na tendencję do coraz bardziej niebezpiecznych i ponawianych ataków na wielką skalę przeprowadzanych na systemy informatyczne o zasadniczym znaczeniu dla państw lub poszczególnych funkcji w sektorze publicznym lub prywatnym. Tendencji tej towarzyszy w coraz szerszym stopniu tworzenie coraz bardziej wyrafinowanych narzędzi, z których przestępcy mogą korzystać do przeprowadzania różnego rodzaju cyberataków.

---

[17] Dz.U. C […] z […], s. […].

(4) Wspólne definicje w tej dziedzinie, w szczególności definicji systemów informatycznych oraz danych komputerowych, mają istotne znaczenie dla zagwarantowania przyjęcia przez państwa członkowskie spójnego podejścia do stosowania niniejszej dyrektywy.

(5) Zachodzi potrzeba zapewnienia wspólnego podejścia do kwestii znamion przestępstwa poprzez powszechne wprowadzenie przestępstw polegających na nielegalnym dostępie do systemu informatycznego, nielegalnym ingerowaniu w system, nielegalnym ingerowaniu w dane oraz nielegalnym przechwytywaniu.

(6) Państwa członkowskie powinny przewidzieć kary za ataki na systemy informatyczne. Przewidziane kary powinny być skuteczne, proporcjonalne i odstraszające.

(7) Należy przewidzieć surowsze kary za ataki na systemy informatyczne popełniane przez organizację przestępczą, zdefiniowaną w decyzji ramowej Rady 2008/841/WSiSW z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej[18], ataki przeprowadzane w dużej skali, lub w sytuacji, gdy sprawca przestępstwa ukrywa swoją prawdziwą tożsamość, narażając na podejrzenia prawowitego właściciela tożsamości. Należy również przewidzieć surowsze kary w sytuacji, gdy atak spowodował poważne szkody lub naruszył zasadnicze interesy.

(8) W konkluzjach Rady z dnia 27-28 listopada 2008 r. zaznaczono, że Komisja powinna wraz z państwami członkowskimi opracować nową strategię, przy uwzględnieniu treści Konwencji Rady Europy z 2001 r. o cyberprzestępczości. Konwencja ta wyznacza prawne ramy odniesienia dla zwalczania cyberprzestępczości, w tym ataków na systemy informatyczne. Niniejsza dyrektywa opiera się na tej konwencji.

(9) Ze względu na to, że ataki mogą być przeprowadzone na różna sposoby oraz uwzględniając szybki rozwój sprzętu i oprogramowania, w niniejszej dyrektywie mowa jest o „narzędziach", które mogą zostać wykorzystane do popełnienia przestępstw w niej wyszczególnionych. Narzędziami jest przykładowo „złośliwe" oprogramowanie, w tym botnety, wykorzystywane do przeprowadzania cyberataków.

(10) Dyrektywa nie służy ustanowieniu odpowiedzialności karnej za czyny popełniane w celach nieprzestępczych, takie jak dozwolone testowanie lub zabezpieczanie systemów informatycznych.

(11) Niniejsza dyrektywa zwiększa znaczenie sieci, takich jak G8 oraz sieć całodobowych punktów kontaktowych działających siedem dni w tygodniu Rady Europy, w wymianie informacji mającej zagwarantować niezwłoczne udzielenie pomocy w celu prowadzenia dochodzenia lub innego postępowania w sprawach przestępstw związanych z systemami i danymi informatycznymi lub w celu gromadzenia dowodów przestępstwa w formie elektronicznej. Ze względu na to, jak szybko można przeprowadzić ataki na wielką skalę, państwa członkowskie powinny być zdolne do szybkiego reagowania na wnioski składane w pilnym trybie w ramach tej sieci punktów kontaktowych. Taka pomoc powinna obejmować ułatwienie lub bezpośrednią realizację takich środków jak: doradztwo techniczne, zachowanie danych, gromadzenie dowodów, udzielenie informacji prawnych oraz lokalizacja podejrzanych.

---

[18] Dz.U. L 300 z 11.11.2008, s. 42.

(12) Zachodzi potrzeba gromadzenia danych o przestępstwach, o których mowa w niniejszej dyrektywie, w celu uzyskania bardziej kompletnego obrazu problemu na szczeblu Unii, a tym samym przyczynienia się do opracowania skuteczniejszych środków zaradczych. Dane te pomogą ponadto wyspecjalizowanym agencjom, takim jak Europol i Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji, lepiej ocenić zakres zjawiska cyberprzestępczości oraz stan bezpieczeństwa sieci i informacji w Europie.

(13) Znaczące luki i różnice w przepisach państw członkowskich w dziedzinie ataków na systemy informatyczne mogą utrudniać walkę z przestępczością zorganizowaną i terroryzmem oraz komplikować skuteczną współpracę sądową i policyjną w tej dziedzinie. Międzynarodowy i transgraniczny charakter współczesnych systemów informatycznych nadaje atakom na takie systemy wymiar transgraniczny, przez co jeszcze pilniejsza staje się potrzeba dalszych działań na rzecz zbliżenia przepisów prawnokarnych w tej dziedzinie. Ponadto koordynacja ścigania przypadków ataków na systemy informatyczne powinna zostać ułatwiona dzięki przyjęciu decyzji ramowej Rady 2009/948/WSiSW w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów.

(14) Ponieważ cele niniejszej dyrektywy, tzn. zagwarantowanie, by ataki na systemy informatyczne były karane we wszystkich państwach członkowskich skutecznymi, proporcjonalnymi i odstraszającymi karami kryminalnymi oraz poprawa współpracy wymiarów sprawiedliwości i propagowanie tej współpracy poprzez usunięcie potencjalnych komplikacji, nie może zostać wystarczająco osiągnięty przez państwa członkowskie, ponieważ wymaga wspólnych i zgodnych ze sobą przepisów, i dlatego może zostać lepiej osiągnięty na szczeblu Unii, ta ostatnia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Niniejsza dyrektywa nie wykracza poza zakres niezbędny do osiągnięcia tych celów.

(15) Wszelkie dane osobowe przetworzone w kontekście wdrażania niniejszej dyrektywy powinny być chronione zgodnie z przepisami ustanowionymi w decyzji ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[19] w odniesieniu do tych działań związanych z przetwarzaniem, które wchodzą w zakres tego aktu oraz rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[20].

(16) Niniejsza dyrektywa respektuje prawa podstawowe oraz jest zgodna z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej, w tym z zasadami ochrony danych osobowych, swobody wypowiedzi i informacji, prawem do rzetelnego procesu, domniemaniem niewinności i prawem do obrony, jak również zasadami legalizmu i proporcjonalności przestępstw i kar kryminalnych. W szczególności niniejsza dyrektywa zmierza do pełnego zagwarantowania poszanowania tych praw i zasad oraz musi być odpowiednio do tego wdrażana.

---

[19] Dz.U. L 350 z 30.12.2008, s. 60.
[20] Dz.U. L 8 z 12.1.2001, s. 1.

(17) [Zgodnie z art. 1, 2, 3 i 4 Protokołu w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości załączonego do Traktatu o funkcjonowaniu Unii Europejskiej, Zjednoczone Królestwo i Irlandia notyfikowały życzenie uczestniczenia w przyjęciu i stosowaniu niniejszej dyrektywy] LUB [Bez uszczerbku dla art. 4 Protokołu w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, Zjednoczone Królestwo i Irlandia nie będą uczestniczyć w przyjęciu niniejszej dyrektywy i nie będzie ona ich wiązać ani mieć do nich zastosowania].

(18) Zgodnie z art.1 i 2 Protokołu w sprawie stanowiska Danii załączonego do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczy w przyjęciu niniejszej dyrektywy, w związku z czym nie jest nią związana ani nie ma ona do niej zastosowania.

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

Artykuł 1
Przedmiot

Niniejsza dyrektywa określa przestępstwa w dziedzinie ataków na systemy informatyczne oraz ustanawia reguły minimalne dotyczące kar za takie przestępstwa. Służy ona również wprowadzeniu wspólnych przepisów w celu zapobiegania takim atakom oraz poprawy współpracy wymiarów sprawiedliwości w sprawach karnych w tej dziedzinie.

Artykuł 2
Definicje

Do celów niniejszej dyrektywy stosuje się następujące definicje:

a) "system informatyczny" oznacza wszelkie urządzenia lub grupę połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez nie w celach ich eksploatacji, użycia, ochrony lub utrzymania;

b) „dane komputerowe” oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie nadającej się do przetwarzania w systemie informatycznym, włącznie z programem umożliwiającym spowodowanie wykonania funkcji przez system informatyczny;

c) „osoba prawna” oznacza wszelkie podmioty mające taki status na mocy właściwego prawa, z wyjątkiem organów państwowych lub innych organów publicznych wykonujących władzę państwową oraz publicznych organizacji międzynarodowych;

d) d) „bezprawnie” oznacza dostęp lub ingerencję, na którą właściciel, inny posiadacz prawa do systemu lub jego części nie udzielił zgody lub która nie jest dozwolona na mocy prawa krajowego

Artykuł 3

Nielegalny dostęp do systemów informatycznych

Państwa członkowskie podejmują środki niezbędne dla zagwarantowania, by umyślne i bezprawne uzyskiwanie dostępu do całości lub części systemu informatycznego było karalne jako przestępstwo, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Artykuł 4

Nielegalne ingerowanie w system

Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne poważne i bezprawne utrudnienie lub zakłócenie funkcjonowania systemu informatycznego poprzez wprowadzenie, przekazywanie, uszkadzanie, usuwanie, pogarszanie, zmienianie albo eliminowanie danych lub czynienie ich niedostępnymi, było karalne jako przestępstwo, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Artykuł 5

Nielegalne ingerowanie w dane

Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne bezprawne usuwanie, uszkadzanie, pogarszanie, zmienianie albo eliminowanie danych lub czynienie ich niedostępnymi było karalne jako przestępstwo, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi.

Artykuł 6

Nielegalne przechwytywanie

Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne przechwytywanie środkami technicznymi niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego, w tym emisji elektromagnetycznych z systemu informatycznego zawierającego takie dane komputerowe, było karalne jako przestępstwo, jeżeli zostało dokonane bezprawnie.

Artykuł 7

Narzędzia używane do popełniania przestępstw

Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by wytwarzanie, sprzedaż, dostarczanie w celu użycia, przywóz, posiadanie, rozpowszechnianie lub udostępnianie w inny sposób następujących elementów było karalne jako przestępstwo, jeżeli zostało dokonane umyślnie i bezprawnie w celu popełnienia przestępstw, o których mowa w art. 3-6:

a) urządzenia, w tym programu komputerowego, zaprojektowanego lub przystosowanego głównie do celu popełniania przestępstw, o których mowa w art. 3-6;

b) hasła komputerowego, kodu dostępu lub podobnych danych umożliwiających dostęp do całości lub części systemu informatycznego;

Artykuł 8

Podżeganie, pomocnictwo i usiłowanie

1. Państwa członkowskie zapewniają, by podżeganie do przestępstw, o których mowa w art. 3-7, oraz pomocnictwo w tych przestępstwach, było karane jako przestępstwo.

2. Państwa członkowskie zapewniają, by usiłowanie popełnienia przestępstw, o których mowa w art. 3-6, było karane jako przestępstwo.

Artykuł 9

Kary

1. Państwa członkowskie przyjmują środki niezbędne do zagwarantowania, by przestępstwa, o których mowa w art. 3-8, podlegały skutecznym, proporcjonalnym i odstraszającym karom kryminalnym.

2. Państwa członkowskie przyjmują środki niezbędne do zagwarantowania, by przestępstwa, o których mowa w art. 3-7, podlegały karom kryminalnym w maksymalnej wysokości nie mniejszej niż dwa lata pozbawienia wolności.

Artykuł 10

Okoliczności obciążające

1. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by przestępstwa, o których mowa w art. 3-7, podlegały karom kryminalnym o maksymalnej wysokości nie mniejszej niż pięć lat pozbawienia wolności, jeżeli zostały popełnione w ramach organizacji przestępczej określonej w decyzji ramowej 2008/841/WSiSW.

2. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by przestępstwa, o których mowa w art. 3-6, podlegały karom kryminalnym o maksymalnej wysokości nie mniejszej niż pięć lat pozbawienia wolności, jeżeli zostały popełnione z wykorzystaniem narzędzia zaprojektowanego do przeprowadzania ataków dotykających znacznej liczby systemów informatycznych lub ataków powodujących znaczne szkody, takie jak zakłócenie usług systemowych, straty finansowe lub utrata danych osobowych.

3. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by przestępstwa, o których mowa w art. 3-6 podlegały karom kryminalnym o maksymalnej wysokości nie mniejszej niż pięć lat pozbawienia wolności jeżeli zostały popełnione przez sprawcę ukrywającego swoją prawdziwą tożsamość i narażającego na podejrzenia prawowitego właściciela tożsamości.

Artykuł 11

Odpowiedzialność osób prawnych

1. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by osoby prawne mogły zostać pociągnięte do odpowiedzialności za przestępstwa, o których mowa w art. 3–8, popełnione na ich korzyść przez jakąkolwiek osobę działającą

indywidualnie albo jako członek organu osoby prawnej i pełniącą funkcje kierownicze w tej osobie prawnej, w oparciu o jedną z poniższych podstaw:

a) prawo reprezentowania danej osoby prawnej;

b) uprawnienie do podejmowania decyzji w imieniu danej osoby prawnej;

c) uprawnienie do sprawowania kontroli w ramach osoby prawnej.

2. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by osoby prawne mogły podlegać odpowiedzialności, gdy brak nadzoru przez osobę, o której mowa w ust. 1, umożliwił popełnienie, przez osobę podlegającą danej osobie prawnej, któregokolwiek z przestępstw, o których mowa w art. 3-8, na korzyść tej osoby prawnej.

3. Odpowiedzialność osoby prawnej na podstawie ust. 1 i 2 nie wyklucza karnego postępowania sądowego przeciw osobom fizycznym, które są sprawcami przestępstw określonych w art. 3–8 lub pomocnikami w tych przestępstwach.

Artykuł 12
Kary dla osób prawnych

1. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by osoba prawna pociągnięta do odpowiedzialności na mocy art. 11 ust. 1 podlegała skutecznym, proporcjonalnym i odstraszającym karom, w tym grzywnom o charakterze kryminalnym lub innym, oraz mogącym obejmować inne sankcje, na przykład:

   a) pozbawienie prawa do korzystania ze świadczeń publicznych lub pomocy publicznej;

   b) czasowy lub stały zakaz prowadzenia działalności gospodarczej;

   c) umieszczenie pod nadzorem sądowym;

   d) likwidację sądową;

   e) czasowe lub stałe zamknięcie zakładów wykorzystanych w celu popełnienia przestępstwa.

2. Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by osoba prawna pociągnięta do odpowiedzialności na mocy art. 11 ust. 2 podlegała skutecznym, proporcjonalnym i odstraszającym karom lub środkom.

Artykuł 13
Jurysdykcja

1. Państwa członkowskie ustanawiają swoją jurysdykcję w odniesieniu do przestępstw, o których mowa w art. 3-8, popełnionych:

   a) w całości lub w części na terytorium danego państwa członkowskiego lub

b) przez jednego z ich obywateli lub osobę mającą miejsce zwykłego pobytu na jego terytorium; lub

c) na korzyść osoby prawnej mającej główną siedzibę na terytorium tego państwa członkowskiego.

2. Ustanawiając swoją jurysdykcję zgodnie z ust. 1 lit. a), państwa członkowskie zapewniają, by obejmowała ona przypadki, w których:

a) sprawca popełnia przestępstwo, znajdując się na terytorium danego państwa członkowskiego, niezależnie od tego, czy przestępstwo jest skierowane przeciwko systemowi informatycznemu na jego terytorium; lub

b) przestępstwo jest skierowane przeciwko systemowi informatycznemu na terytorium danego państwa członkowskiego, niezależnie od tego, czy sprawca popełnia przestępstwo, znajdując się na jego terytorium.

Artykuł 14
Wymiana informacji

1. Do celów wymiany informacji odnoszących się do przestępstw, o których mowa w art. 3-8, oraz zgodnie z przepisami o ochronie danych, państwa członkowskie korzystają z istniejącej sieci operacyjnych punktów kontaktowych dostępnych 24 godziny na dobę oraz przez siedem dni w tygodniu. Państwa członkowskie zapewniają również procedury umożliwiające im zareagowanie na pilne wnioski w czasie nie dłuższym niż osiem godzin. Reakcja ta polega przynajmniej na poinformowaniu, czy udzielona zostanie odpowiedź na wniosek i w jakiej formie oraz kiedy to nastąpi.

2. Państwa członkowskie informują Komisję o swoich wyznaczonych punktach kontaktowych do celów wymiany informacji na temat przestępstw, o których mowa w art. 3-8. Komisja przekazuje te informacje pozostałym państwom członkowskim.

Artykuł 15
Monitorowanie i statystyki

1. Państwa członkowskie zapewniają istnienie systemu umożliwiającego rejestrowanie, wytwarzanie i dostarczanie danych statystycznych o przestępstwach, o których mowa w art. 3-8.

2. Dane statystyczne, o których mowa w ust. 1, obejmują co najmniej liczbę przestępstw, o których mowa w art. 3-8, zgłoszonych państwom członkowskim oraz działania podjęte w wyniku tych zgłoszeń, jak również wskazują, w skali rocznej , liczbę zgłoszonych przypadków, które były przedmiotem dochodzenia, liczbę osób oskarżonych oraz liczbę osób, które zostały skazane za przestępstwa, o których mowa w art. 3-8.

3. Państwa członkowskie przekazują Komisji dane zgromadzone zgodnie z niniejszym artykułem. Państwa członkowskie zapewniają również publikację skonsolidowanego zestawienia tych sprawozdań statystycznych.

Artykuł 16
Uchylenie decyzji ramowej 2005/222/WSiSW

Niniejszym uchyla się decyzję ramową 2005/222/WSiSW, bez uszczerbku dla zobowiązań państw członkowskich dotyczących terminów jej transpozycji do prawa krajowego.

Odniesienia do uchylonej decyzji ramowej traktuje się jako odniesienia do niniejszej dyrektywy.

Artykuł 17
Transpozycja

1. Państwa członkowskie wprowadzą w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy najpóźniej [w terminie dwóch lat od daty jej przyjęcia]. Niezwłocznie przekazują Komisji tekst tych przepisów oraz tabelę korelacji pomiędzy tymi przepisami a niniejszą dyrektywą. Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.

2. Państwa członkowskie przekazują Komisji tekst podstawowych przepisów prawa krajowego, przyjętych w dziedzinie objętej niniejszą dyrektywą.

Artykuł 18
Sprawozdawczość

1. Do dnia [CZTERY LATA OD DATY PRZYJĘCIA], a następnie co trzy lata, Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie w sprawie stosowania niniejszej dyrektywy w państwach członkowskich, w tym wszelkie niezbędne propozycje.

2. Państwa członkowskie przesyłają Komisji wszystkie informacje odpowiednie do sporządzenia sprawozdania, o którym mowa w ust. 1. Informacje te obejmują szczegółowy opis środków legislacyjnych i nielegislacyjnych przyjętych w ramach wdrażania niniejszej dyrektywy.

Artykuł 19
Wejście w życie

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 20
Adresaci

Niniejsza dyrektywa jest skierowana do państw członkowskich zgodnie z Traktatami.

Sporządzono w Brukseli dnia

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*