2024/2659

16.10.2024

ZALECENIE KOMISJI (UE) 2024/2659

z dnia 11 października 2024 r.

w sprawie wytycznych dotyczących wywozu produktów służących do cyberinwigilacji na podstawie art. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/821

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 292,

a także mając na uwadze, co następuje:

(1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/821 ([1]) ustanawia unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania.

(2) W rozporządzenie (UE) 2021/821 odniesiono się do ryzyka wykorzystania produktów służących do cyberinwigilacji do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego.

(3) Zgodnie z art. 5 ust. 2 i art. 26 ust. 1 rozporządzenia (UE) 2021/821 Komisja i Rada udostępniają eksporterom wytyczne dotyczące produktów służących do cyberinwigilacji niewymienionych w wykazie, mając na uwadze potrzebę zapewnienia skuteczności unijnego systemu kontroli wywozu pod względem cyberbezpieczeństwa oraz potrzebę zapewnienia spójności wdrażania rozporządzenia (UE) 2021/821.

(4) Niniejsze zalecenie i załączone do niego wytyczne mają stanowić pomoc dla eksporterów w stosowaniu środków kontroli produktów służących do cyberinwigilacji niewymienionych w wykazie, m.in. środków należytej staranności umożliwiających ocenę ryzyka związanego z wywozem takich produktów.

(5) Wytyczne załączone do niniejszego zalecenia były przedmiotem szczegółowych konsultacji przeprowadzonych przez grupę ekspertów ds. technologii inwigilacji w 2022 i 2023 r. i uwzględniają uwagi otrzymane w trakcie konsultacji publicznych ([2]) przeprowadzonych w drugim kwartale 2023 r.

(6) Należy przypomnieć, że niniejsze zalecenie oraz załączone do niego wytyczne nie są wiążące. Eksporterzy powinni zatem zachować odpowiedzialność za wypełnianie swoich obowiązków wynikających z rozporządzenia (UE) 2021/821, a Komisja powinna zapewnić, aby z upływem czasu niniejsze zalecenie pozostawało aktualne i przydatne,

([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 (Dz.U. L 206 z 11.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

([2]) https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en.

PRZYJMUJE NINIEJSZE ZALECENIE:

Zaleca się, aby właściwe organy państw członkowskich i eksporterzy uwzględniali niewiążące wytyczne zawarte w załączniku do niniejszego zalecenia w celu wypełnienia swoich obowiązków wynikających z art. 5 ust. 2 rozporządzenia (UE) 2021/821.

Sporządzono w Brukseli dnia 11 października 2024 r.

W imieniu Komisji
Valdis DOMBROVSKIS
Wiceprzewodniczący wykonawczy

ZAŁĄCZNIK

SPIS TREŚCI

Strona

WPROWADZENIE

Unijne ramy kontroli wywozu ustanowione rozporządzeniem (UE) 2021/821 („rozporządzenie") mają na celu zapewnienie przestrzegania międzynarodowych obowiązków i zobowiązań Unii i jej państw członkowskich, w tym dotyczących pokoju, bezpieczeństwa i stabilności w regionie oraz poszanowania praw człowieka i międzynarodowego prawa humanitarnego. W związku z tym Unia i jej państwa członkowskie wdrożyły decyzje podjęte w ramach wielostronnych reżimów kontroli eksportu i odpowiednio zaktualizowały unijny wykaz kontrolny w załączniku I do rozporządzenia ([1]). Ponadto, zanim art. 5 rozporządzenia zaczął obowiązywać, właściwe organy państw członkowskich kontrolowały już wywóz niektórych wymienionych w wykazie produktów, które mogą służyć do prowadzenia nadzoru ([2]), biorąc pod uwagę ryzyko niewłaściwego wykorzystania tych produktów w pewnych szczególnych okolicznościach. W wyjątkowo poważnych okolicznościach Unia nałożyła sankcje ograniczające wywóz niektórych urządzeń dozorowania ([3]).

Rozporządzenie odzwierciedla zobowiązanie Unii do skutecznego przeciwdziałania ryzyku wykorzystania produktów służących do cyberinwigilacji do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego. W rozporządzeniu wprowadzono w szczególności nowe przepisy dotyczące kontroli wywozu niewymienionych w wykazie produktów służących do cyberinwigilacji, w tym zobowiązanie eksporterów do powiadamiania właściwego organu, jeżeli zgodnie ze swoimi ustaleniami dokonanymi w ramach procedury należytej staranności są świadomi, że niewymienione w wykazie produkty służące do cyberinwigilacji, które eksporterzy zamierzają wywieźć, są przeznaczone, w całości lub w części, do wykorzystywania do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego. W rozporządzeniu wzywa się ponadto Komisję i Radę do udostępnienia wytycznych dla eksporterów w celu wsparcia skutecznego wdrażania nowych kontroli niewymienionych w wykazie produktów służących do cyberinwigilacji.

Wytyczne te mają zatem na celu wspieranie eksporterów w przeprowadzaniu kontroli niewymienionych w wykazie produktów służących do cyberinwigilacji, w tym m.in. stosowaniu środków należytej staranności służących do oceny ryzyka związanego z wywozem takich produktów z przeznaczeniem dla użytkowników końcowych i do zastosowań końcowych zgodnie z nowymi przepisami rozporządzenia.

1. ODPOWIEDNIE PRZEPISY PRAWNE, DEFINICJE I KLUCZOWE POJĘCIA

1.1. Przegląd odpowiednich przepisów prawnych

W rozporządzeniu wprowadzono nowe przepisy przewidujące w sposób wyraźny kontrole wywozu produktów służących do cyberinwigilacji niewymienionych w załączniku I do rozporządzenia, które to produkty są lub mogą być przeznaczone, w całości lub w części, do wykorzystywania do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego. Odpowiednie motywy i artykuły obejmują:

a) motyw 8: „Aby wyeliminować ryzyko, że niektóre niewymienione w wykazie produkty służące do cyberinwigilacji wywożone z obszaru celnego Unii będą niewłaściwie wykorzystywane przez osoby, które dopuszczają się poważnych naruszeń praw człowieka lub międzynarodowego prawa humanitarnego bądź są odpowiedzialne za zlecanie lub popełnianie tych naruszeń, należy kontrolować wywóz takich produktów. Związane z tymi produktami ryzyko dotyczy w szczególności przypadków, w których produkty służące do cyberinwigilacji są specjalnie zaprojektowane po to, by umożliwić włamania lub głęboką inspekcję pakietów w systemach informatycznych i telekomunikacyjnych

([1]) Zob. w szczególności kontrole związane z systemami przechwytywania przekazów telekomunikacyjnych (5A001.f), systemami nadzoru internetu (5A001.j.), złośliwym oprogramowaniem (4A005, 4D004 i powiązane kontrole w ramach pozycji 4E001.a i 4E001.c) oraz oprogramowaniem monitorującym stosowanym przez organy egzekwowania prawa (5D001.e). Ponadto zob. kontrole dotyczące niektórych narzędzi kryminalistycznych/dochodzeniowych (5A004.b 5D002.a.3.b i 5D002.c.3.b), oparte na indywidualnej ocenie każdego przypadku.

([2]) W szczególności systemy związane z ochroną informacji.

([3]) Zob. rozporządzenie Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczące środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz.U. L 134 z 20.5.2006, s. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); rozporządzenie Rady (UE) nr 359/2011 z dnia 12 kwietnia 2011 r. dotyczące środków ograniczających skierowanych przeciwko niektórym osobom, podmiotom i organom w związku z sytuacją w Iranie (Dz.U. L 100 z 14.4.2011, s. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); rozporządzenie Rady (UE) nr 36/2012 z dnia 18 stycznia 2012 r. w sprawie środków ograniczających w związku z sytuacją w Syrii oraz uchylające rozporządzenie (UE) nr 442/2011 (Dz.U. L 16 z 19.1.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); rozporządzenie Rady (UE) nr 401/2013 z dnia 2 maja 2013 r. dotyczące środków ograniczających w związku z sytuacją w Mjanmie/Birmie i uchylające rozporządzenie (WE) nr 194/2008 (Dz.U. L 121 z 3.5.2013, s. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj); rozporządzenie Rady (UE) 2017/2063 z dnia 13 listopada 2017 r. w sprawie środków ograniczających w związku z sytuacją w Wenezueli (Dz.U. L 295 z 14.11.2017, s. 21, ELI: https://eur-lex.europa.eu/eli/reg/2017/2063/oj).

w celu prowadzenia niejawnego nadzoru osób fizycznych poprzez monitorowanie, pobieranie, gromadzenie lub analizowanie danych, w tym danych biometrycznych, z tych systemów. Uznaje się, że produkty stosowane wyłącznie do celów komercyjnych, takich jak naliczanie opłat, marketing, wysokiej jakości usługi, badanie satysfakcji użytkowników lub bezpieczeństwo sieci, nie wiążą się co do zasady z takim ryzykiem";

b) motyw 9: „W celu wzmocnienia skutecznej kontroli wywozu niewymienionych w wykazie produktów służących do cyberinwigilacji konieczne jest dalsze ujednolicenie stosowania kontroli typu *catch-all* w tym obszarze. W tym celu państwa członkowskie zobowiązały się do wspierania takich kontroli poprzez wymianę informacji między sobą i z Komisją, w szczególności w odniesieniu do postępu technologicznego produktów służących do cyberinwigilacji, oraz poprzez zachowanie czujności przy stosowaniu takich kontroli, aby wspierać wymianę informacji na szczeblu unijnym";

c) art. 2 pkt 20, w którym produkty służące do cyberinwigilacji zdefiniowano jako „produkty podwójnego zastosowania specjalnie zaprojektowane po to, by umożliwić niejawny nadzór osób fizycznych poprzez monitorowanie, pobieranie, gromadzenie lub analizowanie danych z systemów informatycznych i telekomunikacyjnych";

d) w art. 5 wprowadzono wymóg uzyskania zezwolenia w przypadku wywozu niewymienionych w wykazie produktów służących do cyberinwigilacji, jeżeli eksporter zostanie poinformowany przez właściwy organ, że wskazane produkty są lub mogą być przeznaczone, w całości lub w części, do wykorzystywania do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego (art. 5 ust. 1). Ponadto w artykule tym wymaga się, aby eksporterzy powiadamiali właściwy organ, jeżeli są świadomi, zgodnie ze swoimi ustaleniami dokonanymi w ramach procedury należytej staranności, że produkty te są przeznaczone, w całości lub w części, do wykorzystywania do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego (art. 5 ust. 2). Ten właściwy organ podejmuje decyzję o ewentualnym poddaniu danego wywozu wymogowi uzyskania zezwolenia;

e) art. 5 ust. 2 stanowi ponadto, że „Komisja i Rada udostępniają eksporterom wytyczne, o których mowa w art. 26 ust. 1".

1.2. **Kluczowe definicje**

Rozporządzenie zawiera specjalne motywy i przepisy, w których sprecyzowano konkretne terminy istotne dla kontroli wywozu niewymienionych w wykazie produktów służących do cyberinwigilacji, które to terminy eksporterzy powinni dobrze rozumieć, aby móc przeprowadzać procedury należytej staranności i wdrażać skuteczną kontrolę. Szczególne znaczenie ma art. 2 pkt 20, który zawiera następującą dokładną definicję „produktów służących do cyberinwigilacji": „produkty podwójnego zastosowania specjalnie zaprojektowane po to, by umożliwić niejawny nadzór osób fizycznych poprzez monitorowanie, pobieranie, gromadzenie lub analizowanie danych z systemów informatycznych i telekomunikacyjnych".

Do celów niniejszych wytycznych należy wyjaśnić konkretne aspekty tej definicji.

1.2.1. *„Specjalnie zaprojektowany"*

Produkt jest przeznaczony do prowadzenia niejawnego nadzoru, gdy jego cechy techniczne są odpowiednie do celów niejawnego nadzoru nad osobami fizycznymi i obiektywnie umożliwiają taki nadzór. W związku z tym termin „specjalnie zaprojektowany" oznacza, że niejawny nadzór nad osobami fizycznymi musi być głównym celem opracowania i zaprojektowania danego produktu. W przypadku tego terminu nie wymaga się jednak, aby produkt mógł być wykorzystywany wyłącznie do prowadzenia niejawnego nadzoru nad osobami fizycznymi.

Jak wyjaśniono w motywie 8 rozporządzenia, produkty stosowane wyłącznie do celów komercyjnych, takich jak naliczanie opłat, marketing, wysokiej jakości usługi, badanie satysfakcji użytkowników lub bezpieczeństwo sieci, nie są specjalnie zaprojektowane do celów niejawnego nadzoru osób fizycznych i w związku z tym nie wchodzą w zakres definicji produktów służących do cyberinwigilacji. Na przykład, nawet jeśli produkty przeznaczone do nadzoru systemów operacyjnych w przemyśle lub monitorowania ruchu użytkowników mogłyby zostać wykorzystane do celów nadzoru, zgodnie z przywołaną definicją produkty te nie są produktami służącymi do cyberinwigilacji, ponieważ nie są specjalnie zaprojektowane po to, by umożliwić niejawny nadzór nad osobami fizycznymi.

1.2.2. *„Niejawny nadzór”*

Produkty umożliwiają prowadzenie niejawnego nadzoru w szczególności w przypadku, gdy nadzór nie jest w sposób oczywisty dostrzegalny dla osoby fizycznej objętej takim nadzorem. Ma to miejsce w przypadku, gdy osoby objęte niejawnym nadzorem nie są świadome obecności ani działania produktów służących do cyberinwigilacji i w związku z tym nie mają możliwości uwolnienia się od tego nadzoru lub przynajmniej odpowiedniego dostosowania swojego zachowania. Nawet jeżeli nadzór prowadzony jest za pomocą produktów zainstalowanych lub działających w przestrzeni publicznej, pozyskanie danych można w niektórych przypadkach uznać za wchodzące w zakres definicji niejawnego nadzoru, w szczególności jeśli zgromadzone dane mogą być przekierowywane, oceniane lub przetwarzane do celów innych niż te, o których poinformowano daną osobę fizyczną. Innymi słowy, jeżeli osoba fizyczna nie może obiektywnie przypuszczać, że jest objęta nadzorem, nadzór można uznać za niejawny zgodnie z art. 2 pkt 20 rozporządzenia.

1.2.3. *„Osoby fizyczne”*

Termin „osoba fizyczna” odnosi się do żywego człowieka w przeciwieństwie do osoby prawnej lub podmiotu prawnego, które w związku z tym nie podlegają przepisom. Termin ten nie odnosi się do nadzoru nad przedmiotami, obiektami ani maszynami jako takimi.

1.2.4. *„Monitorowanie, pobieranie, gromadzenie, analizowanie danych”*

Według *Oxford English Dictionary* słowa „monitorowanie, pobieranie, gromadzenie i analizowanie” mają następujące znaczenie językowe:

— „monitorowanie”: nadzór; inwigilacja, nasłuch;

— „pobieranie”: wydobywanie;

— „gromadzenie”: zbieranie, kompilowanie;

— „analizowanie”: wyodrębnienie lub ustalenie elementów czegoś (złożonego) w celu określenia jego struktury lub charakteru, a tym samym jego wyjaśnienia lub zrozumienia; dokładne i metodyczne badanie do celów interpretacji; poddanie analizie krytycznej lub obliczeniowej.

Terminy te oznaczają, że produkty wykorzystywane do nadzoru powinny mieć precyzyjne techniczne możliwości przetwarzania danych w celu ich monitorowania, gromadzenia, pobierania lub analizowania, czego przykładem są następujące produkty:

a) produkty wykorzystywane do monitorowania danych z systemów informatycznych i telekomunikacyjnych ([4]) (np. wielkości plików lub przepływu pakietów danych przesyłanych w takim systemie);

b) produkty, które pobierają dane z systemów informatycznych i telekomunikacyjnych poprzez włamanie, a następnie pobranie danych (np. złośliwe oprogramowanie);

c) produkty umożliwiające analizę danych pobranych z systemów informatycznych i telekomunikacyjnych, w tym produkty, które mogą przetwarzać przechowywane w tych systemach obrazy z kamer (np. niektóre rodzaje technologii analizy danych wykorzystywane jako część systemów rozpoznawania twarzy).

Produkty wykorzystywane do zwykłego monitorowania systemów informatycznych lub obserwowania ludzi za pomocą kamer do monitoringu wizyjnego, które umożliwiają zarejestrowanie rozmów, wymian danych, przemieszczania się i indywidualnych zachowań, nie byłyby produktami służącymi do cyberinwigilacji w rozumieniu rozporządzenia, ponieważ nie są specjalnie zaprojektowane do tego celu i muszą współpracować z innymi technologiami, takimi jak sztuczna inteligencja lub duże zbiory danych. Cały system (współpracujący z innymi technologiami, takimi jak sztuczna inteligencja lub technologie dużych zbiorów danych) mógłby jednak potencjalnie stanowić produkt służący do cyberinwigilacji zgodnie z definicją zawartą w art. 2 pkt 20 rozporządzenia.

Co istotne, mimo iż wskazano kilka przykładów przydatnych do celów ilustracyjnych, przykłady te nie ograniczają definicji ani zakresu produktów służących do cyberinwigilacji, ponieważ celem art. 5 jest umożliwienie skutecznej kontroli wywozu produktów niewymienionych w wykazie.

([4]) Definicja znajduje się w pkt 1.2.5 poniżej.

Jak wynika z użycia spójnika „lub” w definicji, wymienione zdolności techniczne należy uznać za alternatywne i nie jest konieczne, aby dany produkt posiadał wszystkie te zdolności techniczne do monitorowania, pozyskiwania, gromadzenia lub analizowania danych. Innymi słowy, wystarczy, że produkt ma jedną z tych zdolności technicznych, aby wchodził w zakres zawartej w art. 2 pkt 20 definicji produktu służącego do cyberinwigilacji.

1.2.5. *„Z systemów informatycznych i telekomunikacyjnych”*

Terminy te odnoszą się do systemów, które elektronicznie przetwarzają informacje, np. do systemów programowania/kodowania, operacji systemowych (sprzętowych) wykonywanych na komputerach osobistych oraz do innych systemów zarządzania informacjami, w tym do technologii oprogramowania, technologii internetowej, technologii komputerowej, technologii przechowywania danych itp., oraz do niektórych systemów, które przekazują informacje na odległość, na przykład systemów technicznych przekazujących dźwięki, sygnały, tekst, inne znaki i obrazy zarówno za pośrednictwem kanałów przewodowych, jak i bezprzewodowych, za pośrednictwem światłowodów, łączności radiowej i innych systemów elektromagnetycznych. Te dwa pojęcia łącznie obejmują szeroki zakres systemów przekazywania lub przetwarzania informacji. Należy zauważyć, że termin ten odnosi się do systemów, a nie do urządzeń.

1.2.6. *„Świadomość” i „przeznaczone do”*

Zgodnie z art. 5 ust. 2 rozporządzenia eksporter musi powiadomić właściwy organ, jeżeli jest świadomy, że produkty służące do cyberinwigilacji są przeznaczone do wykorzystywania do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego.

Termin „świadomy” nie jest nową koncepcją prawną, lecz został użyty w związku z wymogami dotyczącymi zezwoleń związanymi z zastosowaniem końcowym (tzw. kontrole typu *catch-all*) zgodnie z art. 4, 6, 7 i 8 rozporządzenia. Bycie „świadomym” oznacza, że eksporter wie o zamierzonym niewłaściwym wykorzystaniu. Sama możliwość wystąpienia takiego ryzyka nie wystarcza do wykazania świadomości. Terminu „świadomość” nie można jednak utożsamiać z biernością: od eksportera wymaga się podjęcia kroków w celu uzyskania wystarczającej i odpowiedniej wiedzy w celu oceny ryzyka związanego z wywozem oraz zapewnienia zgodności z rozporządzeniem.

Wskazanie, że produkty muszą być „przeznaczone do” odpowiedniego wrażliwego końcowego zastosowania, oznacza, że eksporter powinien ocenić końcowe zastosowanie indywidualnie, w świetle szczególnych okoliczności danego przypadku. Z drugiej strony teoretyczne ryzyko, to znaczy ryzyko nieoparte na ocenie stanu faktycznego sprawy, że produkty mogą być wykorzystywane w sposób naruszający prawa człowieka, nie wystarcza, aby sugerować, że „są przeznaczone do” celów konkretnego niewłaściwego wykorzystania, o którym mowa w art. 5.

1.3. **Wewnętrzne represje, poważne naruszenia praw człowieka i międzynarodowego prawa humanitarnego**

Zgodnie z art. 15 rozporządzenia, w którym przedstawiono względy, które należy wziąć pod uwagę przy ocenie na potrzeby ewentualnego zezwolenia, państwa członkowskie muszą wziąć pod uwagę wszystkie istotne względy, w tym kwestie objęte wspólnym stanowiskiem Rady 2008/944/WPZiB ([5]).

W art. 5 rozporządzenia rozszerzono zakres kontroli na wywóz niewymienionych w wykazie produktów służących do cyberinwigilacji ze względu na ryzyko, że zostaną one wykorzystane do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego. Przydatne wskazówki w tym zakresie można znaleźć w tekście wspólnego stanowiska 2008/944/WPZiB oraz w przewodniku do tego wspólnego stanowiska ([6]).

([5]) Wspólne stanowisko Rady 2008/944/WPZiB z dnia 8 grudnia 2008 r. określające wspólne zasady kontroli wywozu technologii wojskowych i sprzętu wojskowego (Dz.U. L 335 z 13.12.2008, s. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Zob. przewodnik do wspólnego stanowiska Rady 2008/944/WPZiB określającego wspólne zasady kontroli wywozu technologii wojskowych i sprzętu wojskowego, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1. *Wewnętrzne represje*

Zgodnie z art. 2 ust. 2 wspólnego stanowiska 2008/944/WPZiB „[r]epresje wewnętrzne obejmują między innymi tortury i inne okrutne, nieludzkie i poniżające traktowanie lub karanie, zbiorowe lub samowolne egzekucje, zaginięcia, samowolne aresztowania i inne poważne pogwałcenia praw człowieka i podstawowych wolności, które są określone w odpowiednich międzynarodowych instrumentach praw człowieka, w tym w Powszechnej deklaracji praw człowieka oraz w Międzynarodowym pakcie praw obywatelskich i politycznych" (ICCPR). Przewodnik do wspólnego stanowiska 2008/944/WPZiB zawiera wskazówki dotyczące elementów, jakie eksporter powinien wziąć pod uwagę przy dokonywaniu oceny, do których to elementów należą m.in. „obecne i przeszłe informacje dotyczące proponowanego użytkownika końcowego w odniesieniu do poszanowania przez niego praw człowieka oraz dane dotyczące państwa-odbiorcy w ogóle".

1.3.2. *Dopuszczanie się poważnych naruszeń praw człowieka*

Niewłaściwe wykorzystywanie niewymienionych w wykazie produktów służących do cyberinwigilacji może mieć negatywny wpływ na szeroki zakres praw człowieka i bezpośrednio koliduje z prawem do prywatności i do ochrony danych. Arbitralna lub bezprawna inwigilacja może również naruszać inne prawa człowieka, takie jak prawo do wolności wypowiedzi, zrzeszania się i zgromadzeń, wolność myśli, sumienia i religii, a także prawo do równego traktowania lub zakaz dyskryminacji oraz prawo do wolnych, równych i tajnych wyborów. W szczególnych przypadkach inwigilacja, w tym monitorowanie lub gromadzenie informacji na temat osób fizycznych, takich jak obrońcy praw człowieka, działacze, osobistości polityczne, słabsze grupy społeczne i dziennikarze, może prowadzić do zastraszania, wywierania nacisków, arbitralnych zatrzymań, tortur, a nawet egzekucji pozasądowych. W związku z tym eksporterzy powinni uwzględnić w swoich ocenach aspekty związane z poważnymi naruszeniami praw człowieka.

Praktyka międzynarodowa pokazuje, że wszelkie ograniczenia praw człowieka muszą być „odpowiednie" i zgodne z międzynarodowymi standardami praw człowieka. W praktyce oznacza to, że istnieją odpowiednie zabezpieczenia służące zapewnieniu, aby ograniczenia były przewidziane prawem i aby pozwalały zachować istotę praw. Ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście służą uzasadnionemu celowi – na przykład bezpieczeństwu narodowemu lub publicznemu, porządkowi publicznemu, ochronie zdrowia publicznego lub ochronie praw i wolności innych osób. Muszą być one ponadto zgodne z zasadą proporcjonalności.

Produkty służące do cyberinwigilacji mogą obejmować legalne i regulowane narzędzia stosowane do egzekwowanie prawa, m.in. do zapobiegania przestępstwom, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych, w tym w dziedzinie zwalczania terroryzmu, lub wykonywania kar. Jednocześnie produkty służące do cyberinwigilacji mogą być również wykorzystywane niezgodnie z przeznaczeniem do celów poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego, jeśli zostaną wywiezione do represyjnych reżimów lub prywatnych użytkowników końcowych lub na obszary objęte konfliktem.

Konieczna jest indywidualna ocena okoliczności każdej sprawy, a właściwe organy, takie jak np. Organizacja Narodów Zjednoczonych, Unia czy Rada Europy, powinny stosować odpowiednie przepisy w odniesieniu do wszelkich doniesień o poważnych naruszeniach praw człowieka. O „poważnym" naruszeniu praw człowieka może świadczyć uznanie tych naruszeń za takie w informacjach publikowanych przez właściwe organy Organizacji Narodów Zjednoczonych, przez Unię lub Radę Europy. Takie wyraźne uznanie przez te organy nie jest absolutnie konieczne, lecz jest istotnym czynnikiem warunkującym spełnienie kryteriów.

Zgodnie z brzmieniem art. 5 naruszenie praw człowieka musi być „poważne". Przydatne wskazówki dotyczące klasyfikowania ewentualnych naruszeń praw człowieka jako „poważne" można znaleźć w przewodniku do wspólnego stanowiska 2008/944/WPZiB. Zgodnie z tym przewodnikiem decydujące znaczenie mają charakter i skutki naruszenia. Jako poważne postrzegane są zazwyczaj naruszenia praw człowieka, które są systematyczne lub szeroko rozpowszechnione, ale również naruszenia, które nie są systematyczne lub szeroko rozpowszechnione, można uznać za „poważne" – na przykład ze względu na dotkliwość interwencji w odniesieniu do poszkodowanych osób.

Załącznik II do przewodnika do wspólnego stanowiska 2008/944/WPZiB zawiera niewyczerpujący wykaz głównych międzynarodowych i regionalnych instrumentów dotyczących praw człowieka, obejmujący Międzynarodowy pakt praw obywatelskich i politycznych (ICCPR), Konwencję w sprawie zakazu stosowania tortur oraz innego okrutnego, nieludzkiego lub poniżającego traktowania albo karania, Konwencję o ochronie praw człowieka i podstawowych wolności („konwencja") oraz Kartę praw podstawowych („Karta"), które to instrumenty mogą dostarczyć istotnych wskazówek w zakresie interpretacji i stosowania kryteriów i ułatwiać tym samym rzetelną ocenę przestrzegania praw człowieka. Wspomniane instrumenty i dołączone do nich odpowiednie protokoły dodatkowe wyznaczają podstawowe międzynarodowe normy i standardy w dziedzinie praw człowieka i podstawowych wolności.

1.3.3. *Dopuszczanie się poważnych naruszeń międzynarodowego prawa humanitarnego*

Międzynarodowe prawo humanitarne (zwane również „prawem genewskim" lub „prawem konfliktów zbrojnych") wypracowano w drodze szeregu traktatów międzynarodowych, przede wszystkim konwencji haskich, konwencji genewskich i ich dwóch protokołów dodatkowych z 1977 r. Prawo to określa zasady, na jakich w czasie konfliktu zbrojnego ochronione są osoby, które nie uczestniczą w działaniach wojennych lub już w nich nie uczestniczą (np. cywile i ranni, chorzy lub schwytani kombatanci), i nakłada na strony walczące ograniczenia w odniesieniu do środków i metod prowadzenia wojny (prawo haskie).

Stosowanie niewymienionych w wykazie produktów służących do cyberinwigilacji powinno być zgodne z międzynarodowym prawem humanitarnym, gdy są one wykorzystywane jako środki i metody walki w kontekście konfliktu zbrojnego. W takich okolicznościach ryzyko poważnych naruszeń międzynarodowego prawa humanitarnego stanowi wzgląd przewidziany w rozporządzeniu i – podobnie jak w przypadku poważnych naruszeń praw człowieka – należy je oceniać w świetle ich zamierzonego końcowego zastosowania w danym przypadku. Przewodnik do wspólnego stanowiska 2008/944/WPZiB zawiera wskazówki dotyczące elementów, które należy wziąć pod uwagę przy ocenie takiego ryzyka, obejmujących m.in. przebadanie przeszłości i teraźniejszości odbiorcy pod względem poszanowania międzynarodowego prawa humanitarnego, intencji odbiorcy wyrażanych w formalnie podejmowanych zobowiązaniach oraz zdolności odbiorcy do zagwarantowania, że sprzęt lub technologia będące przedmiotem transferu zostaną wykorzystane w sposób spójny z międzynarodowym prawem humanitarnym i że nie zostaną przekierowane lub przetransferowane do innych miejsc przeznaczenia, w których mogłyby być wykorzystane do poważnych naruszeń tego prawa.

Zgodnie z art. 5 naruszenie międzynarodowego prawa humanitarnego musi być „poważne". Odnośne wskazówki można znaleźć w przewodniku do wspólnego stanowiska 2008/944/WPZiB, w którym uznano, że „[p]ojedyncze incydenty pogwałcenia międzynarodowego prawa humanitarnego nie muszą być wskaźnikiem stosunku państwa-odbiorcy do międzynarodowego prawa humanitarnego", natomiast „gdy można zaobserwować pewne regularności pogwałceń lub jeżeli państwo-odbiorca nie podjęło odpowiednich kroków, aby ukarać osoby winne pogwałceń, należy się poważnie zastanowić". Wytyczne dotyczące oceny naruszeń międzynarodowego prawa humanitarnego do celów kontroli wywozu przedstawił Międzynarodowy Komitet Czerwonego Krzyża (MKCK). Według MKCK „naruszenia międzynarodowego prawa humanitarnego są poważne, jeżeli zagrażają osobom podlegającym ochronie (np. cywilom, jeńcom wojennym, rannym i chorym) lub przedmiotom (na przykład obiektom cywilnym lub infrastrukturze cywilnej), lub jeżeli naruszają ważne uniwersalne wartości". Przykładem poważnego naruszenia międzynarodowego prawa humanitarnego są zbrodnie wojenne. MKCK wymienia ponadto podobne czynniki, które należy uwzględnić, co w przewodniku do wspólnego stanowiska 2008/944/WPZiB, w tym formalne zobowiązania do stosowania zasad międzynarodowego prawa humanitarnego, odpowiednie środki zapewniające rozliczalność za naruszenia międzynarodowego prawa humanitarnego, szkolenia dla wojska w zakresie międzynarodowego prawa humanitarnego oraz zakaz werbowania dzieci do sił zbrojnych.

2. **ZAKRES TECHNICZNY**

2.1. **Wymienione w wykazie produkty służące do cyberinwigilacji**

W dodatku do niniejszych wytycznych zawarto informacje na temat produktów służących do cyberinwigilacji wymienionych w załączniku I do rozporządzenia, aby pomóc eksporterom w identyfikacji potencjalnych produktów służących do cyberinwigilacji niewymienionych w wykazie.

2.2. **Potencjalne produkty służące do cyberinwigilacji niewymienione w wykazie**

Chociaż z oczywistych względów niemożliwe jest przedstawienie wyczerpującego wykazu tych produktów, które mogą być kontrolowane jako „produkty niewymienione w wykazie" na mocy art. 5, następujące produkty mogą potencjalnie stanowić produkty służące do inwigilacji i wymagać szczególnej czujności zgodnie z rozporządzeniem.

Jak wyjaśniono w motywie 8 rozporządzenia, zasadniczo uznaje się, że produkty stosowane wyłącznie do celów komercyjnych, takich jak naliczanie opłat, marketing, wysokiej jakości usługi, badanie satysfakcji użytkowników lub bezpieczeństwo sieci, nie wiążą się co do zasady z ryzykiem niewłaściwego wykorzystania w rozumieniu poważnych naruszeń praw człowieka lub międzynarodowego prawa humanitarnego, a zatem zasadniczo nie podlegają kontroli na mocy art. 5. Wiele z tych produktów posiada funkcje bezpieczeństwa informacji (kryptograficzne, a nawet kryptoanalityczne), które spełniają parametry kontroli należące do kategorii 5 część 2 tekstu dotyczącego kontroli w załączniku I do rozporządzenia. Urządzenia sieciowe do zapewnienia bezpieczeństwa – w tym routery, przełączniki lub przekaźniki, w przypadku których funkcje ochrony informacji są ograniczone do zadań z zakresu „eksploatacji, administrowania lub utrzymywania" i wykorzystują wyłącznie publiczne lub komercyjne standardy kryptograficzne – również nie są objęte definicją „produktów służących do cyberinwigilacji", chociaż eksporterzy powinni zachować czujność w związku z różnymi doniesieniami o niewłaściwym wykorzystywaniu takich produktów do celów naruszeń praw człowieka.

2.2.1. *Technologie rozpoznawania twarzy i emocji*

Technologie rozpoznawania twarzy i emocji mają wiele zastosowań innych niż cyberinwigilacja – na przykład do identyfikacji lub uwierzytelnienia – i nie wchodzą automatycznie w zakres definicji. W pewnych okolicznościach technologie te mogą jednak wchodzić w zakres art. 2 pkt 20 rozporządzenia.

Technologie rozpoznawania twarzy i emocji, które można wykorzystać do monitorowania lub analizowania przechowywanych obrazów wideo, mogą wchodzić w zakres definicji produktu służącego do cyberinwigilacji. Jednak nawet jeżeli powyższe kryteria są spełnione, należy dokładnie zbadać, czy oprogramowanie jest specjalnie zaprojektowane do celów niejawnego nadzoru.

2.2.2. *Urządzenia do śledzenia lokalizacji*

Urządzenia do śledzenia lokalizacji umożliwiają śledzenie fizycznej lokalizacji urządzenia w czasie, a niektóre technologie śledzenia lokalizacji są od pewnego czasu wykorzystywane przez organy ścigania i agencje wywiadowcze. Ich potencjał w zakresie ukierunkowanej i masowej inwigilacji znacznie się rozwinął, ponieważ technologie śledzenia stały się bardziej zaawansowane – dotyczy to m.in. satelitarnego śledzenia lokalizacji, śledzenia lokalizacji opartego na masztach telefonii komórkowej, nadajniko-odbiorników Wi-Fi i Bluetooth – oraz upowszechniły się „urządzenia lokacyjne" takie jak smartfony i inne urządzenia elektroniczne (np. systemy pokładowe w samochodach).

Urządzenia do śledzenia lokalizacji są wykorzystywane przez organy egzekwowania prawa i agencje wywiadowcze na przykład do gromadzenia dowodów w trakcie postępowania przygotowawczego lub do śledzenia podejrzanych, ale również przez przedsiębiorstwa w celach komercyjnych, na przykład do zgłaszania zagregowanych wzorców przemieszczania się na ulicach handlowych, do śledzenia pracowników pracujących poza terenem przedsiębiorstwa lub do celów reklamowych z wykorzystaniem lokalizacji.

2.2.3. *Systemy monitoringu wizyjnego*

Aby pomóc eksporterom w identyfikacji potencjalnego przypadku cyberinwigilacji, należy wyjaśnić, które produkty nie są objęte definicją. W tym sensie na przykład systemy monitoringu wizyjnego i kamery – w tym kamery o wysokiej rozdzielczości – wykorzystywane do filmowania osób w przestrzeni publicznej nie są objęte definicją produktów służących do cyberinwigilacji, ponieważ nie monitorują ani nie gromadzą danych z systemów informatycznych i telekomunikacyjnych.

3. ŚRODKI NALEŻYTEJ STARANNOŚCI

Zgodnie z motywem 7 rozporządzenia „[k]luczowe znaczenie ma udział eksporterów […] w dążeniu do ogólnego celu kontroli handlu. Aby umożliwić im działanie zgodne z niniejszym rozporządzeniem, ocenę ryzyka związanego z transakcjami, których dotyczy niniejsze rozporządzenie, należy przeprowadzać za pomocą środków kontroli transakcji, znanych również jako zasada należytej staranności, w ramach wewnętrznego programu przestrzegania przepisów".

W art. 2 pkt 21 zdefiniowano „wewnętrzny system kontroli" lub „ICP" jako „obowiązujące skuteczne, odpowiednie i proporcjonalne strategie i procedury przyjmowane przez eksporterów w trosce o przestrzeganie przepisów i osiągnięcie celów niniejszego rozporządzenia oraz spełnienie warunków zezwoleń wdrażanych na mocy niniejszego rozporządzenia, w tym między innymi środki należytej staranności oceniające ryzyko związane z wywozem produktów z przeznaczeniem dla użytkowników końcowych i do zastosowań końcowych".

Zalecenie Komisji (UE) 2019/1318 ([7]) zawiera ramy, które pomogą eksporterom w identyfikacji ryzyka związanego z kontrolą produktów podwójnego zastosowania, zarządzaniu nim i ograniczaniu go, a także w zapewnianiu zgodności z właściwymi unijnymi i krajowymi przepisami ustawowymi i wykonawczymi.

Niniejsze wytyczne mogą zapewniać eksporterom wsparcie przy wdrażaniu środków kontroli transakcji, znanych również jako zasada należytej staranności, w ramach ICP.

Zgodnie z art. 5 ust. 2 rozporządzenia (UE) 2021/821 eksporterzy niewymienionych w wykazie produktów służących do cyberinwigilacji są zobowiązani do przeprowadzenia procedury należytej staranności z zastosowaniem środków kontroli transakcji, co oznacza podjęcie działań dotyczących klasyfikacji produktu i oceny ryzyka transakcji. W praktyce zachęca się eksporterów do sprawdzenia następujących kwestii:

([7]) Zalecenie Komisji (UE) 2019/1318 z dnia 30 lipca 2019 r. w sprawie wewnętrznych programów zgodności dla kontroli handlu produktami podwójnego zastosowania na podstawie rozporządzenia Rady (WE) nr 428/2009 (Dz.U. L 205 z 5.8.2019, s. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Należy sprawdzić, czy produkt niewymieniony w wykazie, który ma zostać wywieziony, może być „produktem służącym do cyberinwigilacji", czyli specjalnie zaprojektowanym w celu umożliwienia niejawnego nadzoru nad osobami fizycznymi poprzez monitorowanie, pobieranie, gromadzenie lub analizowanie danych z systemów informatycznych i telekomunikacyjnych.**

Etap ten dotyczy określenia produktu na podstawie przepisów mających zastosowanie do produktów służących do cyberinwigilacji. W tym celu przeprowadza się badanie właściwości technicznych produktów na podstawie parametrów technicznych określonych w załączniku I do rozporządzenia w przypadku produktów wymienionych w wykazie oraz w świetle konkretnych terminów i pojęć zawartych w definicji produktów służących do cyberinwigilacji w przypadku produktów niewymienionych w wykazie i w świetle późniejszej klasyfikacji badanych produktów (towarów, technologii lub oprogramowania).

3.2. **Należy sprawdzić właściwości danego produktu w celu ustalenia możliwości jego niewłaściwego wykorzystania do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego przez zagranicznych użytkowników końcowych.**

Eksporterzy powinni przeprowadzić ocenę w celu ustalenia, czy produkt może zostać wykorzystany niezgodnie z przeznaczeniem do celów wewnętrznych represji, naruszania lub łamania praw człowieka, w tym prawa do życia, prawa do wolności od tortur, nieludzkiego i poniżającego traktowania, prawa do prywatności, prawa do wolności słowa, prawa do zrzeszania się i zgromadzeń, prawa do wolności myśli, sumienia i religii, prawa do równego traktowania lub zakazu dyskryminacji lub prawa do wolnych, równych i tajnych wyborów.

Na tym etapie należy również ocenić, czy produkt może być wykorzystywany jako część lub element systemu, który mógłby skutkować takimi samymi naruszeniami lub niewłaściwym wykorzystaniem.

Eksporterzy powinni stosować w swojej ocenie tzw. czerwone flagi, które ostrzegają o wszelkich nadzwyczajnych okolicznościach transakcji wskazujących, że wywóz może być przeznaczony do niewłaściwego zastosowania końcowego, dla niewłaściwego użytkownika końcowego lub do niewłaściwego miejsca przeznaczenia.

Czerwone flagi (sygnały ostrzegawcze):

a) produkt wprowadzany do obrotu opatrzono informacjami dotyczącymi jego potencjalnego wykorzystania do niejawnego nadzoru;

b) informacje wskazujące, że podobny produkt został niewłaściwie wykorzystany do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego (zob. pkt 1.3);

c) informacje wskazujące, że dany produkt został bezprawnie wykorzystany w działaniach inwigilacyjnych skierowanych przeciwko państwu członkowskiemu lub w związku z bezprawną inwigilacją obywatela Unii;

d) informacje wskazujące, że transakcja obejmuje produkty, które mogą zostać wykorzystane do budowy, dostosowania lub skonfigurowania systemu, o którym wiadomo, że jest wykorzystywany niezgodnie z przeznaczeniem do celów wewnętrznych represji lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego (zob. pkt 1.3);

e) dany produkt lub produkt podobny znajduje się w wykazie opublikowanym w serii C *Dziennika Urzędowego Unii Europejskiej* zgodnie z art. 5 ust. 6 rozporządzenia.

3.3. **W celu wsparcia właściwych organów należy sprawdzić zainteresowane strony zaangażowane w transakcję (w tym użytkowników końcowych i odbiorców, takich jak dystrybutorzy i odsprzedawcy).**

W celu wsparcia właściwych organów eksporterzy powinni w miarę możliwości:

a) przed transakcją i w jej trakcie sprawdzić, w jaki sposób odbiorcy lub użytkownicy końcowi zamierzają korzystać z produktu lub usługi, na podstawie deklaracji zastosowania końcowego;

b) zapoznać się z sytuacją panującą w miejscu przeznaczenia produktów, zwłaszcza ogólną sytuacją w zakresie praw człowieka, ponieważ stanowi to ważny wskaźnik związanego z wywozem ryzyka poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego;

c) dokonać przeglądu ryzyka, że produkt lub usługa zostaną przekierowane do innego nieupoważnionego użytkownika końcowego, na podstawie „czerwonych flag" wymienionych poniżej.

Czerwone flagi (sygnały ostrzegawcze):

a) użytkownik końcowy utrzymuje oczywistą relację z obcym rządem, który dopuścił się represji wewnętrznych lub poważnych naruszeń praw człowieka i międzynarodowego prawa humanitarnego;

b) użytkownik końcowy jest strukturalnie częścią sił zbrojnych lub innej grupy będącej uczestnikiem konfliktu zbrojnego obejmującego wewnętrzne środki represji lub poważne naruszenia praw człowieka i międzynarodowego prawa humanitarnego;

c) użytkownik końcowy wywoził w przeszłości produkty służące do cyberinwigilacji do krajów, w których wykorzystanie takich produktów doprowadziło do zastosowania wewnętrznych środków represji lub poważnego naruszenia praw człowieka i międzynarodowego prawa humanitarnego.

3.4. **Należy wykorzystać ustalenia dokonane w ramach procedury należytej staranności do opracowania planów zapobiegania potencjalnym przyszłym niekorzystnym skutkom i ich łagodzenia.**

Eksporterzy powinni, na podstawie swoich ustaleń dokonanych w ramach procedury należytej staranności, zaprzestać działań, które wywołują niekorzystne skutki związane z prawami człowieka lub przyczyniają się do ich wywołania, a także opracować i wdrożyć plan działań naprawczych. Działania takie mogą obejmować:

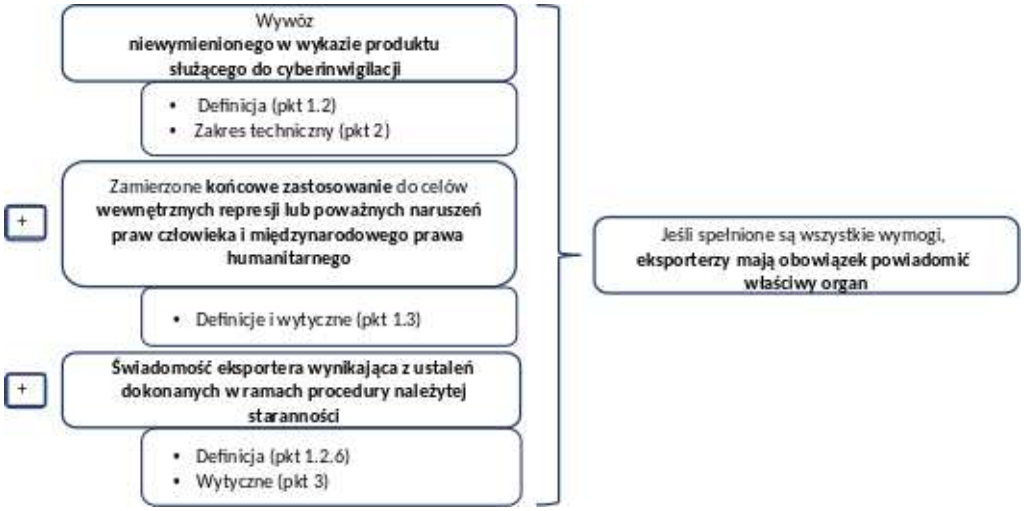
a) zaktualizowanie polityki przedsiębiorstwa w celu przedstawienia wytycznych dotyczących sposobów unikania niekorzystnych skutków i przeciwdziałania im w przyszłości oraz zadbanie o wdrożenie tych wytycznych;

b) wyciąganie wniosków z wyników oceny ryzyka w celu aktualizacji i wzmocnienia systemów zarządzania, aby usprawnić śledzenie informacji i sygnalizowanie ryzyka przed wystąpieniem niekorzystnych skutków;

c) gromadzenie informacji w celu zrozumienia wysokiego ryzyka niekorzystnych skutków związanych z danym sektorem;

d) powiadamianie właściwych organów państw członkowskich o ustaleniach dokonanych w ramach procedury należytej staranności w celu ułatwienia przepływu informacji w odniesieniu do niektórych produktów, użytkowników końcowych i miejsc przeznaczenia.

Wymogi określone w art. 5 ust. 2 rozporządzenia (UE) 2021/821



4. **DODATEK**

Wymienione w wykazie produkty służące do cyberinwigilacji podlegające kontroli zgodnie z załącznikiem I do rozporządzenia (UE) 2021/821

— **Systemy przechwytywania przekazów telekomunikacyjnych (5A001.f.)**

W większości państw, w tym w państwach członkowskich, poufność komunikacji jest chroniona prawem, ale ramy prawne mogą dopuszczać niejawny nadzór elektroniczny komunikacji prowadzony przez organy rządowe (tzw. uprawnione przechwytywanie). W erze cyfrowej pojawiła się jednak możliwość korzystania z technologii przechwytywania na masową skalę. Wykorzystanie narzędzi przechwytywania przez reżim libijski unaoczniło potencjał masowego zastosowania tych technologii i przyspieszyło wprowadzenie kontroli wywozu systemów przechwytywania przekazów telekomunikacyjnych w 2012 r.

Kontrola w ramach tej pozycji ma zastosowanie do urządzeń zaprojektowanych do pobierania treści komunikatu (głosu lub danych), jak również identyfikatorów abonenta lub innych metadanych przesyłanych bezprzewodowo za pośrednictwem łączności bezprzewodowej, a także do urządzeń do monitorowania częstotliwości radiowych. Kontrola ta ma zastosowanie na przykład do urządzeń typu *IMSI Catcher* (ang. *International Mobile Subscriber Identity*, międzynarodowy numer tożsamości telefonicznej abonenta mobilnego), które przechwytują dane na temat ruchu w sieci telefonii komórkowej i monitorują ruch użytkowników telefonów komórkowych, lub do urządzeń tworzących fałszywe hotspoty Wi-Fi, które mogą pobierać numery IMSI z telefonu, a także do niektórych rodzajów produktów specjalnie zaprojektowanych w celu umożliwienia „głębokiej inspekcji pakietów" w systemach telekomunikacyjnych. Urządzenia zakłócające telekomunikację ruchomą nie wchodzą w zakres produktów służących do cyberinwigilacji, ponieważ nie gromadzą danych.

Chociaż do budowy takich systemów można wykorzystać technologię ogólnego zastosowania, ich zdolność przechwytywania na masową skalę będzie zależeć od określonych części i komponentów, w tym na przykład konkretnego oprogramowania oraz zaawansowanych lub specjalizowanych układów scalonych (np. czipów FPGA, układów ASIC itp.), umożliwiających zwiększenie liczby pakietów lub sesji komunikacyjnych możliwych do przetworzenia w ciągu sekundy.

— **Systemy nadzoru internetu (5A001.j.)**

Chociaż komunikacja w internecie jest obecnie w dużym stopniu domyślnie szyfrowana, przechwytywanie danych o ruchu (metadanych) dotyczących komunikacji – takich jak adresy IP oraz częstotliwość i wielkość wymiany danych – może być nadal wykorzystywane do identyfikacji powiązań między osobami a nazwami domen. Rządy mogą korzystać z tych systemów zgodnie z prawem i pod nadzorem sądowym w uzasadnionych celach, takich jak identyfikacja osób, które odwiedzają domeny związane z treściami przestępczymi lub terrorystycznymi. Monitorowanie i analiza ruchu internetowego na podstawie charakterystyki etnicznej, religijnej, politycznej lub społecznej może jednak prowadzić do kompleksowego mapowania społeczeństwa danego kraju w celu kontroli ludności i represji, a także do innych celów, na przykład by identyfikować dysydentów politycznych. Oprócz kwestii związanych z prawami człowieka i represjami wewnętrznymi produkty te mogą również przyczynić się do zwiększenia bezpieczeństwa i zdolności wojskowych.

Kontrola w ramach pozycji 5A001.j ma zastosowanie do systemów kontroli internetu, które są wykorzystywane w „sieci IP klasy operatorskiej (np. krajowa sieć szkieletowa IP)" do celów analizy, pobierania i indeksowania przekazywanych treści metadanych (głosu, wideo, wiadomości, załączników) w oparciu o „twarde parametry" oraz do celów mapowania sieci powiązań międzyludzkich. Są to produkty, które służą do prowadzenia „niejawnego nadzoru", ponieważ osoby inwigilowane nie są świadome przechwytywania komunikatów. Kontrole w ramach tej pozycji nie dotyczą natomiast systemów, w których występuje działanie użytkownika lub abonenta lub interakcja z użytkownikiem lub abonentem, i na przykład nie mają zastosowania do sieci społecznościowych lub wyszukiwarek komercyjnych. Ponadto kontrole mają zastosowanie do systemów przetwarzających dane pochodzące z sieci bazowej dostawcy internetu, a nie mają zastosowania do sieci społecznościowych ani wyszukiwarek komercyjnych, które przetwarzają dane przekazane przez użytkowników.

— **„Złośliwe oprogramowanie" (4A005, 4D004 i związane z nim kontrole w ramach pozycji 4E001.a. i 4E001.c.)**

Złośliwe oprogramowanie zapewnia korzystającej z niego osobie niejawny dostęp zdalny do urządzenia elektronicznego, takiego jak smartfon, laptop, serwer lub urządzenie podłączone do internetu rzeczy, i uzyskanie danych przechowywanych na takim urządzeniu, podsłuchiwanie za pośrednictwem kamery lub mikrofonu wbudowanego w urządzeniu lub podłączonego do niego oraz wykorzystanie urządzenia do przeprowadzenia ataków na sprzęt, do którego się ono podłącza, lub ataków za pośrednictwem kontaktów użytkownika („hakowanie za pośrednictwem urządzeń osób trzecich"). Chociaż istnieją legalne zastosowania [8] złośliwego oprogramowania, na przykład „oprogramowanie zdalnego dostępu" wykorzystywane do zdalnego wsparcia ze strony działów informatycznych, niejawny charakter nadzoru i ilość ewentualnie gromadzonych informacji stwarza wysokie ryzyko naruszenia prawa do prywatności i ochrony danych osobowych oraz może poważnie naruszyć prawo do wolności wypowiedzi.

[8] Dla zachowania jasności w odniesieniu do wymienionych w wykazie produktów służących do cyberinwigilacji podlegających kontroli zgodnie z załącznikiem I do rozporządzenia w sprawie produktów podwójnego zastosowania wymaga się zezwolenia na wywóz do państw trzecich, niezależnie od tego, czy korzystanie z tych produktów jest zgodne z prawem.

Kontrola w ramach pozycji 4A005 i in. obejmuje oprogramowanie, jak również systemy, wyposażenie, części składowe i powiązane z nimi technologie, specjalnie zaprojektowane lub zmodyfikowane do tworzenia „złośliwego oprogramowania", zarządzania i sterowania nim lub dostarczania takiego oprogramowania, ale nie ma zastosowania do samego „złośliwego oprogramowania", jak określono w załączniku I do rozporządzenia. Te narzędzia cybernetyczne podlegają kontroli pod kątem potencjalnych zakłóceń i szkód, jakie mogą one spowodować, jeżeli zostaną z powodzeniem użyte i zastosowane, ale taka kontrola nie ma wpływać negatywnie na przykład na działalność badaczy zajmujących się cyberbezpieczeństwem ani samej branży ogółem, ponieważ badacze i branża muszą wymieniać się informacjami związanymi ze złośliwym oprogramowaniem, aby móc opracować rozwiązania dla swoich produktów i wdrożyć je przed publicznym udostępnieniem informacji na temat podatności.

— **Oprogramowanie do monitorowania komunikacji (5D001.e.)**

Oprogramowanie to jest przeznaczone do monitorowania i analizy przez upoważnione organy egzekwowania prawa danych zgromadzonych za pomocą środków ukierunkowanego przechwytywania, o których udostępnienie poproszono dostawcę usług komunikacyjnych. Oprogramowanie to umożliwia wyszukiwanie w oparciu o „twarde parametry" zawartości komunikatów lub metadanych, z wykorzystaniem interfejsu do uprawnionego przechwytywania danych, a także mapowanie sieci powiązań lub śledzenie ruchu namierzanych osób na podstawie wyników wyszukiwania. Oprogramowanie to jest przeznaczone do „niejawnego nadzoru", ponieważ wykorzystuje ono dane zgromadzone w wyniku przechwytywania komunikacji bez wiedzy osób, których dane te dotyczą. Ponadto „analizuje" ono dane gromadzone za pośrednictwem „systemów telekomunikacyjnych". Oprogramowanie jest zainstalowane w organie rządowym [np. w ośrodku monitoringu egzekwowania prawa (LEMF)] a kontrola nie ma zastosowania do systemów monitorowania uprawnionego przechwytywania (LI) (np. systemów zarządzania uprawnionym przechwytywaniem i urządzeń mediacyjnych), które są opracowywane komercyjne i instalowane w przestrzeni dostawcy usług komunikacyjnych (na przykład zintegrowane z siecią łączności) oraz które dostawca usług eksploatuje i utrzymuje. Jak wyjaśniono w tekście dotyczącym kontroli, kontrole nie mają zastosowania do „oprogramowania" specjalnie zaprojektowanego lub zmodyfikowanego do celów czysto komercyjnych, takich jak cele rozliczeniowe, sieciowa jakość usług (QoS), postrzegalna jakość usług (QoE), urządzenia mediacyjne i wykorzystanie do płatności mobilnych lub bankowości.

— **Produkty stosowane do przeprowadzania kryptoanalizy (5A004.a.)**

Kontrole w ramach tej pozycji dotyczą produktów zaprojektowanych do łamania mechanizmów kryptograficznych w celu uzyskania tajnych informacji lub wrażliwych danych, włączając w to tekst jawny, hasła lub klucze kryptograficzne. Kryptografia jest wykorzystywana do ochrony poufności informacji przesyłanych i przechowywanych. Kryptoanaliza jest stosowana w celu przełamania tej poufności, a zatem technologia ta umożliwia niejawny nadzór poprzez monitorowanie, pobieranie, gromadzenie lub analizowanie danych z systemów informacyjnych i telekomunikacyjnych.

— **Narzędzia kryminalistyczne/dochodzeniowe (5A004.b., 5D002.a.3.b. i 5D002.c.3.b.)**

Narzędzia kryminalistyczne/dochodzeniowe są zaprojektowane do pobierania surowych danych z urządzenia (na przykład z obliczeń lub komunikacji) tak, aby dane te nie zostały naruszone ani uszkodzone i aby mogły być wykorzystane do celów sądowych, tj. w postępowaniu przygotowawczym lub w sądzie. Produkty te pozwalają obejść „uwierzytelnianie" lub kontrole autoryzacji w urządzeniu, tak aby zapewnić możliwość pobrania nieprzetworzonych danych z urządzenia. Produkty te są wykorzystywane przez rząd i organy egzekwowania prawa, jak również przez siły wojskowe do pobierania i analizowania danych z zajętych urządzeń. Chociaż są one wykorzystywane zgodnie z prawem, istnieje możliwość ich niewłaściwego wykorzystywania, w związku z czym stwarzają ryzyko dla danych szczególnie chronionych lub handlowych.

Narzędzia kryminalistyczne/dochodzeniowe, które nie są „specjalnie zaprojektowane" do celów niejawnego nadzoru, nie wchodzą jednak w zakres definicji produktów służących do cyberinwigilacji zawartej w art. 2 pkt 20. Ponadto narzędzia kryminalistyczne/dochodzeniowe, które pobierają wyłącznie dane użytkownika lub gdy dane te nie są chronione na urządzeniu, nie są ujęte w tekście dotyczącym kontroli w pozycji 5A004.b. i in. Jednocześnie kontrole nie mają zastosowania do urządzeń produkcyjnych ani badawczych producenta, narzędzi administratora systemu ani produktów przeznaczonych wyłącznie dla komercyjnego sektora detalicznego, na przykład produktów do odblokowywania telefonów komórkowych. W związku z tym, biorąc pod uwagę różnorodność tych rodzajów technologii, stosowanie kontroli zależy od indywidualnej oceny każdego produktu.

Ponadto należy zauważyć, że istnieją inne produkty związane z prowadzeniem nadzoru, wymienione w załączniku I do rozporządzenia, których nie należy uznawać za wchodzące w zakres definicji produktów służących do cyberinwigilacji, takie jak urządzenia zakłócające telekomunikację ruchomą (5A001.f.) zaprojektowane do uszkadzania lub zakłócania komunikacji lub systemów, złośliwe oprogramowanie modyfikujące system (4D004) oraz laserowe urządzenia do detekcji akustycznej (6A005.g.) gromadzące dane dźwiękowe za pomocą lasera lub umożliwiające słuchanie rozmów na odległość (czasami zwane „mikrofonem laserowym"). Podobnie wykorzystanie wymienionych w wykazie bezzałogowych statków powietrznych do celów nadzoru nie spowodowałoby objęcia tych produktów definicją produktów służących do cyberinwigilacji.