

# EUROPEJSKI INSPEKTOR OCHRONY DANYCH

## **Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie rozpowszechniania i wykorzystywania technologii obserwacji niejawnej**

*(Pełny tekst niniejszej opinii jest dostępny w wersji angielskiej, francuskiej i niemieckiej na stronie internetowej EIOD [www.edps.europa.eu](http://www.edps.europa.eu))*

(2016/C 79/04)

W niniejszej opinii Europejski Inspektor Ochrony Danych porusza problemy ochrony danych i prywatności, jakie pojawiły się za sprawą rozpowszechniania i stosowania ingerujących w prywatność technologii nadzoru. Stosowanie takich narzędzi wiąże się nieodłącznie z przetwarzaniem danych osobowych i potencjalnym ingerowaniem w prywatność; głównym celem ingerujących w prywatność narzędzi nadzoru jest zdalne infiltrowanie systemów informatycznych (zazwyczaj przez internet) w celu niejawnego monitorowania działań takich systemów informatycznych oraz – z czasem – przesyłanie danych z powrotem do użytkownika narzędzi nadzoru.

Chociaż takie narzędzia mogą być wykorzystywane zgodnie z prawem (i w sposób regulowany) przez organy ścigania i agencje wywiadowcze, mogą one być również stosowane jako „konie trojańskie” służące obchodzeniu zabezpieczeń w komunikacji elektronicznej i przetwarzaniu danych.

Problem napięcia między pozytywnym wykorzystywaniem narzędzi ICT a negatywnym wpływem, jaki użytkowanie technologii w niewłaściwy sposób może mieć na prawa człowieka, w szczególności na ochronę danych osobowych i prywatności, musi zostać rozwiązany w ramach krajowych i unijnych strategii oraz przez wszystkie podmioty zaangażowane w sektor ICT (programiści, usługodawcy, sprzedawcy, pośrednicy, dystrybutorzy i użytkownicy).

W przedmiotowej opinii EIOD proponuje, aby na zagrożenie stworzone przez wykorzystywanie ingerujących w prywatność technologii nadzoru reagować w następujący sposób:

- należy przeprowadzić ocenę istniejących norm unijnych dotyczących ICT w celu zwiększenia ochrony praw człowieka, szczególnie w przypadku eksportu technologii przechwytywania lub nadzoru oraz powiązanych usług,
- wykorzystanie i rozpowszechnianie (w tym w obrębie UE) narzędzi nadzoru i przechwytywania oraz powiązanych usług powinno podlegać odpowiednim regulacjom z uwzględnieniem potencjalnego ryzyka naruszenia praw podstawowych, w szczególności prawa do prywatności i ochrony danych,
- Rada UE, Parlament Europejski, Komisja Europejska i ESDZ powinny opracować spójniejszą i sprawniejszą politykę w zakresie eksportu ingerujących w prywatność narzędzi nadzoru w kontekście technologii podwójnego zastosowania, zarówno na szczeblu UE, jak i krajowym,
- zaktualizowane strategie powinny regulować kwestię programów wykorzystujących luki „zero-day” oraz słabości w celu unikania wykorzystywania ich do naruszania praw podstawowych,
- polityka UE w zakresie bezpieczeństwa cybernetycznego powinna uwzględniać rozpowszechnianie technologii przechwytywania i nadzoru oraz reagować na ten właśnie problem odpowiednim prawodawstwem,
- należy promować inwestycje w bezpieczeństwo w internecie oraz inicjatywy służące uwzględnianiu prywatności w nowych rozwiązaniach technologicznych na etapie projektowania,
- należy wprowadzić spójne stanowisko w kwestii udzielania międzynarodowej ochrony osobom zgłaszającym naruszenia, które to osoby mogą przyczynić się do ujawnienia naruszenia praw człowieka za sprawą stosowania technologii przechwytywania i nadzoru.

Sporządzono w Brukseli dnia 15 grudnia 2015 r.

Giovanni BUTTARELLI

Europejski Inspektor Ochrony Danych