Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji do Rady i Parlamentu Europejskiego dotyczącego ustanowienia Europejskiego Centrum ds. Walki z Cyberprzestępczością

(Niniejsza opinia jest dostępna w pełnym brzmieniu w języku angielskim, francuskim i niemieckim na stronie internetowej EIOD: http://www.edps.europa.eu)

(2012/C 336/05)

1. Wprowadzenie

1.1. *Konsultacje z EIOD*

1. W dniu 28 marca 2012 r. Komisja przyjęła komunikat zatytułowany „Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością" ([1]).

2. EIOD zauważa, że Rada ogłosiła konkluzje w sprawie ustanowienia Europejskiego Centrum ds. Walki z Cyberprzestępczością w dniach 7–8 czerwca 2012 r. ([2]) Rada wyraża aprobatę dla celów wskazanych w komunikacie, popiera ustanowienie Centrum (zwanego również „EC3") w obrębie Europolu oraz wykorzystanie istniejących struktur do zwalczania przestępczości w innych obszarach, potwierdza, że powinno ono pełnić rolę punktu koordynującego działania w zakresie walki z cyberprzestępczością i ściśle współpracować ze stosownymi agencjami oraz podmiotami na szczeblu międzynarodowym, jak również wzywa Komisję do obszerniejszego określenia we współpracy z Europolem szczegółowego zakresu zadań, które należy wykonać, aby Centrum rozpoczęło funkcjonowanie do 2013 r. W konkluzjach nie odniesiono się jednak do znaczenia praw podstawowych, a w szczególności ochrony danych w związku z ustanowieniem Centrum.

3. Przed przyjęciem komunikatu Komisji EIOD miał możliwość przedstawienia nieformalnych uwag dotyczących jego projektu. W swoich nieformalnych uwagach EIOD podkreślił, że ochrona danych jest podstawowym aspektem, który należy uwzględnić przy ustanawianiu Europejskiego Centrum ds. Walki z Cyberprzestępczością (zwanego dalej „Centrum"). Komisja nie uwzględniła niestety nieformalnych uwag zgłaszanych na tym etapie. W konkluzjach Rady wnioskuje się ponadto o to, aby zapewnić uruchomienie Centrum już w przyszłym roku. Dlatego też na kolejnych etapach, które nastąpią już w bardzo krótkiej perspektywie czasowej, należy uwzględnić ochronę danych.

4. W niniejszej opinii zajęto się znaczeniem ochrony danych przy ustanawianiu Centrum i przedstawiono konkretne sugestie, które można wziąć pod uwagę podczas opracowywania zakresu jego zadań oraz zmiany ram prawnych Europolu. Działając z własnej inicjatywy, EIOD przyjął zatem niniejszą opinię w oparciu o art. 41 ust. 2 rozporządzenia (WE) nr 45/2001.

1.2. *Zakres komunikatu*

5. W swoim komunikacie Komisja przedstawia zamiar ustanowienia Europejskiego Centrum ds. Walki z Cyberprzestępczością jako priorytet w ramach strategii bezpieczeństwa wewnętrznego ([3]).

6. Komisja wymienia niektóre formy cyberprzestępczości, na których powinno koncentrować się Centrum: cyberprzestępstwa popełniane przez zorganizowane grupy przestępcze, w szczególności przestępstwa przynoszące duże zyski, takie jak oszustwa internetowe, cyberprzestępstwa wyrządzające poważne szkody ofiarom, takie jak przemoc seksualna wobec dzieci w Internecie, oraz cyberprzestępstwa mające poważny wpływ na krytyczne systemy w ramach technologii informacyjno-komunikacyjnych (ICT) na terenie Unii.

7. Jeżeli chodzi o prace Centrum, Komisja wymienia cztery podstawowe zadania ([4]):

— pełnienie funkcji europejskiego punktu kontaktowego w zakresie informacji dotyczących cyberprzestępczości,

— gromadzenie dostępnej w Europie wiedzy specjalistycznej na temat cyberprzestępczości potrzebnej do budowania potencjału państw członkowskich w zakresie walki z tym zjawiskiem,

([1]) W prawodawstwie UE nie istnieje definicja cyberprzestępczości.
([2]) Konkluzje Rady w sprawie ustanowienia Europejskiego Centrum ds. Walki z Cyberprzestępczością, 3172. posiedzenie Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w Luksemburgu w dniach 7—8 czerwca 2012 r.
([3]) Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy, COM(2010) 673 wersja ostateczna, dnia 22 listopada 2010 r. Zob. też opinię EIOD w sprawie tego komunikatu wydaną w dniu 17 grudnia 2010 r. (Dz.U. C 101 z 1.4.2011, s. 6).
([4]) Komunikat, s. 4–5.

— wspieranie krajowych dochodzeń dotyczących cyberprzestępstw,

— zapewnianie wspólnego głosu służbom ścigania i służbom sądowniczym zaangażowanym w europejskie dochodzenia w zakresie cyberprzestępczości.

8. Informacje przetwarzane przez Centrum będą gromadzone z „najróżniejszych źródeł – publicznych, prywatnych i ogólnie dostępnych" – stanowiących uzupełnienie danych policyjnych, i będą dotyczyć „działań cyberprzestępców, stosowanych przez nich metod, jak również osób podejrzanych o cyberprzestępczość". Centrum nawiąże też bezpośrednią współpracę z innymi agencjami i organami europejskimi. Przyjmie ona postać członkostwa tych podmiotów w jego radzie programowej, jak również w stosownych przypadkach współpracy operacyjnej.

9. Komisja wnioskuje o to, aby Centrum stało się naturalnym punktem styku działań Europolu w zakresie cyberprzestępczości oraz działań innych międzynarodowych jednostek policyjnych zajmujących się walką z tym zjawiskiem. Powinno ono również we współpracy z Interpolem i innymi partnerami strategicznymi na całym świecie dążyć do lepszej koordynacji działań dotyczących walki z cyberprzestępczością.

10. Jeżeli chodzi o aspekt praktyczny, Komisja wnioskuje o to, aby Centrum stanowiło część struktur Europolu. Wejdzie ono w skład Europolu ([1]), w związku z czym będzie funkcjonować w obrębie jego ram prawnych ([2]).

11. Według Komisji Europejskiej ([3]) najważniejszymi nowościami, jakie do obecnej działalności Europolu wniesie wnioskowane Centrum, będą: (i) zwiększenie zasobów w celu wydajniejszego gromadzenia informacji z różnych źródeł; (ii) wymiana informacji z partnerami spoza organów ścigania (głównie z sektora prywatnego).

1.3. *Zakres opinii*

12. W niniejszej opinii EIOD zamierza:

— poprosić Komisję o jasne określenie zakresu działalności Centrum w dziedzinach, w których ma ona znaczenie z punktu widzenia ochrony danych,

— ocenić przewidywaną działalność w kontekście obecnych ram prawnych Europolu, a zwłaszcza jej zgodność z tymi ramami,

— podkreślić stosowne aspekty, w odniesieniu do których prawodawcy powinni wprowadzić bardziej szczegółowe uregulowania w kontekście przyszłego przeglądu ram prawnych Europolu w celu zagwarantowania wyższego poziomu ochrony danych.

13. Struktura niniejszej opinii jest następująca: w części 2.1 wskazano, dlaczego ochrona danych jest w kontekście ustanowienia Centrum elementem fundamentalnym. W części 2.2 rozważono zgodność celów Centrum wskazanych w komunikacie z mandatem Europolu. W części 2.3 omówiono współpracę z sektorem prywatnym i partnerami z innych krajów.

3. **Wnioski**

50. EIOD uznaje walkę z cyberprzestępczością za fundamentalny element ochrony i bezpieczeństwa w przestrzeni cyfrowej oraz budowy niezbędnego zaufania. EIOD zauważa, że zgodność z zasadami ochrony danych należy uznawać za integralną część walki z cyberprzestępczością, a nie za przeszkodę zmniejszającą jej skuteczność.

51. W komunikacie mowa jest o ustanowieniu w ramach Europolu nowego Europejskiego Centrum ds. Walki z Cyberprzestępczością, podczas gdy od kilku lat istnieje już Centrum ds. Walki z Cyberprzestępczością Europolu. EIOD chętnie zapoznałby się z jaśniejszym opisem uprawnień i zakresu działalności nowego Centrum odróżniającym je od istniejącego Centrum ds. Walki z Cyberprzestępczością Europolu.

([1]) Zgodnie z zaleceniem zawartym w opublikowanym w lutym 2012 r. studium wykonalności obejmującym ocenę możliwych opcji (utrzymanie stanu obecnego, wykorzystanie struktur Europolu, Centrum jako własność/część Europolu, Centrum wirtualne), http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf

([2]) Decyzja Rady z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji (Europol) (2009/371/WSiSW).

([3]) Komunikat prasowy z dnia 28 marca 2012 r., „Frequently Asked Questions: the new European Cybercrime Centre", nr ref.: MEMO/12/221, data: 28.3.2012, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221

52. EIOD wskazuje, że kompetencje Centrum należy wyraźnie zdefiniować, nie odwołując się wyłącznie do pojęcia „przestępczości komputerowej" zawartego w obecnym prawodawstwie dotyczącym Europolu. W ramach przeglądu prawodawstwa dotyczącego Europolu należy również określić kompetencje Centrum oraz stosowane przez nie zabezpieczenia służące ochronie danych. EIOD zaleca, aby do chwili, gdy wejdzie w życie nowe prawodawstwo dotyczące Europolu, Komisja określiła te kompetencje i zabezpieczenia służące ochronie danych w zakresie uprawnień Centrum. W zakresie uprawnień można zawrzeć:

— jasne określenie zadań związanych z przetwarzaniem danych (w szczególności dochodzeń i działań w ramach wsparcia operacyjnego), w których pracownicy Centrum mogą uczestniczyć samodzielnie lub we współpracy ze wspólnymi zespołami dochodzeniowymi, oraz

— wyraźne procedury, które z jednej strony zapewniają poszanowanie praw jednostki (w tym prawo do ochrony danych), a z drugiej strony dają gwarancję, że dowody zostały uzyskane zgodnie z prawem i mogą zostać wykorzystane w sądzie.

53. Zdaniem EIOD wymiana danych osobowych Centrum z „najróżniejszymi podmiotami publicznymi, prywatnymi i ogólnie dostępnymi" niesie konkretne zagrożenia z punktu widzenia ochrony danych, gdyż często będzie wiązać się z przetwarzaniem danych gromadzonych do celów komercyjnych i przekazywaniem danych między krajami. Do zagrożeń tych odniesiono się w obecnej decyzji w sprawie Europolu, w której stwierdza się, że instytucja ta generalnie nie powinna wymieniać danych bezpośrednio z sektorem prywatnym, a z konkretnymi organizacjami międzynarodowymi tylko w ściśle określonych okolicznościach.

54. W tym kontekście i ze względu na znaczenie tych dwóch rodzajów działalności dla Centrum EIOD zaleca zapewnienie odpowiednich zabezpieczeń służących ochronie danych zgodnie z obowiązującymi przepisami decyzji w sprawie Europolu. Zabezpieczenia te należy zawrzeć w zakresie uprawnień, który ma zostać opracowany przez zespół wdrożeniowy ds. Centrum (później zaś w zmienionych ramach prawnych Europolu), i w żadnym przypadku nie powinny one skutkować niższym poziomem ochrony danych.

Sporządzono w Brukseli dnia 29 czerwca 2012 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych