Grafika: Toscanabanana

ZALECENIA DLA UNII EUROPEJSKIEJ W SPRAWIE ZAPRZESTANIA STOSOWANIA BEZPRAWNEJ I UKIERUNKOWANEJ INWIGILACJI

AMNESTY INTERNATIONAL

Zalecenia dla Unii Europejskiej w sprawie zaprzestania stosowania bezprawnej i ukierunkowanej inwigilacji.

Amnesty International to globalny ruch zrzeszający ponad 10 milionów osób działających na rzecz świata, w którym wszyscy mogą korzystać z praw człowieka.

Chcemy zapewnić każdemu możliwość realizacji praw zapisanych w Powszechnej Deklaracji Praw Człowieka oraz innych dokumentach międzynarodowych poświęconych prawom człowieka.

Jesteśmy niezależni od władz państwowych, ideologii politycznych, interesów gospodarczych lub religii, a fundusze na swoją działalność pozyskujemy w większości ze składek członkowskich i dotacji osób indywidualnych.

AMNESTY INTERNATIONAL

Projekt Pegasus ujawnił, w jaki sposób oprogramowanie szpiegowskie firmy NSO było wykorzystywane do śledzenia aktywistów, dziennikarzy, prawników i polityków. Unaocznił on również druzgocący wpływ, jaki słabo uregulowana branża nadzoru ma na prawa i jakość życia bezprawnie szpiegowanych obywateli, bliskich im osób, a także na sam międzynarodowy system ochrony praw człowieka oraz bezpieczeństwo środowiska cyfrowego. Ustalenia Projektu Pegasus wskazują w szczególności, że doszło do rażącego naruszenia prawa do prywatności i prawa do swobody wypowiedzi. Należy również podkreślić, że niekontrolowane wykorzystanie technologii szpiegowskich negatywnie wpływa na działania na rzecz ochrony praw człowieka oraz przyczynia się do bardzo szybkiego nasilenia się cyfrowych zagrożeń dla obrońców praw człowieka, które przenoszą się ze świata wirtualnego do rzeczywistego.

Skłoniło to Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka, a także ekspertów ONZ do wezwania do podjęcia pilnych działań zmierzających do zwalczenia problemu bezprawnej i ukierunkowanej inwigilacji, w tym do wprowadzenia moratorium na sprzedaż i przekazywanie technologii inwigilacyjnych.

Ustalenia Projektu Pegasus zaprzeczają wszelkim twierdzeniom NSO Group, że takie ataki są rzadkie, stanowią anomalię lub wynikają z niewłaściwego wykorzystania technologii szpiegowskiej. Firma zapewnia, że jej oprogramowanie jest używane jedynie do śledztw w sprawach karnych, a także w sprawach o terroryzm. Jednak stało się jasne, że technologia NSO Group ułatwia systemowe nadużycia na dużą skalę, którym firma wydaje się być współwinna.

Amnesty International chciałaby zwrócić uwagę na raport zatytułowany „Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector" ["Odkrywanie góry lodowej: kryzys cyfrowej inwigilacji wywołany przez państwa oraz sektor prywatny"], jak również wspólne oświadczenie organizacji pozarządowych wzywające do wprowadzenia nowych zasad Unii Europejskiej w sprawie kontroli eksportu oraz zbadania roli państw członkowskich w działaniach objętych dochodzeniem Projektu Pegasus.

W niniejszym dokumencie Amnesty International przedstawia środki, które są kluczowe dla zagwarantowania większej kontroli nad firmami wytwarzającymi oprogramowanie szpiegowskie, odpowiedzialności za naruszenia praw człowieka, a także bardziej niezależnego nadzoru nad całą branżą. Biorąc pod uwagę znaczenie tych informacji, wzywamy Unię Europejską oraz państwa członkowskie do skorzystania z instrumentów polityki wewnętrznej i zagranicznej i zajęcia się tymi nadużyciami, tak by zagwarantować należytą kontrolę nad branżą systemu nadzoru komputerowego.

Obejmuje to następujące rekomendacje dla UE i państw członkowskich:

1. **Rekomendacje dla działań w ramach Unii Europejskiej.**

W niniejszym dokumencie informacyjnym Amnesty International przedstawia kluczowe środki, które są pilnie potrzebne do zapewnienia większej regulacji branży oprogramowania szpiegowskiego:

- Państwa członkowskie UE muszą niezwłocznie wprowadzić moratorium na sprzedaż, przekazywanie i wykorzystywanie technologii cyberinwigilacji. Biorąc pod uwagę zakres i skalę tych ustaleń, konieczne jest by państwa i firmy zaprzestały stosowania technologii inwigilacyjnych, dopóki nie zostaną wprowadzone odpowiednie i zgodne z prawami człowieka ramy regulacyjne.

- Państwa członkowskie UE muszą zapewnić efektywne odszkodowanie i/lub zadośćuczynienie dla ofiar bezprawnej inwigilacji i pociągnąć do odpowiedzialności sprawców naruszeń. Ponadto,

państwa członkowskie muszą zreformować swoje ustawodawstwo, tak by zlikwidować przeszkody uniemożliwiające uzyskanie odszkodowania (zadośćuczynienia) przez ofiary, a także by zagwarantować zarówno sądowe, jak i pozasądowe drogi dochodzenia roszczeń za naruszenia.

- Państwa członkowskie UE muszą wprowadzić i wykonywać przepisy, które zgodnie z wytycznymi ONZ gwarantują przestrzeganie przez firmy prywatne praw człowieka oraz nakładają na nie obowiązek wprowadzenia środków należytej staranności. Firmy te powinny również być zobowiązane do identyfikowania, zapobiegania oraz łagodzenia negatywnych skutków ich działań dla praw człowieka.

- Państwa członkowie UE mają obowiązek przyjąć i wdrożyć przepisy krajowe, które wprowadzą zabezpieczenia przed naruszeniami praw człowieka, a także nadużyciami wynikającymi z bezprawnej inwigilacji cyfrowej. Powinny one być zgodne z wyrokiem Europejskiego Trybunału Praw Człowieka z 2015 r. w sprawie Roman Zakharov przeciwko Rosji oraz międzynarodowymi zasadami dotyczącymi ochrony praw człowieka podczas inwigilacji. Państwa członkowskie UE powinny wprowadzić mechanizm odpowiedzialności, podstawę dla wytoczenia powództwa oraz inne instrumenty, które umożliwiłyby ofiarom nielegalnej inwigilacji dochodzenie roszczeń o odszkodowanie (zadośćuczynienie).

- Państwa członkowskie UE oraz Komisja Europejska powinny zagwarantować sprawne wdrożenie nowych przepisów dotyczących kontroli eksportu, które weszły w życie 9 września 2021 r. wraz z wersją przekształconą rozporządzenia o produktach podwójnego zastosowania[1]. Obejmuje to podjęcie natychmiastowych działań mających na celu podkreślenie wagi obowiązków z zakresu należytego działania w obszarze praw człowieka, które wynikają z rozporządzenia o produktach podwójnego zastosowania, a także stworzenie przejrzystych zasad działania rynku technologii cyberinwigilacji, które uwzględniałyby gwarancje z zakresu praw człowieka.
    - Nowe rozporządzenie stanowi, że Komisja ma obowiązek opublikować roczne publiczne sprawozdania dla Parlamentu i Rady. Powinno ono co najmniej zawierać liczbę wniosków o licencję w podziale na poszczególne produkty, nazwę eksportera, opis użytkownika końcowego, miejsce przeznaczenia, sposób zamierzonego wykorzystania, wyszczególnienie agencji rządowej zaangażowanej w zakup, wartość licencji, a także informację o przyznaniu lub odmowie przyznania licencji wraz z uzasadnieniem.
    - Ponadto, środki kontroli transakcji stosowane przez państwa członkowskie powinny obejmować ocenę strategicznej natury produktów oraz zagrożenia dla praw człowieka jakie mogą się z nimi wiązać. Organy państwowe powinny składać sprawozdania z realizacji swoich zobowiązań z zakresu starannego działania, a także nakłaniać przedsiębiorstwa by te informowały opinię publiczną o zakresie, charakterze i wynikach wdrożonych przez siebie procedur starannego działania z obszaru praw człowieka.
    - Państwa członkowskie powinny zapewnić, aby państwa wywozu wprowadziły odpowiednie mechanizmy zapewniające skuteczne odszkodowanie (zadośćuczynienie) za naruszenia praw człowieka, do których doszło przy wykorzystaniu przekazanej technologii. Wytyczne które zostaną opublikowane w myśl art. 26 ust. 1 rozporządzenia o produktach podwójnego

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/821 z dnia 20 maja 2021 r. ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania (wersja przekształcona).

zastosowania musi szczegółowo określić wymogi dotyczące programów badania zgodności oraz programów starannego działania, czego wymaga się od eksporterów, w myśl rozporządzenia o produktach podwójnego zastosowania oraz zgodnie z wytycznymi ONZ dotyczącymi biznesu i praw człowieka (wytyczne ONZ) oraz wytycznymi OECD dla przedsiębiorstw wielonarodowych.

- Rada i państwa członkowskie UE powinny odnieść się do obaw dotyczących stosowania przez Polskę oraz Węgry[2] niezgodnych z prawem technologii nadzoru w toczącym się postępowaniu dotyczącym naruszenia art. 7 Traktatu o Unii Europejskiej (TUE). Powinny one wezwać Polskę i Węgrydo podjęcia działań naprawczych w celu usunięcia naruszeń praw podstawowych oraz praworządności.
- Biorąc pod uwagę bezprawną, ukierunkowaną inwigilację stosowaną przez Polskę i Węgry Komisja Europejska powinna zbadać nadużywanie technologii nadzoru cyfrowego przez władze tego państwa, jak również to, czy inne państwa członkowskie UE dopuszczały się podobnych nadużyć. W ramach tego dochodzenia należy ocenić, czy Polska, Węgry lub jakiekolwiek inne państwo członkowskie przestrzegały swoich zobowiązań wynikających z traktatów UE, Karty praw podstawowych UE, ogólnego rozporządzenia o ochronie danych[3], dyrektywy o ochronie danych w sprawach karnych[4] oraz dyrektywy o prywatności i łączności elektronicznej[5]. Jeżeli okaże się, że Polska lub Węgry naruszyły zobowiązania wynikające z tych dokumentów, Komisja Europejska powinna wszcząć postępowanie w sprawie uchylenia zobowiązaniom państwa członkowskiego.
- Komisja Europejska powinna niezwłocznie przeprowadzić dochodzenie mające na celu zbadanie pozwoleń wszystkich państw członkowskich na wywóz, włączając w to ogólne unijne zezwolenie na wywóz EU005, obejmujące oprogramowanie przeznaczone dla urządzeń monitorujących oraz przechwytujących komunikację. Powinna również zapewnić, że państwa członkowskie UE cofną wszelkie pozwolenia na wywóz oraz sprzedaż w sytuacji, gdy istnieje poważne zagrożenie, że dana technologia mogłaby przyczynić się do naruszenia praw człowieka. NSO Group działa na obszarze Luksemburga i zgodnie z jej sprawozdaniem za rok 2021 dotyczącym przejrzystości i odpowiedzialności, eksportuje swoje produkty z Belgii i Cypru. Jeśli okaże się, że pozwolenia na wywóz państw członkowskich naruszają przepisy prawa, Komisja Europejska powinna wszcząć postępowanie w sprawie uchybienia zobowiązaniom państwa członkowskiego.

- Parlament Europejski powinien podjąć działania międzykomisyjne i ponadpartyjne, aby właściwie przenalizować wewnętrzne i zewnętrzne aspekty tej sprawy i zażądać odpowiedniej reakcji na poziomie europejskim. Parlament Europejski oraz jego posłowie powinni wezwać Komisję Europejską, Radę i państwa członkowskie do wykorzystania zarówno instrumentów polityki

[2] Rekomendacje dotyczyły początkowo jedynie Węgier ale zostały uzupełnione po ujawnieniu informacji o możliwych nadużyciach związanych ze stosowaniem oprogramowania Pegasus przez Polskę.
[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.
[5] 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.

wewnętrznej, jak i zagranicznej w celu podjęcia odpowiednich działań w odpowiedzi na te naruszenia, a uregulowania w sposób efektywny branży nadzoru. Działania te powinny obejmować wdrożenie wszystkich zaleceń wynikających z niniejszego dokumentu.

2. Zalecenia dla działań Unii Europejskiej i jej państw członkowskich z zakresu instrumentów polityki zagranicznej:

- UE i jej państwa członkowskie muszą jasno wyrazić swoje stanowisko w odniesieniu do ustaleń Projektu Pegasus, w tym poprzez wydanie oficjalnego oświadczenia. Wymiar naruszeń ujawnionych w ramach projektu Pegasus był ogromny, a pełna ich skala prawdopodobnie wykracza daleko poza przypadki ujawnione do tej pory. Biorąc pod uwagę cel Unii Europejskiej, by stać się światowym wyznacznikiem standardów, musi ona odegrać czynną rolę w zapewnianiu ochrony praw człowieka i przestrzegania praworządności w sferze cyfrowej zarówno w kraju jak i za granicą. Ma to swoją podstawę w zobowiązaniach UE i państw członkowskich w zakresie ochrony i promowania praw człowieka na całym świecie, co wynika z art. 21 Traktatu Lizbońskiego. Ponadto jest to zgodne ze zobowiązaniami UE zawartymi w konkluzjach Rady w sprawie kształtowania cyfrowej przyszłości Europy, planie działania UE dotyczącym praw człowieka i demokracji, a także innych wytycznych UE z zakresu praw człowieka. Przywódcy UE, w tym przewodnicząca Komisji Von Der Leyen i wysoki przedstawiciel Borrell, wielokrotnie podkreślali już znaczenie ochrony społeczeństwa obywatelskiego oraz przestrzegania prawa do prywatności i wolności słowa w Internecie w epoce cyfrowej. UE i jej państwa członkowskie powinny wydać dalsze oświadczenia, w których:
    - wyrażą zaniepokojenia informacjami ujawnionymi przez media dotyczącymi faktu, że oprogramowanie szpiegowskie opracowane przez NSO było wykorzystywane do inwigilowania dziennikarzy, aktywistów i głów państw na szeroką skalę oraz podkreślą, że takie działania są niedopuszczalne i naruszają prawo do wolności słowa, pokojowych zgromadzeń i prywatności,
    - podkreślą, że te ustalenia wyraźnie wskazują na pilną potrzebę wprowadzenia większej przejrzystości i odpowiedzialności prawnej w branży nadzoru,
    - podkreślą, że ujawnione informacje jasno pokazują, że ataki cyfrowe się nasilają oraz coraz bardziej powszechna jest praktyka stosowania przez rządy na całym świecie ukierunkowanej inwigilacja w odniesieniu do obrońców praw człowieka, dziennikarzy i społeczeństwa obywatelskiego, co ma na celu uciszenie i zastraszenie tych podmiotów,
    - wezwą inne państwa do podjęcia pilnych działań w celu szerszego uregulowania branży cybernetycznego nadzoru, a także zapewnienia większego nadzoru nad nią oraz większej odpowiedzialności za naruszenia praw człowieka wynikające z inwigilacji.

- Państwa członkowskie UE powinny nawiązać dwustronne kontakty i wydać oświadczenie skierowane do właściwych organów w państwach trzecich, których projekt Pegasus wskazał jako potencjalnych klientów NSO Group. W ramach projektu Pegasus zidentyfikowano osoby, które zostały wytypowane do potencjalnego namierzenia przez następujące państwa: Azerbejdżan, Bahrajn, Polska, Węgry, Indie, Kazachstan, Meksyk, Maroko, Rwanda, Arabia Saudyjska, Togo i Zjednoczone Emiraty Arabskie. UE i państwa członkowskie powinny zwrócić się do władz tych państw o wyjaśnienia, a także:

- wezwać do przeprowadzenia natychmiastowego, niezależnego, przejrzystego i bezstronnego dochodzenia w sprawie wszelkich przypadków bezprawnej inwigilacji ujawnionych w ramach projektu Pegasus oraz w stosownych przypadkach do wykorzystania środków prawnych w celu zapewnienia ofiarom odpowiedniego zadośćuczynienia i pociągnięcia do odpowiedzialności sprawców, zgodnie z międzynarodowymi standardami praw człowieka.
- podkreślić, że stosowanie oprogramowania szpiegowskiego jest zgodne z prawem tylko wtedy, gdy spełniono ściśle określone warunki, opisane w międzynarodowym prawie ochrony praw człowieka, oraz że każdy przypadek inwigilacji musi być zgodny z prawem, konieczny, proporcjonalny i ograniczony w czasie,
- wezwać te państwa do przestrzegania swoich zobowiązań wynikających z międzynarodowego prawa ochrony praw człowieka, w tym tych określonych w Międzynarodowym pakcie praw obywatelskich i politycznych oraz deklaracji ONZ o obrońcach praw człowieka,
- przedstawić organom najwyższego szczebla przypadki inwigilacji obrońców praw człowieka, dziennikarzy i aktywistów, a także zaoferować tym osobom wsparcie polityczne, techniczne oraz inne zgodne z wytycznymi UE w sprawie obrońców praw człowieka, wytycznymi UE w zakresie wolności słowa oraz planem działania UE dotyczącym praw człowieka i demokracji.

- Państwa członkowskie UE muszą wezwać Izrael i wszystkie inne państwa wywozu technologii służącej cyberinwigilacji do natychmiastowego cofnięcia wszystkich zezwoleń wydanych NSO Group i przeprowadzenia niezależnego, bezstronnego, przejrzystego dochodzenia w celu określenia zakresu bezprawnej inwigilacji cyfrowej. Powinno to obejmować pełną analizę oraz późniejszą reformę systemu eksportu licencji w celu zapewnienia, że jest on zgodny z prawem i obowiązującą praktyką, a także zapobiega przyszłym naruszeniom praw człowieka związanym z eksportem sprzętu do inwigilacji cybernetycznej. Powinno to zakończyć się opublikowaniem wyników dochodzenia, a także podjęciem niezbędnych kroków zmierzających do zapobieżenia przyszłym nadużyciom. Państwa te powinny również podjąć środki w celu zapewnienia, że NSO Group:
  - w sposób natychmiastowy zaprzestanie wykorzystywania, wspierania i sprzedaży Pegasusa do czasu wejścia w życie efektywnych uregulowań prawnych z zakresu ochrony praw człowieka, które określałyby szczegółowe warunki sprzedaży, przekazywanie i wykorzystywanie technologii nadzoru,
  - zapewni odpowiednie odszkodowanie (zadośćuczynienie) lub inne formy skutecznej rekompensaty dla ofiar bezprawnej inwigilacji, do której doszło z wykorzystaniem produktów NSO Group,
  - podejmie kroki w celu zapewnienia, że nie spowoduje ani nie przyczyni się w przyszłości do dalszych naruszeń praw człowieka, oraz że zareaguje na nie w odpowiedni sposób, jeżeli by do nich doszło. Obejmuje to również wszelkie sprawy objęte bieżącym dochodzeniem. W celu wypełnienia tego zobowiązania, NSO Group musi przeprowadzić odpowiednią analizę starannego działania w zakresie praw człowieka i podjąć odpowiednie kroki w celu zapewnienia, że obrońcy praw człowieka, dziennikarze i społeczeństwo obywatelskie nie padną już ofiarą bezprawnej inwigilacji.

- Państwa członkowskie UE powinny wziąć udział w kluczowych wielostronnych działaniach, w tym w posiedzeniach Rady Praw Człowieka ONZ, Zgromadzenia Ogólnego ONZ oraz w powszechnym okresowym przeglądzie praw człowieka w celu opracowania efektywnych standardów ochrony praw człowieka regulujących rozwój, sprzedaż, przekazywanie i wykorzystywanie technologii nadzoru, a także określających niedopuszczalne cele inwigilacji. Zawiera się w tym również apel o natychmiastowe moratorium na sprzedaż, przekazywanie i wykorzystywanie technologii nadzoru.

AMNESTY INTERNATIONAL TO GLOBALNY RUCH NA RZECZ PRAW CZŁOWIEKA. JEŚLI NIESPRAWIEDLIWOŚĆ SPOTYKA JEDNĄ OSOBĘ, DOTYKA NAS WSZYSTKICH.

AMNESTY INTERNATIONAL

Zalecenia dla Unii Europejskiej w sprawie zaprzestania stosowania bezprawnej i ukierunkowanej inwigilacji.