**Sylwia Ćmiel**

# OCHRONA NIELETNICH W CYBERPRZESTRZENI POPRZEZ BEZPIECZNE ŚRODOWISKO ONLINE W DZIAŁANIACH UNII EUROPEJSKIEJ

# Wstęp

Działania Unii Europejskiej na poziomie zarówno unijnym, jak i krajowym na rzecz umacniania praw i edukacji nieletnich osób w cyberprzestrzeni, powinny zostać zintensyfikowane, aby zadbać o ich ochronę. Nieletni nie zawsze dostrzegają potencjalne zagrożenia, na jakie są narażeni w środowisku *online*, nie zawsze są też świadomi swoich ewentualnych działań.

Narażanie nieletnich na szkodliwe treści i zachowania w cyberprzestrzeni może prowadzić do niepokojących doświadczeń nieletnich w świecie wirtualnym i prowadzić do przenoszenia zachowań ryzykownych do świata rzeczywistego.

Głównym celem niniejszego artykułu jest analiza zarówno teoretyczna, jak i praktyczna aktualnych działań Unii Europejskiej w obszarze zapewnienia optymalnej ochrony nieletnich w cyberprzestrzeni poprzez wspieranie bezpiecznego środowiska *online*. Przedmiotem badań uczyniono:

1. Unijne propozycje środków ochrony nieletnich w Internecie;
2. Innowacyjne rozwiązania technicznych zabezpieczeń infrastruktury informatycznej;
3. Ochronę przed niegodziwym traktowaniem dzieci w celach seksualnych oraz wykorzystywaniem seksualnym dzieci w Internecie;
4. Współpracę z partnerami międzynarodowymi na rzecz zwalczania niegodziwego traktowania dzieci w celach seksualnych oraz wykorzystywania seksualnego dzieci w Internecie;
5. Współpracę międzynarodową Unii Europejskiej na rzecz bezpieczeństwa cybernetycznego mającą wpływ na poziom bezpieczeństwa nieletnich w cyberprzestrzeni;

5.1. Poziom krajowy,

5.2. Poziom unijny i międzynarodowy.

## 1. Unijne propozycje środków ochrony nieletnich w Internecie

Proponowane przez Unię Europejską **środki** zapobiegawcze odnoszą się do nieletnich w różnym wieku zagrożonych demoralizacją, ponieważ w zależności od wieku nieletni w różny sposób korzystają z nowych technologii i nie jest możliwe znalezienie rozwiązań jednolitych dla wszystkich z tej kategorii osób. Na szczeblu zarówno unijnym, jak i krajowym należy permanentnie wdrożyć środki zapobiegające sytuacjom, w których nieletni mają kontakt z niewłaściwymi treściami i zachowaniami przestępczymi w cyberprzestrzeni.

Zagrożenie prywatności dotyczy wprawdzie wszystkich użytkowników, jednak nieletni są grupą szczególnie na nie podatną, bowiem nie orientu-

ją się, w jaki sposób należy zmienić swoje ustawienia dotyczące prywatności i nie rozumieją ewentualnych konsekwencji swoich działań. Często też nie zdają sobie sprawy, że mogą stać się łatwym obiektem nagabywania dla celów seksualnych lub narazić się na utratę swojego dobrego imienia w cyberprzestrzeni.

Ważne jest zatem zdobywanie nie tylko przez dzieci, ale i przez rodziców, umiejętności odpowiedniego zarządzania automatycznymi ustawieniami dotyczącymi prywatności, tak aby zapewnić maksymalne bezpieczeństwo. Jak podaje Komisja Europejska w „Europejskiej strategii na rzecz lepszego Internetu dla dzieci", aż 80% rodziców jest przekonanych, że powszechniejsza dostępność i lepsza efektywność narzędzi kontroli rodzicielskiej przyczyniłyby się do bezpieczniejszego i skuteczniejszego korzystania z Internetu przez ich dzieci. Jednak średnio jedynie 28% rodziców w Europie blokuje określone strony internetowe lub instaluje filtry na stronach internetowych, które odwiedzają ich dzieci. Przy należnym poszanowaniu wolności wypowiedzi, kontrole rodzicielskie uważane są za uzupełniający środek ochrony młodszych dzieci przed oglądaniem nieodpowiednich treści w Internecie; w ramach tego środka rodzice wprowadzają ustawienia filtrujące treści i nadzorujące zachowanie dziecka w środowisku *online*. Niezbędne jest zapewnienie większej dostępności i rozpowszechnienie stosowania narzędzi kontroli rodzicielskiej w wielu językach, aby pozwolić rodzicom na świadomy wybór w zakresie wykorzystania takich narzędzi.

Ważnym wydarzeniem wzmacniającym ochronę nieletnich w Internecie było podjęcie cytowanej powyżej europejskiej strategii, która pozwala Komisji Europejskiej wspierać działania w obszarach:

1. Dokonywania analiz oraz testowania narzędzi kontroli rodzicielskiej i powiązanych usług wpierających, które mają na celu umocnienie praw rodziców i dzieci.

2. Badania rozwoju, aby rozważyć możliwości interpretacji systemów ratingów wiekowych oraz klasyfikacji treści przez skuteczne narzędzia kontroli rodzicielskiej, które funkcjonowałyby w wielu językach.

3. Podejmowania środków legislacyjnych, jeżeli podejmowane przez branżę środki samoregulacji nie przyniosą efektów.[1]

## 2. Innowacyjne rozwiązania technicznych zabezpieczeń infrastruktury informatycznej

Jednym z zagrożeń, na jakie narażone są dzieci w Internecie, jest oglądanie nieodpowiednich treści (takich jak materiały pornograficzne lub prezentujące przemoc). Celem ochrony nieletnich przed tymi zagro-

1) Por. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 02.05.2012 r. (Com(2012) 196 final)*; Europejska strategia na rzecz lepszego internetu dla dzieci*. Bruksela, s. 13-14.

żeniami powinno zatem być powszechnie stosowane, przejrzyste i spójne podejście do systemu ratingów wiekowych oraz klasyfikacji treści na obszarze nie tylko naszego kraju, ale i Unii Europejskiej w odniesieniu do szeregu treści i usług, w tym gier internetowych, aplikacji oraz treści edukacyjnych i innych treści o znaczeniu kulturowym. To również wprowadzanie innowacyjnych rozwiązań (np. ratingi według użytkownika lub ratingi automatyczne).

System powinien oferować rodzicom łatwo zrozumiałe kategorie wiekowe, przy czym należy wziąć pod uwagę, że te same treści mogą zostać uznane za odpowiednie dla różnych kategorii wiekowych w różnych krajach. Podejście to powinno być stosowane w spójny sposób we wszystkich sektorach; należy reagować na rozbieżności we wdrażaniu aktualnych systemów w odniesieniu do różnych mediów, co poprawi konkurencję na rynku.

W związku z tym Komisja Europejska będzie wspierać:

1) Środki samoregulacji w tym obszarze, rozważy ponadto potencjalne środki legislacyjne na wypadek, gdyby środki samoregulacji branży nie przyniosły oczekiwanych rezultatów.

2) Uruchomienie inter-operacyjnych platform udostępniających usługi odpowiednie do wieku – począwszy od 2014 roku.[2]

Warto również wspomnieć o ochronie szkolnej infrastruktury informatycznej. W Polsce zintegrowany i spójny system zasad bezpieczeństwa w tym obszarze zaproponował D. Stachecki[3]. Według niego nie tylko środowisko rodzinne powinno dbać o ochronę infrastruktury informatycznej ale również o tę ochronę powinna zadbać szkoła. Dlatego też ważne jest, aby w szkole m.in.:

1. Wyraźne oddzielić sieć administracyjną od urządzeń, z których korzystają uczniowie.
2. Wdrożyć regulaminy dotyczące korzystania ze sprzętu informatycznego przez uczniów, ale i nauczycieli i administrację szkoły.
3. Wprowadzać zakazy korzystania przez uczniów z komputerów na stanowiskach pracy nauczycieli.
4. Zapewnić bezpieczeństwo szkolnym serwisom internetowym - między innymi chodzi tu o nadzorowanie treści i niedopuszczanie bądź usuwanie treści nieuprawnionych, na przykład wrogich wobec konkretnych osób (uczniów lub nauczycieli).
5. Moderować forum szkolne i dbać o odpowiedni poziom dyskusji.
6. Unikać anonimowości poprzez zakładanie loginów i haseł dla wszystkich użytkowników infrastruktury informatycznej, w tym internetowej w środowisku szkolnym.

2) Tamże, s. 15.

3) Por. D. Stachecki, *Postulaty w zakresie bezpiecznej szkolnej infrastruktury informatycznej. Opis zaleceń na przykładzie praktyk*i, [w:] Ł. Wojtasik (red.), *Jak reagować na cyberprzemoc.* Poradnik dla Szkół, Fundacja Dzieci Niczyje, Warszawa 2009, s. 23-34.

# 3. Ochrona przed niegodziwym traktowania dzieci w celach seksualnych oraz wykorzystywania seksualnego dzieci w Internecie

Ochrona nieletnich w cyberprzestrzeni poprzez stwarzanie bezpiecznego środowiska *online* wiąże się również z ochroną przed niegodziwym traktowaniem dzieci w celach seksualnych oraz wykorzystywaniem seksualnym dzieci w Internecie.

Internet w coraz większym stopniu wykorzystywany jest w celu rozpowszechniania zdjęć prezentujących niegodziwe traktowanie dzieci w celach seksualnych. Występuje tu szereg problemów, dlatego konieczna jest identyfikacja, ratowanie i wspieranie ofiar; podejmowanie działań przeciwko sprawcom oraz ograniczanie nieustannego obiegu zdjęć poprzez wykrywanie i usuwanie zdjęć prezentujących niegodziwe traktowanie dzieci w celach seksualnych z Internetu i zapobieganie ich ponownemu umieszczaniu.

Powinna zostać zwiększona widzialność istniejących punktów zgłoszeniowych (linie interwencyjne), w których obywatele mogą zgłaszać nielegalne treści; należy ponadto umocnić powiązania z wszelkimi ogólnoeuropejskimi mechanizmami i środkami zgłaszania cyberprzestępczości. Należy usprawnić procedury systematycznego wykrywania i usuwania zdjęć prezentujących niegodziwe traktowanie dzieci w celach seksualnych oraz zapobiegania ich ponownemu umieszczaniu w Internecie. Podejmowane w tym obszarze działania muszą być zgodne z nową Dyrektywą unijną *w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej,* jak również z obowiązującymi przepisami z zakresu ochrony danych osobowych i Kartą praw podstawowych Unii Europejskiej. Wobec tego Komisja Europejska:

- będzie wspierała współpracę między branżą, organami ścigania oraz telefonicznymi liniami interwencyjnymi w celu usprawnienia procesu i skrócenia czasu, w jakim usuwane są zdjęcia prezentujące niegodziwe traktowanie dzieci w celach seksualnych;

- będzie koordynować wymianę narzędzi i zasobów oraz w dalszym ciągu wspierać sieć INHOPE, która skupia linie interwencyjne, w celu ułatwienia obywatelom zgłaszania nielegalnych treści, podejmowania działań następczych zmierzających do zmniejszenia opóźnień w usuwaniu treści i rozpoznawania możliwości zwiększenia widzialności tych działań w społeczeństwie;

- będzie wspierać badania i rozwój w celu opracowywania i uruchamiania innowacyjnych rozwiązań technicznych na rzecz dochodzeń policyjnych, zwłaszcza w celu skuteczniejszej identyfikacji oraz przyporządkowania materiałów prezentujących niegodziwe traktowanie dzieci w celach seksualnych, rozpowszechnianych za pośrednictwem różnych kanałów

w Internecie, oraz w celu zapobiegania ponownemu umieszczaniu zdjęć prezentujących niegodziwe traktowanie dzieci w celach seksualnych;

- będzie wspierać przeprowadzanie szkoleń dla organów ścigania;
- przyjmie inicjatywę horyzontalną w sprawie procedur zgłaszania i podejmowania działań. Będzie ona ukierunkowana przede wszystkim na znoszenie barier utrudniających skuteczne mechanizmy zgłaszania i usuwania nielegalnych treści wszelkiego rodzaju, w tym zdjęć prezentujących niegodziwe traktowanie dzieci w celach seksualnych.[4]

Zgodnie z cytowaną powyżej Dyrektywą unijną *w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej* - państwa członkowskie powinny podjąć stosowne działania mające na celu powołanie służb informacyjnych, których zadaniem będzie dostarczanie informacji, jak rozpoznawać oznaki niegodziwego traktowania w celach seksualnych oraz wykorzystywania seksualnego[5].

Pornografia dziecięca, czyli obrazy przestawiające niegodziwe traktowanie dzieci w celach seksualnych, to szczególny rodzaj treści, której nie można interpretować jako wyrażanie opinii. W celu zwalczania tego zjawiska należy ograniczyć obieg materiałów przedstawiających niegodziwe traktowanie dzieci poprzez utrudnienie sprawcom wprowadzania takich treści do publicznie dostępnych stron internetowych. Dlatego konieczne są działania w celu usuwania takich treści oraz zatrzymywania osób odpowiedzialnych za produkcję, dystrybucję lub pobieranie obrazów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych.

Z myślą o wspieraniu działań Unii Europejskiej na rzecz zwalczania pornografii dziecięcej państwa członkowskie powinny dokładać wszelkich starań, aby współpracować z państwami trzecimi w zakresie zabezpieczenia usuwania takich treści z serwerów znajdujących się na ich terytorium. Jednakże pomimo takich wysiłków, usuwanie u źródła treści zawierających pornografię dziecięcą jest często niemożliwe, w przypadku gdy oryginalne materiały znajdują się poza terytorium Unii Europejskiej, ze względu na brak woli współpracy ze strony państwa, w którym znajdują się serwery, lub ze względu na to, że procedura prowadząca do usunięcia tych materiałów w danym państwie jest wyjątkowo długotrwała. Można zatem ustanowić także mechanizmy blokowania dostępu z terytorium Unii Europejskiej do stron internetowych, w odniesieniu do których ustalono, że zawierają pornografię dziecięcą lub służą do jej rozpowszechniania. Środki podejmowane przez państwa członkowskie na mocy omawianej dyrektywy w celu usunięcia lub, w odpowiednich przypadkach, blokowania stron internetowych zawierających pornografię dziecięcą mogą opierać się na różnych rodzajach dzia-

4) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 02.05.2012 r. (Com(2012) 196 final)*; Europejska strategia na rzecz lepszego internetu dla dzieci*. Bruksela 2012 r., s. 18.

5) Por. M. Sitek, *Prawne i instytucjonalne ramy zwalczania, handlu ludźmi,* [w:] *Wykorzystywanie człowieka w XX i XXI wieku*, Olsztyn 2012.

łań publicznych, np. legislacyjnych, nielegislacyjnych, sądowych lub innych. W tym kontekście dyrektywa nie stanowi uszczerbku dla dobrowolnych działań podejmowanych przez dostawców usług internetowych w celu zapobiegania niewłaściwemu wykorzystywaniu świadczonych przez nich usług ani dla jakiegokolwiek wsparcia tych działań ze strony państw członkowskich.

Bez względu na rodzaj podstawy lub metody wybranej dla takich działań państwa członkowskie powinny zagwarantować, że zapewnia ona stosowny poziom pewności prawnej i przewidywalności dla użytkowników i usługodawców. Zarówno w celu usuwania, jak i blokowania treści przedstawiających niegodziwe traktowanie dzieci w celach seksualnych należy ustanowić i umacniać współpracę między organami publicznymi, w szczególności w celu zapewnienia, by krajowe wykazy stron internetowych zawierających materiały z pornografią dziecięcą były jak najbardziej kompletne, a także by unikać powielania prac. Wszelkie inicjatywy w tym zakresie muszą uwzględnić prawa użytkowników końcowych, muszą być prowadzone z zastosowaniem obowiązujących procedur prawnych i sądowych oraz muszą być zgodne z Europejską Konwencją o ochronie praw człowieka i podstawowych wolności oraz z Kartą Praw Podstawowych Unii Europejskiej. W ramach programu na rzecz bezpieczniejszego Internetu ustanowiono sieć telefonów interwencyjnych, służących gromadzeniu informacji oraz zapewnieniu odpowiedniego zakresu i wymiany raportów dotyczących głównych rodzajów nielegalnych treści zamieszczanych online[6].

Unia Europejska proponuje szereg działań dla wszystkich państw członkowskich mających na celu zwiększenie bezpieczeństwa dzieci w Internecie. Są to działania w dziedzinie kształcenia i szkoleń, niezbędne do osłabienia i ograniczenia popytu sprzyjającego wszelkim formom wykorzystywania seksualnego dzieci. W odpowiednich przypadkach we współpracy z właściwymi organizacjami społeczeństwa obywatelskiego i innymi zainteresowanymi stronami – również za pośrednictwem Internetu – powinny być podjęte odpowiednie działania, takie jak kampanie informacyjne i uświadamiające, programy badawcze i edukacyjne służące podniesieniu świadomości i ograniczeniu ryzyka, że dzieci staną się ofiarami niegodziwego traktowania w celach seksualnych lub wykorzystywania seksualnego. Każde państwo członkowskie powinno poza tym propagować regularne szkolenie dla urzędników (np. policjantów) mogących mieć kontakt z dziećmi pokrzywdzonymi w wyniku niegodziwego traktowania w celach seksualnych lub wykorzystywania seksualnego. Państwa członkowskie muszą podejmować środki niezbędne do zapewnienia szybkiego usunięcia stron internetowych zawierających lub rozpowszechniających pornografię dziecięcą utrzymywanych na ich terytorium oraz dążyć do zapewnienia usunięcia takich stron utrzymywanych poza ich terytorium[7].

6) Dyrektywa Parlamentu Europejskiego i Rady 20011/92/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 z dnia 22 grudnia 2003 r. (Dz. U. L 335 z 17.12.2011), s. 6.
7) Tamże, s. 12-13.

# 4. Współpraca z partnerami międzynarodowymi na rzecz zwalczania niegodziwego traktowania dzieci w celach seksualnych oraz wykorzystywania seksualnego dzieci w Internecie

Internet to medium, które nie zna granic i jest wszechobecne, dlatego międzynarodowa współpraca w zakresie ochrony dzieci ma ogromne znaczenie. Istnieje potrzeba wprowadzenia globalnego podejścia stanowiącego odpowiedź na te zagadnienia, które byłoby lepiej skoordynowane i oparte na solidnych podstawach. Materiały prezentujące niegodziwe traktowanie dzieci w celach seksualnych mogą być oglądane i zgłaszane w jednym kraju, podczas gdy przechowywane są w drugim kraju, zaś umieszczane w Internecie w jeszcze innym kraju[8].

Jak podaje organizacja Internet Watch Foundation, w 2011 r. w ponad połowie materiałów prezentujących wykorzystywanie dzieci ustalono, że są one zlokalizowane poza Europą. W tym samym sprawozdaniu podano, że wraz z technologiami zmieniają się metody rozpowszechniania tych materiałów, jak i dostępu do nich.

W związku z tym konieczne jest, aby telefoniczne linie interwencyjne rozwijały swoje strategie oraz narzędzia i aby wspólnie mogły identyfikować przypadki umieszczania materiałów prezentujących wykorzystywanie dzieci w zmieniającym się środowisku *online* oraz zwalczać takowe przypadki. Wobec tego zgodnie z przyjętą *Europejską strategią na rzecz lepszego Internetu dla dzieci* zadaniem Komisji Europejskiej jest[9]:

1. Zachęcać sieć INHOPE, która skupia telefoniczne linie interwencyjne, aby zwiększała liczbę swoich członków na całym świecie, wśród których znajdują się obecnie takie państwa, jak Rosja, Japonia, Stany Zjednoczone, Republika Południowej Afryki, Australia lub Korea Południowa.

2. Wspierać wykonanie konwencji Rady Europy o cyberprzestępczości, oraz promowanie jej zasad poprzez gwarantowanie środków ochrony technicznej i prawnej.

3. Współpracować z partnerami międzynarodowymi za pośrednictwem struktur takich jak grupa robocza UE-Stany Zjednoczone ds. bezpieczeństwa cybernetycznego i cyberprzestępczości, która określi wspólne priorytety w tym obszarze, w tym współpracę na rzecz usuwania pornografii dziecięcej z Internetu oraz działanie na rzecz zwiększania praw dziecka w środowisku *online*.

4. Współorganizować konferencje UE-USA.

5. Próbować dotrzeć do innych regionów na świecie i wspierać współpracę na szczeblu światowym.

8) Por. M. Sitek, *Euro 2012 w cieniu turystyki seksualnej,* [w:] M. Zdanowicz, D. Lutyński (red.), *Przyjazna granica - rok do Euro 2012*, Kętrzyn 2011, s. 103-113.

9) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 02.05.2012 r. (Com(2012) 196 final)*; Europejska strategia na rzecz lepszego internetu dla dzieci*. Bruksela 2012r., str. 19.

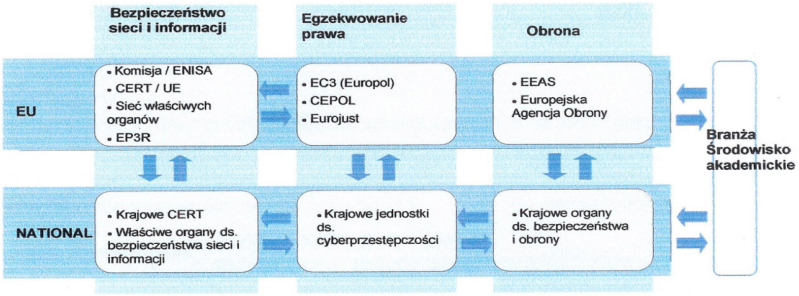
# 5. Współpraca międzynarodowa Unii Europejskiej na rzecz bezpieczeństwa cybernetycznego mająca wpływ na poziom bezpieczeństwa nieletnich w cyberprzestrzeni

Jednym z głównych wyzwań dla Unii Europejskiej w zakresie bezpieczeństwa w cyberprzestrzeni jest sprecyzowanie ról i obowiązków licznych zainteresowanych podmiotów, ponieważ w grę mogą wchodzić różne ramy prawne i różne jurysdykcje rządów krajowych. Dlatego też, ze względu na złożoność zagadnienia i różnorodność zainteresowanych podmiotów, scentralizowany nadzór europejski nie jest odpowiednim rozwiązaniem. Rządy krajowe mają najlepsze warunki do organizacji działań w zakresie zapobiegania incydentom i atakom cybernetycznym i reagowania na nie oraz w zakresie nawiązywania kontaktów i współtworzenia sieci z sektorem prywatnym i z ogółem społeczeństwa, w oparciu o prowadzone już działania polityczne i istniejące ramy prawne.

Jednocześnie, ze względu na potencjalny lub rzeczywisty transgraniczny charakter zagrożeń, skuteczna reakcja na poziomie krajowym często wymaga zaangażowania na poziomie Unii Europejskiej.

W celu rozwiązania problemu bezpieczeństwa cybernetycznego w kompleksowy sposób działania powinny obejmować trzy filary – bezpieczeństwo sieci i informacji, egzekwowanie przepisów i obronę – które również funkcjonują w oparciu o różne ramy prawne (poniższy rysunek).

**Rysunek 1.** Koordynacja między właściwymi organami ds. bezpieczeństwa sieci i informacji CERT, organami egzekwowania prawa i organami obrony




Zródło: Wspólny Komunikat Komisji Europejskiej, Wysokiego przedstawiciela UE do spraw zagranicznych i polityki bezpieczeństwa do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno - Społecznego i Komitetu Regionów z dnia 07.02.2013 r. - *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*. Bruksela 2013, s. 21.

## 5.1. Poziom krajowy

Państwa członkowskie na swoim poziomie krajowym powinny utworzyć struktury przeznaczone do działań w zakresie odporności cybernetycznej, cyberprzestępczości, oraz obrony; powinny też osiągnąć poziom zdolności wymagany do celów reagowania na incydenty cybernetyczne. Jednak z uwagi na fakt, że kilka podmiotów może mieć obowiązki operacyjne dotyczące różnych aspektów bezpieczeństwa cybernetycznego, a także biorąc pod uwagę znaczenie udziału sektora prywatnego, na poziomie krajowym należy zapewnić optymalną koordynację z udziałem różnych ministerstw. Państwa członkowskie powinny określić w swoich krajowych strategiach bezpieczeństwa cybernetycznego role i obowiązki poszczególnych podmiotów krajowych. Należy wspierać wymianę informacji między podmiotami krajowymi oraz między nimi a sektorem prywatnym, tak aby umożliwić państwom członkowskim i sektorowi prywatnemu posiadanie ogólnego obrazu różnych zagrożeń oraz lepsze zrozumienie nowych tendencji i technik wykorzystywanych zarówno do przeprowadzania cyberataków, jak i do szybszego reagowania na nie[10].

Dzięki ustanowieniu krajowych planów współpracy w zakresie bezpieczeństwa sieci i informacji, które miałyby być wykorzystywane w przypadku incydentów cybernetycznych, państwa członkowskie powinny być w stanie dokonać wyraźnego podziału ról i obowiązków oraz zapewnić optymalność podejmowanych działań[11].

## 5.2. Poziom unijny i międzynarodowy

Podobnie jak na poziomie krajowym, to również na poziomie Unii Europejskiej istnieje szereg podmiotów zajmujących się kwestiami bezpieczeństwa cybernetycznego. W szczególności trzy agencje – ENISA, Europol/EC3 i EAO – prowadzą działania w odpowiednich sobie obszarach: bezpieczeństwa sieci i informacji, egzekwowania prawa i obrony. Agencje te posiadają rady zarządzające, w których reprezentowane są państwa członkowskie i które stanowią platformy koordynacji na poziomie Unii Europejskiej.

ENISA, Europol/EC3 i EAO zachęcają do koordynacji i współpracy w dziedzinach, zwłaszcza w zakresie analiz tendencji, oceny zagrożeń, szkoleń i wymiany najlepszych praktyk. Agencje te wraz z CERT-UE,

10) Por. Wspólny Komunikat Komisji Europejskiej, Wysokiego przedstawiciela UE do spraw zagranicznych i polityki bezpieczeństwa do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno - Społecznego i Komitetu Regionów z dnia 07.02.2013r - *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*. Bruksela 2013, s. 21-22.

11) Por. Breński, A. Oleksiuk, *Przemiany gospodarczo-społeczne w Polsce w XX wieku,* wyd. Novea Res - Wydawnictwo Innowacyjne, Gdynia 2008.

Komisją i państwami członkowskimi wspierają rozwój obdarzonej zaufaniem grupy ekspertów technicznych i ekspertów ds. polityki w tej dziedzinie. Nieformalne kanały koordynacji i współpracy zostają uzupełniane przez bardziej ustrukturyzowane powiązania.

Do celów koordynacji w dziedzinie obronności wykorzystywany jest ponadto personel wojskowy Unii Europejskiej oraz działający w ramach EAO zespół projektowy ds. obrony cybernetycznej. W pracach Rady Programowej Europolu/EC3 uczestniczą między innymi Eurojust, CEPOL, państwa członkowskie, ENISA i Komisja, które mają możliwość dzielenia się wiedzą ekspercką i które gwarantują, że działania EC3 są prowadzone w ramach współpracy partnerskiej, przy uznaniu znaczenia dodatkowej wiedzy specjalistycznej oraz z poszanowaniem mandatów wszystkich zainteresowanych stron. Nowy mandat ENISA powinien umożliwić wzmocnienie jej powiązań z Europolem i z zainteresowanymi stronami z branży. Najważniejszy jest jednak fakt, że wniosek ustawodawczy Komisji w sprawie bezpieczeństwa sieci i informacji ustanawia ramy współpracy w oparciu o sieć właściwych organów krajowych ds. bezpieczeństwa sieci i informacji i uwzględnia kwestie wymiany informacji między organami ds. bezpieczeństwa sieci i informacji, i organami ścigania. Komisja Europejska wraz z państwami członkowskimi powinna zapewniać koordynację międzynarodowych działań w dziedzinie bezpieczeństwa cybernetycznego, przy jednoczesnym przestrzeganiu podstawowych wartości Unii Europejskiej i promowaniu pokojowego, otwartego i przejrzystego wykorzystania technologii cybernetycznych[12].

Obecnie Komisja Europejska i państwa członkowskie prowadzą rozmowy na temat kierunków polityki z międzynarodowymi partnerami i organizacjami, takimi jak Rada Europy, OECD, OBWE, NATO i ONZ.

## Zakończenie

Teoretyczna i praktyczna analiza aktualnych działań Unii Europejskiej, w obszarze zapewnienia optymalnej ochrony nieletnich w cyberprzestrzeni poprzez wspieranie bezpiecznego środowiska *online*, pozwoliła na postawienie następujących wniosków:

1. Unijne propozycje środków ochrony nieletnich w Internecie są podejmowane w sposób spójny i permanentny, a najnowsze propozycje zostały ujęte przede wszystkim:

a) 7 lutego 2013 r. w *„Europejskiej strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń”,*

b) 2 maja 2012 r. w *„Europejskiej strategii na rzecz lepszego Internetu dla dzieci*”,

c) 13 grudnia 2011 r. w Dyrektywie *„w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej”;*

12) Tamże, s. 22.

2. Innowacyjne rozwiązania technicznych zabezpieczeń infrastruktury informatycznej, stosowane we wszystkich państwach unijnych mogą być skuteczne jedynie przy odpowiedniej współpracy międzynarodowej z krajami poza UE oraz dzięki stworzeniu odpowiednich środków regulacji prawnych;

3. Ochrona przed niegodziwym traktowania dzieci w celach seksualnych i wykorzystywania seksualnego dzieci w Internecie oraz współpraca z partnerami międzynarodowymi na rzecz zwalczania niegodziwego traktowania dzieci w celach seksualnych i wykorzystywania seksualnego dzieci w Internecie - jest aktywnie podejmowana przez Unię Europejską, jak i państwa członkowskie. Jednak biorąc pod uwagę skalę zjawiska i wprowadzanie coraz to nowszych technologii teleinformatycznych, należy permanentnie prowadzić wszelkie możliwe działania na szczeblu międzynarodowym, unijnym i krajowym;

4. Współpraca międzynarodowa Unii Europejskiej na rzecz bezpieczeństwa cybernetycznego ma bardzo duży wpływ na poziom bezpieczeństwa nieletnich w cyberprzestrzeni.

## Bibliografia


Breński W., Oleksiuk A., *Przemiany gospodarczo-społeczne w Polsce w XX wieku*, wyd. Novea Res - Wydawnictwo Innowacyjne, Gdynia 2008.

Dyrektywa Parlamentu Europejskiego i Rady 20011/92/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 z dnia 22 grudnia 2003 r. ( Dz. U. L 335 z 17.12.2011).

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 02.05.2012 r. (Com(2012) 196 final)*; Europejska strategia na rzecz lepszego Internetu dla dzieci*. Bruksela 2012.

Stachecki D., *Postulaty w zakresie bezpiecznej szkolnej infrastruktury informatycznej. Opis zaleceń na przykładzie praktyk*i, [w:] Wojtasik Ł. (red.), *Jak reagować na cyberprzemoc. Poradnik dla szkół,* Fundacja Dzieci Niczyje, Warszawa 2009.

Sitek M., *Prawne i instytucjonalne ramy zwalczania handlu ludźmi,* [w:] Sitek B., Dammacco G. i in. (red.), *Wykorzystywanie człowieka w XX i XXI wieku*, UWM Wydział Prawa i Administracji, Olsztyn 2012.

Sitek M., Euro 2012 w cieniu turystyki seksualnej, [w:] Przyjazna granica - rok do Euro 2012, red. M. Zdanowicz i D. Lutyński, Kętrzyn 2011, s. 103-113.

Wspólny Komunikat Komisji Europejskiej, Wysokiego przedstawiciela UE do spraw zagranicznych i polityki bezpieczeństwa do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno - Społecznego i Komitetu Regionów z dnia 07.02.2013r - *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*. Bruksela 2013.