P9_TA(2023)0244

Dochodzenie w sprawie wykorzystania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego (zalecenie)

Zalecenie Parlamentu Europejskiego z dnia 15 czerwca 2023 r. dla Rady i Komisji w następstwie dochodzenia w sprawie zarzutów naruszenia prawa Unii i niewłaściwego administrowania w jego stosowaniu w odniesieniu do oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego (2023/2500(RSP))

(C/2024/494)

Parlament Europejski,

— uwzględniając Traktat o Unii Europejskiej (TUE), w szczególności jego art. 2, 4, 6 i 21,

— uwzględniając art. 16, 223, 225 i 226 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE),

— uwzględniając Kartę praw podstawowych Unii Europejskiej (Karta), w szczególności jej art. 7, 8, 11, 17, 21, 41, 42 i 47,

— uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) ([1]) („dyrektywa o e-prywatności"),

— uwzględniając 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 (ogólne rozporządzenie o ochronie danych) ([2]),

— uwzględniając dyrektywę 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 uchylającą decyzję ramową Rady 2008/977/WSiSW ([3]),

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne i zastępującą decyzję ramową Rady 2005/222/WSiSW ([4]) („dyrektywa w sprawie cyberprzestępczości"),

— uwzględniając 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 ([5]) („rozporządzenie w sprawie podwójnego zastosowania"),

— uwzględniając decyzję Rady (WPZiB) 2019/797 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim ([6]), zmienioną decyzją Rady (WPZiB) 2021/796 z dnia 17 maja 2021 r. ([7]),

— uwzględniając Akt dotyczący wyborów przedstawicieli do Parlamentu Europejskiego w powszechnych wyborach bezpośrednich ([8]),

— uwzględniając decyzję 95/167/WE, Euratom, EWWiS Parlamentu Europejskiego, Rady i Komisji z dnia 6 marca 1995 r. w sprawie szczegółowych przepisów regulujących egzekwowanie przez Parlament Europejski jego prawa do prowadzenia dochodzeń ([9]),

([1]) Dz.U. L 201 z 31.7.2002, s. 37.
([2]) Dz.U. L 119 z 4.5.2016, s. 1.
([3]) Dz.U. L 119 z 4.5.2016, s. 89.
([4]) Dz.U. L 218 z 14.8.2013, s. 8.
([5]) Dz.U. L 206 z 11.6.2021, s. 1.
([6]) Dz.U. L 129 I z 17.5.2019, s. 13.
([7]) Dz.U. L 174 I z 18.5.2021, s. 1.
([8]) Dz.U. L 278 z 8.10.1976, s. 5.
([9]) Dz.U. L 113 z 19.5.1995, s. 1.

— uwzględniając decyzję Parlamentu Europejskiego (UE) 2022/480 z dnia 10 marca 2022 r. w sprawie powołania komisji śledczej w celu zbadania stosowania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego służącego inwigilacji oraz określenia przedmiotu dochodzenia, a także zakresu odpowiedzialności, składu liczbowego i czasu trwania mandatu komisji ([10]),

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniającą dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniającą dyrektywy 2009/138/WE i 2013/36/UE ([11]) („dyrektywa w sprawie przeciwdziałania praniu pieniędzy"),

— uwzględniając wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady z dnia 16 września 2022 r. ustanawiającego wspólne ramy dla usług medialnych na rynku wewnętrznym („europejski akt o wolności mediów") i zmieniającego dyrektywę 2010/13/UE (COM(2022)0457),

— uwzględniając art. 12 Powszechnej deklaracji praw człowieka,

— uwzględniając wyrok Trybunału Sprawiedliwości Unii Europejskiej (TSUE) w sprawie C-37/20 ([12]) dotyczącej dyrektywy w sprawie przeciwdziałania praniu pieniędzy stwierdzający nieważność przepisu przewidującego, że informacje o rzeczywistych beneficjentach podmiotów o charakterze korporacyjnym utworzonych na terytorium państw członkowskich mają być we wszystkich przypadkach udostępniane każdej osobie,

— uwzględniając art. 17 Międzynarodowego paktu praw obywatelskich i politycznych,

— uwzględniając Kartę Narodów Zjednoczonych oraz Wytyczne ONZ dotyczące biznesu i praw człowieka ([13]),

— uwzględniając oświadczenie Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka Michelle Bachelet z 19 lipca 2022 r. w sprawie stosowania oprogramowania szpiegowskiego do inwigilacji dziennikarzy i obrońców praw człowieka,

— uwzględniając komentarz Komisarz Praw Człowieka Rady Europy Dunji Mijatovic z 27 stycznia 2023 r. pt. „Wysoce inwazyjne oprogramowanie szpiegowskie zagraża istocie praw człowieka" ([14]),

— uwzględniając uwagi wstępne na temat nowoczesnego oprogramowania szpiegowskiego Europejskiego Inspektora Ochrony Danych (EIOD) z 15 lutego 2022 r. ([15]),

— uwzględniając Konwencję o ochronie praw człowieka i podstawowych wolności, w szczególności jej art. 8, 10, 13, 14 i 17, oraz protokoły do tej konwencji,

— uwzględniając ocenę zagrożenia poważną i zorganizowaną przestępczością w 2021 r. Europolu zatytułowaną „A Corrupting Influence: The infiltration and undermining of Europe's economy and society by organised crime" [„Demoralizujący wpływ: infiltracja i działanie przestępczości zorganizowanej na szkodę europejskiej gospodarki oraz społeczeństwa"],

— uwzględniając sprawozdanie Agencji Praw Podstawowych Unii Europejskiej (FRA) z 2017 r. zatytułowane „Nadzór prowadzony przez służby wywiadowcze: gwarancje praw podstawowych i środki zaradcze w UE", a także jego aktualizację przedstawioną 28 lutego 2023 r. komisji śledczej ds. zbadania stosowania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego służącego inwigilacji (PEGA),

— uwzględniając swoją rezolucję z dnia 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych ([16]), a w szczególności zawarte w niej zalecenia dotyczące wzmocnienia bezpieczeństwa informatycznego w instytucjach, organach i agencjach UE,

— uwzględniając opinię EIOD nr 24/2022 z dnia 11 listopada 2022 r. w sprawie europejskiego aktu o wolności mediów,

— uwzględniając glosariusz opracowany przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) dotyczący złośliwego oprogramowania i oprogramowania szpiegowskiego,

---

([10]) Dz.U. L 98 z 25.3.2022, s. 72.
([11]) Dz.U. L 156 z 19.6.2018, s. 43.
([12]) Wyrok Trybunału (wielka izba) z dnia 22 listopada 2022 r., C-37/20, WM i Sovim SA/Luxembourg Business Registers, ECLI.EU:C:2022:912.
([13]) https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
([14]) https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights
([15]) https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf
([16]) Dz.U. C 378 z 9.11.2017, s. 104.

— uwzględniając decyzję Europejskiego Rzecznika Praw Obywatelskich w sprawie sposobu, w jaki Komisja Europejska oceniła wpływ na prawa człowieka przed udzieleniem wsparcia krajom afrykańskim w rozwijaniu zdolności w zakresie nadzoru (sprawa 1904/2021/MHZ),

— uwzględniając oświadczenie specjalnej sprawozdawczyni ONZ ds. wolności opinii i wypowiedzi Irene Kahn oraz specjalnego sprawozdawcy ONZ ds. mniejszości Fernanda de Varennesa z 2 lutego 2023 r., w którym domagają się oni przeprowadzenia dochodzenia w sprawie domniemanego użycia programu szpiegowskiego przeciwko katalońskim przywódcom ([17]),

— uwzględniając sprawozdanie Europejskiej Komisji na rzecz Demokracji przez Prawo (Komisji Weneckiej) w sprawie demokratycznego nadzoru nad służbami bezpieczeństwa ([18]) oraz jej opinię zatytułowaną „Polska – opinia w sprawie ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw" ([19]),

— uwzględniając sprawozdanie komisji śledczej ds. zbadania stosowania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego służącego inwigilacji (A9-0189/2023),

— uwzględniając art. 208 ust. 12 Regulaminu,

A. mając na uwadze, że dzięki staraniom CitizenLab i Amnesty Tech oraz licznych dziennikarzy śledczych ujawniono, że organy rządowe w kilku krajach, zarówno państwach członkowskich, jak i krajach spoza UE, wykorzystywały oprogramowanie Pegasus i równoważne oprogramowanie szpiegowskie przeciwko dziennikarzom, politykom, funkcjonariuszom organów ścigania, dyplomatom, prawnikom, przedsiębiorcom, podmiotom społeczeństwa obywatelskiego i innym podmiotom w celach politycznych, a nawet przestępczych; mając na uwadze, że takie praktyki są niezwykle niepokojące i wskazują na ryzyko nadużywania technologii nadzoru do naruszania podstawowych praw człowieka, demokracji i procesów wyborczych;

B. mając na uwadze, że ilekroć w sprawozdaniu pojawia się termin „oprogramowanie szpiegowskie", oznacza on „oprogramowanie Pegasus i równoważne oprogramowanie szpiegowskie służące inwigilacji" zgodnie z definicją zawartą w decyzji Parlamentu o utworzeniu komisji śledczej PEGA;

C. mając na uwadze, że zaobserwowano, iż podmioty państwowe celowo używały oprogramowania szpiegowskiego w niewłaściwy sposób, wykorzystując oprogramowanie szpiegowskie, które może ukrywać się jako legalny program, plik lub treści („koń trojański"), np. jako fałszywe komunikaty instytucji publicznych; mając na uwadze, że w niektórych przypadkach organy publiczne wykorzystywały operatorów telefonii komórkowej do przekazywania złośliwych treści na urządzenia inwigilowanych osób; mając na uwadze, że oprogramowanie szpiegowskie można stosować poprzez wykorzystywanie luk zero-day bez interakcji celu z zainfekowanymi treściami i może ono usuwać wszystkie ślady swojej obecności po odinstalowaniu, a także anonimizować powiązanie między operatorami zdalnymi a serwerem;

D. mając na uwadze, że w początkowym okresie istnienia łączności komórkowej przechwytywano rozmowy w celu ich podsłuchiwania, a później – wiadomości tekstowe w zwykłym formacie;

E. mając na uwadze, że pojawienie się szyfrowanych aplikacji do łączności komórkowej doprowadziło do powstania branży oprogramowania szpiegowskiego wykorzystującej luki w systemach operacyjnych smartfonów w celu instalowania oprogramowania służącego do importowania oprogramowania szpiegowskiego do telefonu, w tym poprzez infekcje typu „zero kliknięć", bez wiedzy użytkownika lub jakiegokolwiek działania z jego strony, umożliwiające ekstrakcję danych przed ich zaszyfrowaniem; mając na uwadze, że takie oprogramowanie szpiegowskie typu „zero kliknięć" ze względu na swoją konstrukcję bardzo utrudnia skuteczną i merytoryczną kontrolę jego stosowania;

F. mając na uwadze, że wiedza na temat luk w systemach oprogramowania jest przedmiotem handlu bezpośrednio między stronami lub za pomocą pośredników; mając na uwadze, że handel ten obejmuje podmioty niepaństwowe i organizacje przestępcze;

G. mając na uwadze, że nabywanie luk zero-day, handel nimi i ich akumulacja zasadniczo osłabiają integralność i bezpieczeństwo komunikacji oraz cyberbezpieczeństwo obywateli Unii;

H. mając na uwadze, że inwigilacja za pomocą oprogramowania szpiegowskiego powinna pozostać wyjątkiem i zawsze wymagać uprzedniego uzyskania wiążącej i prawomocnej zgody bezstronnego i niezależnego organu sądowego, który musi upewnić się, że środek ten jest konieczny i proporcjonalny oraz ściśle ograniczony do przypadków mających wpływ na bezpieczeństwo narodowe lub związanych z terroryzmem i poważną przestępczością; mając na uwadze, że w środowisku pozbawionym skutecznych mechanizmów kontroli i równowagi techniki nadzoru bywają nadużywane;

([17]) https://www.ohchr.org/en/press-releases/2023/02/spain-un-experts-demand-investigation-alleged-spying-programme-targeting
([18]) https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e
([19]) https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e

I. mając na uwadze, że wszelkie przypadki inwigilacji z wykorzystaniem oprogramowania szpiegowskiego muszą podlegać kontroli *ex post* ze strony niezależnego organu nadzoru, który musi dopilnować, aby wszelka dozwolona inwigilacja była prowadzona z poszanowaniem praw podstawowych i zgodnie z warunkami określonymi przez TSUE, Europejski Trybunał Praw Człowieka (ETPC) i Komisję Wenecką; mając na uwadze, że taki organ nadzoru *ex post* powinien nakazać natychmiastowe zaprzestanie nadzoru, jeżeli zostanie on uznany za niezgodny z wyżej wymienionymi prawami i warunkami;

J. mając na uwadze, że prowadzona za pomocą oprogramowania szpiegowskiego inwigilacja niespełniająca wymogów określonych w prawie Unii oraz w orzecznictwie TSUE i ETPC jest sprzeczna z wartościami zapisanymi w art. 2 TUE oraz prawami podstawowymi zapisanymi w Karcie, w szczególności w jej art. 7, 8, 11, 17, 21 i 47, w których uznaje się określone w niej szczególne prawa, wolności i zasady, takie jak poszanowanie życia prywatnego i rodzinnego, ochrona danych osobowych, wolność wypowiedzi i informacji, prawo własności, prawo do niedyskryminacji, a także prawo do skutecznego środka prawnego i rzetelnego procesu sądowego oraz domniemania niewinności;

K. mając na uwadze, że prawa inwigilowanych osób są określone w Karcie i konwencjach międzynarodowych, zwłaszcza prawo do prywatności i prawo do rzetelnego procesu sądowego, a także w przepisach Unii dotyczących praw osób podejrzanych i oskarżonych; mając na uwadze, że prawa te znalazły potwierdzenie w orzecznictwie TSUE i ETPC;

L. mając na uwadze, że nadzór ukierunkowany na kobiety może być szczególnie dotkliwy, ponieważ władze mogą wykorzystywać zwiększoną kontrolę społeczną nad kobietami oraz prywatne i intymne dane pozyskane za pomocą oprogramowania szpiegowskiego jako broń w kampaniach zniesławienia;

M. mając na uwadze, że – jak jasno wynika z zeznań osób inwigilowanych – nawet jeśli środki odwoławcze i prawa obywatelskie istnieją na papierze, zwykle pozostają one tylko w sferze teorii w obliczu utrudnień ze strony organów państwowych, braku lub niewdrożenia prawa osób inwigilowanych do otrzymywania informacji oraz bariery administracyjnej polegającej na tym, że osoby muszą udowodnić, że były celem ataków; mając na uwadze, że nawet w systemach z szybkimi i otwartymi procedurami charakter oprogramowania szpiegowskiego znacznie utrudnia udowodnienie autorstwa oraz charakteru i zakresu, w jakim dana osoba była celem ataku;

N. mając na uwadze, że sądy nie akceptują dowodów kryminalistycznych niezależnych ekspertów, a jedynie dowody oparte na badaniu władz, organów bezpieczeństwa lub organów ścigania, które jednocześnie mają stać za atakiem; mając na uwadze, że stawia to ofiary w paradoksalnej sytuacji i pozbawia realnej możliwości udowodnienia zainfekowania oprogramowaniem szpiegowskim;

O. mając na uwadze, że rząd polski osłabił i zlikwidował instytucjonalne i prawne zabezpieczenia, w tym odpowiednie procedury nadzoru i kontroli, w efekcie pozbawiając osoby inwigilowane jakichkolwiek znaczących środków odwoławczych; mając na uwadze, że oprogramowanie szpiegowskie Pegasus wykorzystywano nielegalnie do celów politycznych do szpiegowania dziennikarzy, polityków opozycji, prawników, prokuratorów i podmiotów społeczeństwa obywatelskiego;

P. mając na uwadze, że rząd węgierski osłabił i zlikwidował instytucjonalne i prawne zabezpieczenia, w tym odpowiednie procedury nadzoru i kontroli, w efekcie pozostawiając osoby inwigilowane bez jakichkolwiek istotnych środków odwoławczych; mając na uwadze, że oprogramowanie szpiegowskie Pegasus wykorzystywano nielegalnie do celów politycznych do szpiegowania dziennikarzy, polityków opozycji, prawników, prokuratorów i podmiotów społeczeństwa obywatelskiego;

Q. mając na uwadze, że oficjalnie potwierdzono, iż grecki poseł do Parlamentu Europejskiego i grecki dziennikarz byli podsłuchiwani przez greckie służby wywiadowcze (EYP) i namierzani za pomocą oprogramowania szpiegowskiego Predator; mając na uwadze, że były amerykańsko-grecki pracownik firmy Meta był jednocześnie podsłuchiwany przez EYP i namierzany za pomocą oprogramowania szpiegowskiego Predator, którego użycie jest nielegalne w świetle prawa greckiego; mając na uwadze, że według doniesień medialnych posłowie z partii opozycyjnych i rządowych w Grecji, działacze partyjni i dziennikarze rzekomo również byli celem ataków z użyciem oprogramowania szpiegowskiego Predator lub konwencjonalnych podsłuchów prowadzonych przez EYP lub obu tych metod; mając na uwadze, że rząd grecki zaprzecza, jakoby zakupił lub wykorzystywał oprogramowanie Predator, choć jest wysoce prawdopodobne, że program ten był wykorzystywany przez osoby bardzo blisko związane z biurem premiera lub w ich imieniu; mając na uwadze, że rząd grecki przyznał, iż udzielił firmie Intellexa pozwoleń na sprzedaż oprogramowania szpiegowskiego Predator represyjnym rządom takim jak Madagaskar czy Sudan; mając na uwadze, że w reakcji na skandal rząd wprowadził poprawki legislacyjne, które jeszcze bardziej ograniczają prawa zaatakowanych osób do uzyskania informacji po inwigilacji, oraz dalej utrudniają pracę niezależnych organów;

R. mając na uwadze, że – jak wynika z ustaleń – w Hiszpanii istnieją dwie kategorie celów inwigilacji; mając na uwadze, że pierwsza z nich obejmuje premiera i ministra obrony, ministra spraw wewnętrznych i innych wysokich rangą urzędników; mając na uwadze, że druga kategoria jest częścią tego, co organizacja Citizen Lab określa mianem „CatalanGate", i obejmuje 65 inwigilowanych osób, w tym polityków z regionalnego rządu Katalonii, członków prokatalońskiego ruchu niepodległościowego, posłów do Parlamentu Europejskiego, prawników, pracowników

akademickich i podmioty społeczeństwa obywatelskiego; mając na uwadze, że w maju 2022 r. władze hiszpańskie przyznały się do inwigilowania za zgodą sądu 18 osób, choć do tej pory nie ujawniły nakazów ani żadnych innych informacji, i powołują się na bezpieczeństwo narodowe przy składaniu wyjaśnień dotyczących stosowania nadzoru oprogramowania szpiegowskiego służącego inwigilacji w Hiszpanii; mając na uwadze, że 47 innych osób również rzekomo było inwigilowanych, ale nie otrzymało żadnych informacji poza informacjami od Citizen Lab;

S. mając na uwadze, że na Cyprze nie potwierdzono żadnych zarzutów dotyczących infekowania urządzeń oprogramowaniem szpiegowskim; mając na uwadze, że Cypr jest ważnym europejskim ośrodkiem eksportowym branży inwigilacji oraz atrakcyjną lokalizacją dla przedsiębiorstw sprzedających technologie nadzoru;

T. mając na uwadze, że istnieją poważne przesłanki świadczące o tym, że m.in. rządy Maroka i Rwandy inwigilowały za pomocą oprogramowania szpiegowskiego wysoko postawionych obywateli Unii, w tym prezydenta Francji, premiera, minister obrony i ministra spraw wewnętrznych Hiszpanii, ówczesnego premiera Belgii, byłego przewodniczącego Komisji i byłego premiera Włoch, oraz Carine Kanimbę, córkę Paula Rusesabaginy;

U. mając na uwadze, że można bez wątpienia założyć, iż wszystkie państwa członkowskie zakupiły lub stosowały co najmniej jedno oprogramowanie szpiegowskie; mając na uwadze, że choć większość rządów w Unii Europejskiej nie zdecyduje się na bezprawne stosowanie oprogramowania szpiegowskiego, to przy braku solidnych ram prawnych obejmujących zabezpieczenia i nadzór oraz w świetle wyzwań technicznych związanych z wykrywaniem i śledzeniem infekowania urządzeń ryzyko nadużyć jest bardzo prawdopodobne;

V. mając na uwadze, że większość rządów i parlamentów państw członkowskich nie dostarczyła Parlamentowi Europejskiemu istotnych, wykraczających poza powszechną wiedzę, informacji na temat obowiązujących w ich krajach ram prawnych regulujących stosowanie oprogramowania szpiegowskiego, mimo iż są do tego zobowiązane na mocy art. 3 ust. 4 decyzji Parlamentu Europejskiego, Rady i Komisji z dnia 6 marca 1995 r. w sprawie szczegółowych przepisów regulujących egzekwowanie przez Parlament Europejski jego prawa do prowadzenia dochodzeń; mając na uwadze, że trudno jest ocenić egzekwowanie przepisów Unii oraz zabezpieczenia, nadzór i środki dochodzenia roszczeń, a to uniemożliwia odpowiednią ochronę praw podstawowych obywateli;

W. mając na uwadze, że art. 4 ust. 3 TUE stanowi, że „zgodnie z zasadą lojalnej współpracy Unia i państwa członkowskie wzajemnie się szanują i udzielają sobie wzajemnego wsparcia w wykonywaniu zadań wynikających z traktatów”;

X. mając na uwadze, że kilka kluczowych osób z branży oprogramowania szpiegowskiego uzyskało obywatelstwo maltańskie, co ułatwia im prowadzenie działalności w Unii oraz z Unii;

Y. mając na uwadze, że wielu twórców i dostawców oprogramowania szpiegowskiego jest lub było zarejestrowanych w co najmniej jednym państwie członkowskim; mając na uwadze, że przykładami takich dostawców są: NSO Group, która jest obecna w Luksemburgu, na Cyprze, w Holandii i Bułgarii; spółka dominująca firmy Intellexa, Thalestris Limited, w Irlandii, Grecji, Szwajcarii i na Cyprze; DSIRF w Austrii; QuaDream na Cyprze; Amesys i Nexa Technologies we Francji; Tykelab i RCS Lab we Włoszech oraz FinFisher (obecnie nieistniejąca) w Niemczech;

Z. mając na uwadze, że Unia Europejska nie uczestniczy w Porozumieniu z Wassenaar w sprawie kontroli eksportu broni konwencjonalnej oraz towarów i technologii podwójnego zastosowania; mając na uwadze, że wszystkie państwa członkowskie z wyjątkiem Cypru uczestniczą w porozumieniu z Wassenaar, chociaż Cypr złożył wniosek o przystąpienie do niego dawno temu; mając na uwadze, że Cypr jest związany rozporządzeniem w sprawie produktów podwójnego zastosowania;

AA. mając na uwadze, że izraelskie zasady wywozu ([20]) mają zasadniczo zastosowanie do wszystkich obywateli Izraela, nawet jeśli prowadzą oni działalność z terytorium UE; mając na uwadze, że Izrael nie uczestniczy w porozumieniu z Wassenaar, ale twierdzi, że mimo to stosuje jego zapisy;

AB. mając na uwadze, że wywóz oprogramowania szpiegowskiego z Unii do państw trzecich jest uregulowany w rozporządzeniu w sprawie produktów podwójnego zastosowania, które zostało zmienione w 2021 r.; mając na uwadze, że we wrześniu 2022 r. Komisja opublikowała pierwsze sprawozdanie w sprawie jego wykonania ([21]);

AC. mając na uwadze, że niektórzy producenci eksportujący oprogramowanie szpiegowskie do państw trzecich zakładają działalność w Unii, aby zyskać renomę, a jednocześnie handlują oprogramowaniem szpiegowskim z represyjnymi reżimami; mając na uwadze, że ma miejsce wywóz z Unii do represyjnych reżimów lub podmiotów niepaństwowych, co stanowi naruszenie przepisów UE dotyczących wywozu;

AD. mając na uwadze, że Amesys i Nexa Technologies są obecnie ścigane we Francji za wywóz technologii nadzoru do Libii, Egiptu i Arabii Saudyjskiej; mając na uwadze, że firmy Intellexy z siedzibą w Grecji miały eksportować swoje produkty do Bangladeszu, Sudanu, na Madagaskar i co najmniej do jednego kraju arabskiego; mając na uwadze, że

([20]) Ustawa o kontroli wywozu w obszarze obronności 5766-2007, Ministerstwo Obrony Izraela.
([21]) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223.

oprogramowanie FinFisher jest wykorzystywane w kilkudziesięciu krajach na całym świecie, w tym w Angoli, Arabii Saudyjskiej, Bahrajnie, Bangladeszu, Egipcie, Etiopii, Gabonie, Jordanii, Katarze, Kazachstanie, Mjanmie, Omanie i Turcji oraz że Amnesty International i Forbidden Stories oskarżają służby wywiadowcze Maroka o stosowanie oprogramowania szpiegowskiego Pegasus przeciwko dziennikarzom, obrońcom praw człowieka, społeczeństwu obywatelskiemu i politykom; mając na uwadze, że nie wiadomo, czy zostały udzielone pozwolenia na wywóz oprogramowania szpiegowskiego do wszystkich tych krajów; mając na uwadze, że prokuratura w Monachium postawiła byłym dyrektorom FinFisher zarzut eksportu technologii nadzoru do Turcji bez zezwolenia;

AE. mając na uwadze, że liczba uczestników targów zbrojeniowych i ISSWorld wprowadzających do obrotu rozwiązania z zakresu oprogramowania szpiegowskiego wskazuje na przewagę dostawców oprogramowania szpiegowskiego oraz powiązanych produktów i usług z państw trzecich (przy czym znaczna liczba tych dostawców ma siedzibę w Izraelu, np. NSO Group, Wintego, Quadream i Cellebrite), a także na znaczenie producentów z Indii (ClearTrail), Zjednoczonego Królestwa (BAe Systems i Black Cube) i Zjednoczonych Emiratów Arabskich (DarkMatter), a amerykańska Entity List, czyli czarna lista m.in. producentów oprogramowania szpiegowskiego z siedzibą w Izraelu (NSO Group i Candiru), Rosji (Positive Technologies) i Singapurze (Computer Security Initiative Consultancy PTE LTD.) dodatkowo uwidacznia różnorodność pochodzenia producentów oprogramowania szpiegowskiego; mając na uwadze, że w targach tych uczestniczy również wiele europejskich organów publicznych, w tym krajowe siły policyjne;

AF. mając na uwadze, że art. 4 ust. 2 TUE stanowi, że bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego;

AG. mając jednak na uwadze, że zgodnie z wyrokiem TSUE (sprawa C-623/17) „mimo iż to do państw członkowskich należy określenie ich podstawowych interesów bezpieczeństwa i podjęcie środków zmierzających do zagwarantowania bezpieczeństwa zewnętrznego i wewnętrznego, sam tylko fakt, że środek krajowy został podjęty w celu ochrony bezpieczeństwa narodowego, nie może powodować niemożności stosowania prawa Unii i zwolnienia państw członkowskich z konieczności przestrzegania tego prawa";

AH. mając na uwadze, że zgodnie z wyrokiem TSUE (sprawa C-203/15) „[a]rtykuł 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa dotycząca prywatności i łączności elektronicznej), zmienionej dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r., w związku z art. 7, 8, 11 i art. 52 ust. 1 Karty, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu przewidującemu do celów zwalczania przestępczości uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej";

AI. mając na uwadze, że zgodnie z wyrokiem TSUE (sprawa C-203/15) „[a]rtykuł 15 ust. 1 dyrektywy 2002/58/WE, po zmianach wprowadzonych dyrektywą 2009/136/WE, w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty należy interpretować w ten sposób, że stoi on na przeszkodzie obowiązywaniu uregulowań krajowych dotyczących ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a w szczególności dostępu właściwych organów władz krajowych do przechowywanych danych, które to przepisy, w ramach zwalczania przestępczości, nie ograniczają tego dostępu jedynie do celów walki z poważną przestępczością, nie uzależniają przyznania go od uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny i nie ustanawiają wymogu, aby dane te były przechowywane na obszarze Unii";

AJ. mając na uwadze, że z orzecznictwa Europejskiego Trybunału Praw Człowieka jasno wynika, że wszelka inwigilacja musi odbywać się zgodnie z prawem, służyć uzasadnionemu celowi oraz być konieczna i proporcjonalna; mając na uwadze ponadto, że ramy prawne muszą zapewniać precyzyjne, skuteczne i kompleksowe zabezpieczenia dotyczące wydawania, wykonywania i potencjalnych możliwości dochodzenia roszczeń w odniesieniu do środków nadzoru, które muszą podlegać odpowiedniej kontroli sądowej i skutecznemu nadzorowi ([22]);

AK. mając na uwadze, że Konwencja Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Konwencja 108), ostatnio zaktualizowana jako Konwencja 108+, ma zastosowanie do przetwarzania danych osobowych do celów bezpieczeństwa państwa (narodowego), w tym obronności; mając na uwadze, że wszystkie państwa członkowskie są stronami tej konwencji;

AL. mając na uwadze, że ważne aspekty stosowania oprogramowania szpiegowskiego do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, wchodzą w zakres prawa UE;

([22]) https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf

AM. mając na uwadze, że w Karcie określono warunki ograniczenia korzystania z praw podstawowych, ograniczenia te muszą być jednak przewidziane ustawą i szanować istotę tych praw i wolności oraz z zastrzeżeniem zasady proporcjonalności mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób; mając na uwadze, że w przypadku stosowania oprogramowania szpiegowskiego stopień ingerencji w prawo do prywatności może być tak duży, że dana osoba jest faktycznie pozbawiona tego prawa, a zastosowanie takiego środka nie zawsze może być uznane za proporcjonalne, niezależnie od tego, czy można uważać ten środek za konieczny do osiągnięcia uzasadnionych celów demokratycznego państwa;

AN. mając na uwadze, że zgodnie z przepisami dyrektywy o e-prywatności państwa członkowskie muszą zapewnić poufność komunikacji; mając na uwadze, że zastosowanie narzędzi nadzoru stanowi ograniczenie prawa do ochrony urządzeń końcowych, zapewnionego w dyrektywie o e-prywatności; mając na uwadze, że takie ograniczenia spowodowałyby włączenie krajowych przepisów dotyczących oprogramowania szpiegowskiego w zakres dyrektywy o e-prywatności, podobnie jak w przypadku krajowych przepisów dotyczących zatrzymywania danych; mając na uwadze, że częste stosowanie inwazyjnej technologii szpiegowskiej nie byłoby zgodne z porządkiem prawnym Unii;

AO. mając na uwadze, że zgodnie z prawem międzynarodowym państwo ma prawo do prowadzenia dochodzeń w sprawie potencjalnych przestępstw jedynie w obrębie swojej jurysdykcji i musi korzystać z pomocy innych państw, jeżeli dochodzenie musi być prowadzone w innych państwach, chyba że istnieje podstawa do prowadzenia dochodzenia w innej jurysdykcji na mocy umowy międzynarodowej lub, w przypadku państw członkowskich, prawa unijnego;

AP. mając na uwadze, że zainfekowanie urządzenia oprogramowaniem szpiegowskim, a następnie gromadzenie danych odbywa się za pośrednictwem serwerów dostawców usług telefonii komórkowej; mając na uwadze, że bezpłatny roaming w Unii spowodował, że ludzie czasami mają umowy na telefony komórkowe w innych państwach członkowskich niż państwo, w którym mieszkają, a w prawie Unii nie ma obecnie podstawy prawnej do gromadzenia danych w innym państwie członkowskim przez stosowanie oprogramowania szpiegowskiego;

AQ. mając na uwadze, że David Kaye, były specjalny sprawozdawca ONZ ds. promowania i ochrony prawa do wolności wypowiedzi ([23]) oraz Irene Khan, obecna specjalna sprawozdawczyni ONZ ds. promowania i ochrony prawa do wolności wypowiedzi ([24]) wezwali do natychmiastowego moratorium na stosowanie, przekazywanie i sprzedaż narzędzi nadzoru do czasu wprowadzenia rygorystycznych zabezpieczeń praw człowieka w celu uregulowania praktyk i zagwarantowania, że rządy i podmioty niepaństwowe będą korzystać z tych narzędzi w sposób zgodny z prawem;

AR. mając na uwadze, że istnieją przypadki, w których firmy zajmujące się oprogramowaniem szpiegowskim, w szczególności Intellexa, sprzedawały nie tylko samą technologię przechwytywania i ekstrakcji, ale także całą usługę, określaną również jako „hakowanie jako usługa" lub „aktywny cyberwywiad", oferując pakiet metod inwigilacji i technologii przechwytywania, a także szkolenia dla personelu oraz wsparcie techniczne, operacyjne i metodologiczne; mając na uwadze, że usługa ta może pozwolić przedsiębiorstwu kontrolować całą operację nadzoru i agregować dane z nadzoru; mając na uwadze, że praktyka ta jest prawie niemożliwa do nadzorowania i kontrolowania przez odpowiednie władze; mając na uwadze, że utrudnia to przestrzeganie zasad proporcjonalności, konieczności, legalności, legalizmu i adekwatności; mając na uwadze, że usługa ta nie jest dozwolona przez izraelską Agencję Kontroli Eksportu Wojskowego (DECA); mając na uwadze, że Cypr wykorzystano do obejścia istniejących ograniczeń wynikających z prawa izraelskiego w celu świadczenia „hakowania jako usługi";

AS. mając na uwadze, że państwa członkowskie muszą przestrzegać dyrektywy 2014/24/UE i dyrektywy 2009/81/WE, odpowiednio w sprawie zamówień publicznych i zamówień w dziedzinie obronności; mając na uwadze, że państwa członkowskie muszą właściwie uzasadnić odstępstwa na podstawie art. 346 ust. 1 lit. b) TFUE, ponieważ dyrektywa 2009/81/WE wyraźnie uwzględnia newralgiczne cechy zamówień publicznych w dziedzinie obronności, oraz przestrzegać Porozumienia WTO w sprawie zamówień rządowych ze zmianami z 30 marca 2012 r. ([25]), jeżeli są jego stroną;

AT. mając na uwadze, że EIOD podkreślił, iż państwa członkowskie muszą przestrzegać europejskiej konwencji praw człowieka oraz orzecznictwa ETPC, który wyznacza granice działań inwigilacyjnych na rzecz bezpieczeństwa narodowego; mając ponadto na uwadze, że nadzór wykorzystywany do celów egzekwowania prawa musi być zgodny z prawem UE, w szczególności z Kartą i dyrektywami UE, takimi jak dyrektywa o e-prywatności i dyrektywa w sprawie egzekwowania prawa;

([23]) „Nadzór a prawa człowieka" sprawozdanie specjalnego sprawozdawcy ds. promocji i ochrony prawa do wolności wyrażania opinii oraz wolności wypowiedzi, A/HRC/41/35, 2019.

([24]) Biuro Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka, „Skandal związany z oprogramowaniem szpiegowskim: eksperci ONZ apelują o moratorium na sprzedaż „zagrażających życiu" technologii inwigilacji.

([25]) https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm.

AU. mając na uwadze, że według doniesień duże instytucje finansowe próbowały nakłaniać producentów oprogramowania szpiegowskiego, aby nie stosowali odpowiednich standardów w zakresie praw człowieka ani należytej staranności oraz by kontynuowali sprzedaż oprogramowania szpiegowskiego represyjnym reżimom;

AV. mając na uwadze, że w programie „Horyzont 2020" Izrael zajmuje trzecie miejsce wśród państw stowarzyszonych pod względem ogólnego udziału w programie; mając na uwadze, że całkowity budżet umowy w sprawie programu „Horyzont Europa" zawartej z Izraelem na lata 2021–2027 wynosi 95,5 mld EUR ([26]); mając na uwadze, że w ramach tych programów europejskich ([27]) udostępniono niektóre fundusze izraelskim przedsiębiorstwom wojskowym i obronnym;

AW. mając na uwadze, że głównym instrumentem ustawodawczym w polityce rozwojowej Unii jest rozporządzenie (UE) 2021/947 ([28]) („rozporządzenie w sprawie globalnego wymiaru Europy"), a unijne finansowanie może być udzielane z wykorzystaniem rodzajów finansowania przewidzianych w rozporządzeniu finansowym; mając na uwadze, że pomoc mogłaby zostać zawieszona w razie pogorszenia się sytuacji w zakresie demokracji, praw człowieka lub praworządności w państwach trzecich;

1. podkreśla niezaprzeczalne znaczenie ochrony prywatności, prawa do godności, życia prywatnego i rodzinnego, wolności wypowiedzi i informacji oraz wolności zgromadzania się i stowarzyszania się, a także prawa do rzetelnego procesu sądowego, w szczególności w coraz bardziej cyfrowym świecie, w którym coraz więcej naszych działań odbywa się w internecie;

2. zajmuje zdecydowane stanowisko, że przypadki naruszania tych podstawowych praw i wolności są kluczowe z punktu widzenia poszanowania wspólnych zasad prawnych określonych w traktatach i innych źródłach oraz zauważa, że zagrożona jest sama demokracja, ponieważ wykorzystywanie oprogramowania szpiegowskiego przez polityków, społeczeństwo obywatelskie i dziennikarzy ma efekt mrożący i poważnie wpływa na prawo do pokojowego zgromadzania się, wolność wypowiedzi i udział społeczeństwa;

3. zdecydowanie potępia stosowanie przez rządy państw członkowskich oraz członków organów rządowych lub instytucji państwowych oprogramowania szpiegowskiego w celu monitorowania, szantażowania, zastraszania, manipulowania i dyskredytowania członków opozycji, krytyków i społeczeństwa obywatelskiego, eliminowania kontroli demokratycznej i wolnej prasy, manipulowania wyborami oraz podważania praworządności poprzez atakowanie sędziów, prokuratorów i prawników w celach politycznych;

4. zwraca uwagę, że takie bezprawne wykorzystywanie oprogramowania szpiegowskiego przez rządy krajowe i rządy państw niebędących członkami UE ma bezpośredni i pośredni wpływ na instytucje unijne i proces decyzyjny, a przez to osłabia integralność demokracji Unii Europejskiej;

5. z dużym zaniepokojeniem zauważa, że obecna struktura zarządzania Unią jest zasadniczo nieadekwatna do tego, by reagować na pochodzące z wewnątrz Unii ataki na demokrację, prawa podstawowe i praworządność oraz brak działań ze strony wielu państw członkowskich; zwraca uwagę, że gdy takie zagrożenia występują w jednym państwie członkowskim, cała Unia jest narażona na ryzyko;

6. podkreśla, że normy cyfrowe regulujące rozwój technologiczny w Unii muszą być zgodne z prawami podstawowymi;

7. zajmuje zdecydowane stanowisko, że wywóz oprogramowania szpiegowskiego z Unii do krajów, w których panuje dyktatura, i represyjnych reżimów o słabej reputacji w zakresie przestrzegania praw człowieka, gdzie narzędzia te wykorzystuje się przeciwko działaczom na rzecz praw człowieka, dziennikarzom i krytykom rządu, stanowi poważne naruszenie praw podstawowych zapisanych w Karcie oraz rażące naruszenie unijnych zasad wywozu;

8. wyraża ponadto zaniepokojenie nielegalnym wykorzystywaniem oprogramowania szpiegowskiego i handlem nim przez inne państwa członkowskie, które wspólnie przekształcają Unię w miejsce przeznaczenia dla branży oprogramowania szpiegowskiego;

9. wyraża zaniepokojenie atakowaniem przez państwa niebędące członkami UE wysoko postawionych osób, obrońców praw człowieka i dziennikarzy w Unii za pomocą oprogramowania szpiegowskiego;

([26]) https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/israel-joins-horizon-europe-research-and-innovation-programme-2021-12-06_en.

([27]) https://webgate.ec.europa.eu/dashboard/extensions/CountryProfile/CountryProfile.html?Country=Israel https://elbitsystems.com/products/comercial-aviation/innovation-rd/.

([28]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/947 z dnia 9 czerwca 2021 r. ustanawiające Instrument Sąsiedztwa oraz Współpracy Międzynarodowej i Rozwojowej – Globalny Wymiar Europy, zmieniające i uchylające decyzję Parlamentu Europejskiego i Rady nr 466/2014/UE oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1601 i rozporządzenie Rady (WE, Euratom) nr 480/2009 (Dz.U. L 209 z 14.6.2021, s. 1).

10. jest również zaniepokojony widoczną powściągliwością w prowadzeniu dochodzeń w sprawie nadużywania oprogramowania szpiegowskiego w przypadkach, w których podejrzanym jest organ rządowy państwa członkowskiego lub organ rządowy państwa niebędącego członkiem UE; zauważa bardzo powolne postępy i brak przejrzystości w postępowaniach sądowych dotyczących nadużywania oprogramowania szpiegowskiego wobec przywódców rządów i ministrów państw członkowskich UE oraz członków Komisji, a także członków społeczeństwa obywatelskiego, dziennikarzy lub przeciwników politycznych;

11. zauważa, że ramy prawne niektórych państw członkowskich nie zapewniają precyzyjnych, skutecznych i kompleksowych zabezpieczeń dotyczących zlecania i wykonywania środków nadzoru oraz potencjalnych mechanizmów dochodzenia roszczeń w odniesieniu do tych środków; zauważa, że takie środki muszą służyć uzasadnionemu celowi oraz być konieczne i proporcjonalne;

12. wyraża ubolewanie wobec faktu, że rządy państw członkowskich, Rada i Komisja nie współpracowały w pełni z komisją śledczą i nie dzieliły się wszystkimi istotnymi i znaczącymi informacjami, aby pomóc komisji śledczej w wypełnianiu jej zadań, zgodnie z jej mandatem; potwierdza, że niektóre z tych informacji mogą podlegać ścisłym wymogom prawnym dotyczącym zachowania tajemnicy i poufności; jest zdania, że zbiorowa odpowiedź Rady jest niewystarczająca i sprzeczna z zasadą lojalnej współpracy przewidzianą w art. 4 ust. 3 TUE;

13. stwierdza, że nie wydaje się, aby ani państwa członkowskie, ani Rada, ani Komisja były w ogóle zainteresowane wzmożeniem starań w celu pełnego zbadania nadużyć związanych ze stosowaniem oprogramowania szpiegowskiego, świadomie chroniąc w ten sposób rządy państw członkowskich Unii, które naruszają prawa człowieka w Unii i poza nią;

14. stwierdza, że w Polsce doszło do poważnego naruszenia prawa Unii i niewłaściwego administrowania w jego wdrażaniu;

15. wzywa Polskę, aby:

a) wezwała Prokuratora Generalnego do wszczęcia dochodzenia w sprawie nadużywania oprogramowania szpiegowskiego;

b) pilnie przywróciła odpowiednie zabezpieczenia instytucjonalne i prawne, w tym skuteczną i wiążącą kontrolę *ex ante* i *ex post* oraz niezależne mechanizmy nadzoru, w tym kontrolę sądową działań w zakresie nadzoru; podkreśla, że w kontekście skutecznej kontroli *ex ante* wniosek do sądu o objęcie danej osoby nadzorem operacyjnym, jak również nakaz sądowy dotyczący objęcia danej osoby takim nadzorem powinny zawierać jasne uzasadnienie i wskazanie środków technicznych, które mają zostać wykorzystane do objęcia danej osoby nadzorem, oraz że w kontekście skutecznej kontroli *ex post* należy ustanowić obowiązek informowania osoby objętej nadzorem o tym fakcie oraz o czasie trwania, zakresie i sposobie przetwarzania danych uzyskanych w ramach takiego nadzoru operacyjnego;

c) wprowadziła spójne przepisy chroniące obywateli niezależnie od tego, czy nadzór operacyjny jest prowadzony przez prokuraturę, tajne służby czy jakikolwiek inny organ państwowy;

d) zastosowała się do orzeczenia Trybunału Konstytucyjnego w sprawie ustawy o Policji z 1990 r.;

e) zastosowała się do opinii Komisji Weneckiej z 2016 r. w sprawie ustawy o Policji;

f) stosowała się do orzecznictwa ETPC, np. do wyroku w sprawie Roman Zacharow przeciwko Rosji z 2015 r., w którym podkreślono konieczność stosowania ścisłych kryteriów nadzoru, właściwych zgód organów sądowych i nadzoru sądowego, natychmiastowego niszczenia nieistotnych danych, kontroli sądowej nad procedurami pilnymi, a także wymóg powiadamiania inwigilowanych osób, jak również do wyroku w sprawie Klass i inni przeciwko Niemcom z 1978 r., w którym podkreślono, że stosowanie inwigilacji musi być na tyle istotne, by uzasadniało konieczność takiego naruszenia prywatności;

g) przestrzegała wszystkich orzeczeń TSUE i ETPC związanych z niezawisłością wymiaru sprawiedliwości i nadrzędnością prawa UE;

h) wycofała art. 168a z przeredagowanej ustawy o zmianie ustawy – Kodeks postępowania karnego z 2016 r.;

i) przywróciła pełną niezależność sądownictwa i szanowała ustawowe uprawnienia wszystkich właściwych organów nadzoru, takich jak Rzecznik Praw Obywatelskich, Prezes Urzędu Ochrony Danych Osobowych i Najwyższa Izba Kontroli, zapewniła wszystkim organom nadzoru pełną współpracę i dostęp do informacji oraz zapewniła wszystkim inwigilowanym osobom pełny dostęp do informacji;

j) pilnie wprowadziła losowy przydział spraw sędziom sądów w odniesieniu do wszystkich składanych wniosków, również w weekend i poza normalnymi godzinami pracy, aby nie dochodziło do wyboru „przyjaznych sędziów" przez tajne służby, oraz zapewniła przejrzystość takiego systemu poprzez m.in. upublicznienie algorytmu, na podstawie którego sędzia jest losowo przydzielany do danej sprawy;

k) przywróciła tradycyjny system nadzoru parlamentarnego, w którym przewodniczącym parlamentarnej Komisji do Spraw Służb Specjalnych (KSS) jest członek partii opozycyjnej;

l) pilne wyjaśniła kwestię niewłaściwego wykorzystywania oprogramowania szpiegowskiego w Polsce, aby nie podawać w wątpliwość uczciwości nadchodzących wyborów;

m) odpowiednio wdrożyła dyrektywę (UE) 2016/680 (dyrektywa o ochronie danych w sprawach karnych) i egzekwowała jej przepisy oraz zapewniła organowi ochrony danych uprawnienia do nadzoru nad przetwarzaniem danych osobowych m.in. przez organy takie jak Centralne Biuro Antykorupcyjne i Agencja Bezpieczeństwa Wewnętrznego;

n) wdrożyła dyrektywę o ochronie sygnalistów;

o) powstrzymała się od przyjmowania w nowych ustawach przepisów dotyczących komunikacji elektronicznej, które są sprzeczne z europejską konwencją praw człowieka (EKPC),

p) zapewniła dostępność skutecznych środków odwoławczych dla obywateli Polski, których dotyczy wdrażanie ustaw sprzecznych z Konstytucją RP i EKPC;

q) zwróciła się do Europolu o zbadanie wszystkich przypadków domniemanego nadużywania oprogramowania szpiegowskiego;

r) zagwarantowała niezależną kontrolę zgodności ustaw z Konstytucją;

s) przywróciła niezależność Prokuratora Generalnego od Ministra Sprawiedliwości, by zagwarantować, że dochodzenia w sprawie domniemanych naruszeń praw podstawowych będą wolne od względów politycznych;

16. wzywa Komisję do oceny zgodności polskiej ustawy z 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości z unijną dyrektywą o ochronie danych w sprawach karnych oraz, w razie potrzeby, do wszczęcia postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego;

17. stwierdza, że na Węgrzech doszło do poważnego naruszenia prawa Unii i niewłaściwego administrowania w jego wdrażaniu;

18. wzywa Węgry, aby:

a) pilnie przywróciły odpowiednie zabezpieczenia instytucjonalne i prawne, w tym skuteczną i wiążącą kontrolę *ex ante* i *ex post* oraz niezależne mechanizmy nadzoru, w tym kontrolę sądową działań w zakresie nadzoru; podkreśla, że w kontekście skutecznej kontroli *ex ante* wniosek do sądu o objęcie danej osoby nadzorem operacyjnym, jak również nakaz sądowy dotyczący objęcia danej osoby takim nadzorem, powinny zawierać jasne uzasadnienie i wskazanie środków technicznych, które mają zostać wykorzystane do objęcia danej osoby nadzorem, oraz że w kontekście skutecznej kontroli *ex post* należy ustanowić obowiązek informowania osoby objętej nadzorem o tym fakcie oraz o czasie trwania, zakresie i sposobie przetwarzania danych uzyskanych w ramach takiego nadzoru operacyjnego;

b) stosowały się do orzecznictwa ETPC, np. do wyroku w sprawie Roman Zacharow przeciwko Rosji z 2015 r., w którym podkreśla się konieczność stosowania ścisłych kryteriów nadzoru, właściwych zgód organów sądowych i nadzoru sądowego, natychmiastowego niszczenia nieistotnych danych, kontroli sądowej nad procedurami pilnymi, a także wymóg powiadamiania inwigilowanych osób, jak również do wyroku w sprawie Klass i inni przeciwko Niemcom z 1978 r., w którym podkreślono, że stosowanie inwigilacji musi być na tyle istotne, by uzasadniało konieczność takiego naruszenia prywatności, oraz określono wymóg powiadamiania podmiotów inwigilowanych;

c) przestrzegały wszystkich orzeczeń TSUE i ETPC związanych z niezawisłością wymiaru sprawiedliwości i nadrzędnością prawa UE;

d) przywróciły niezależne organy nadzoru zgodnie z wyrokiem ETPC w sprawie Hüttl przeciwko Węgrom, w którym stwierdzono, że krajowy organ ds. ochrony danych i swobodnego dostępu do informacji (NAIH) nie jest w stanie prowadzić niezależnego nadzoru nad stosowaniem oprogramowania szpiegowskiego, ponieważ służby specjalne mają prawo odmówić dostępu do niektórych dokumentów ze względu na ich tajność;

e) przywróciły pełną niezależność sądownictwa i wszystkich właściwych organów nadzoru, takich jak Rzecznik Praw Obywatelskich i organy ochrony danych, zapewniły wszystkim organom nadzoru pełną współpracę i dostęp do informacji oraz zapewniły wszystkim osobom inwigilowanym pełny dostęp do informacji;

f) przywróciły niezależnych pracowników na stanowiska kierownicze w organach nadzoru, takich jak Trybunał Konstytucyjny, Sąd Najwyższy, Trybunał Obrachunkowy, prokuratura, Narodowy Bank Węgier i Państwowa Komisja Wyborcza;

g) wdrożyły dyrektywę o ochronie sygnalistów;

h) zwróciły się do Europolu o zbadanie wszystkich przypadków domniemanego nadużywania oprogramowania szpiegowskiego;

i) powstrzymały się od przyjmowania przepisów nowych ustaw dotyczących komunikacji elektronicznej, które są sprzeczne z EKPC;

j) zapewniły dostępność skutecznych środków odwoławczych dla obywateli Węgier, których dotyczy wdrażanie ustaw sprzecznych z Konstytucją Węgier i EKPC;

19. stwierdza, że w Grecji doszło do naruszenia prawa Unii i niewłaściwego administrowania w jego wdrażaniu;

20. wzywa Grecję, aby:

a) pilnie przywróciła i wzmocniła zabezpieczenia instytucjonalne i prawne, w tym skuteczną kontrolę *ex ante* i *ex post* oraz niezależne mechanizmy nadzoru;

b) pilnie uchyliła wszystkie pozwolenia na wywóz, które nie są w pełni zgodne z rozporządzeniem w sprawie produktów podwójnego zastosowania, oraz przeprowadziła dochodzenie w sprawie zarzutów dotyczących nielegalnego wywozu, między innymi do Sudanu;

c) dopilnowała, by właściwe organy mogły swobodnie i bez przeszkód badać wszystkie zarzuty dotyczące stosowania oprogramowania szpiegowskiego;

d) pilnie wycofała wprowadzoną do ustawy 2472/1997 poprawkę 826/145, która zniosła możliwość powiadamiania obywateli przez Grecki Urząd ds. Bezpieczeństwa Komunikacji i Prywatności (ADAE) o uchyleniu poufności komunikacji; zmieniła ustawę 5002/2022 w celu przywrócenia prawa do natychmiastowego poinformowania osoby inwigilowanej, na jej wniosek, niezwłocznie po zakończeniu inwigilacji, a także skorygowała inne przepisy, które osłabiają zabezpieczenia, kontrolę i odpowiedzialność;

e) przywróciła pełną niezależność sądownictwa i wszystkich właściwych organów nadzoru, takich jak Rzecznik Praw Obywatelskich i organy ochrony danych oraz w pełni szanowała niezależność ADAE, zapewniła wszystkim organom kontroli i nadzoru pełną współpracę i dostęp do informacji oraz zapewniła wszystkim osobom inwigilowanym pełny dostęp do informacji;

f) zapewniła, aby ADAE mógł utworzyć archiwum elektroniczne, by móc wykonywać swoje zadania;

g) pilne wyjaśniła sytuację związaną z niewłaściwym wykorzystywaniem oprogramowania szpiegowskiego w Grecji, aby nie podawać w wątpliwość uczciwości nadchodzących wyborów;

h) zniosła nowelizację prawa z 2019 r., na mocy której greckie służby wywiadowcze EYP znalazły się pod bezpośrednią kontrolą premiera; wprowadziła gwarancje konstytucyjne i umożliwiła kontrolę parlamentarną nad jego działaniami, bez pretekstu do poufności informacji;

i) zapewniła niezależność kierownictwa krajowego organu ds. przejrzystości (EAD);

j) zapewniła, aby wymiar sprawiedliwości dysponował wszelkimi niezbędnymi środkami i wsparciem w dochodzeniu policyjnym w związku z domniemanym nadużywaniem oprogramowania szpiegowskiego i zajęła dowody rzeczowe dotyczące pełnomocników, firm brokerskich i dostawców oprogramowania szpiegowskiego, którzy są powiązani z infekowaniem urządzeń oprogramowaniem szpiegowskim;

k) zwróciła się do Europolu o natychmiastowe włączenie się do dochodzenia;

l) powstrzymała się od ingerencji politycznej w pracę Prokuratora Generalnego;

21. stwierdza, że, ogólnie rzecz biorąc, ramy regulacyjne w Hiszpanii są zgodne z wymogami określonymi w traktatach; zwraca jednak uwagę, że potrzebne są pewne reformy, a ich wdrażanie w praktyce musi odbywać się w pełnym poszanowaniu praw podstawowych i zapewniać ochronę udziału społeczeństwa;

22. wzywa zatem Hiszpanię, aby:

a) przeprowadziła pełne, uczciwe i skuteczne dochodzenie, w którym zapewniona zostanie pełna przejrzystość wszystkich domniemanych przypadków użycia oprogramowania szpiegowskiego, w tym 47 przypadków, w odniesieniu do których pozostaje niejasne, czy dane osoby były inwigilowane przez hiszpańską Narodową Agencję Wywiadowczą (CNI) na podstawie nakazu sądowego, czy też inny organ otrzymał nakaz sądowy, aby legalnie je inwigilować, a także w sprawie użycia oprogramowania szpiegowskiego przeciwko premierowi i członkom rządu, oraz aby przedstawiła możliwie najszersze wnioski, zgodnie z obowiązującymi przepisami;

b) zapewniła osobom inwigilowanym odpowiedni dostęp do upoważnienia sądowego wydanego CNI przez Sąd Najwyższy w celu objęcia inwigilacją 18 osób;

c) współpracowała z sądami w celu zapewnienia, aby osoby, wobec których zastosowano oprogramowanie szpiegowskie, miały dostęp do rzeczywistych i skutecznych środków prawnych oraz aby dochodzenia sądowe były zamykane bezzwłocznie w sposób bezstronny i dokładny, na co należy przeznaczyć wystarczające zasoby;

d) rozpoczęła reformę ram prawnych CNI, zgodnie z zapowiedzią z maja 2022 r.;

e) zwróciła się do Europolu, który mógłby wnieść wkład w postaci wiedzy eksperckiej, o włączenie się do dochodzeń;

23. stwierdza, że istnieją dowody niewłaściwego administrowania we wdrażaniu unijnego rozporządzenia w sprawie produktów podwójnego zastosowania na Cyprze, co wymaga ścisłej kontroli;

24. wzywa Cypr do:

a) dokładnej oceny wszystkich pozwoleń na wywóz wydanych na oprogramowanie szpiegowskie i uchylenia ich w stosownych przypadkach;

b) dogłębnej oceny dostarczenia oprogramowania szpiegowskiego w ramach rynku wewnętrznego UE między państwami członkowskimi oraz mapowania poszczególnych izraelskich przedsiębiorstw lub przedsiębiorstw będących własnością i zarządzanych przez obywateli Izraela, które są zarejestrowane na Cyprze i zaangażowane w taką działalność;

c) ujawnienia sprawozdania specjalnego śledczego w sprawie „Spyware Van", o co komisja wnioskowała podczas swojej oficjalnej misji na Cyprze;

d) dogłębnego zbadania, z pomocą Europolu, wszystkich zarzutów dotyczących bezprawnego stosowania oprogramowania szpiegowskiego, zwłaszcza wobec dziennikarzy, prawników, podmiotów społeczeństwa obywatelskiego i obywateli Cypru, oraz jego eksportu;

25. jest zdania, że sytuacja w niektórych innych państwach członkowskich również daje powody do niepokoju, zwłaszcza ze względu na obecność lukratywnej i rozwijającej się branży oprogramowania szpiegowskiego, która korzysta z dobrej reputacji, jednolitego rynku i swobodnego przepływu w Unii, czyniąc z niektórych państw członkowskich, takich jak Cypr i Bułgaria, ośrodki wywozu oprogramowania szpiegowskiego do państw o represyjnych reżimach na całym świecie;

26. jest zdania, że sytuacja, w której niektóre organy krajowe nie zapewniają lub odmawiają zapewnienia obywatelom Unii właściwej ochrony, co obejmuje luki regulacyjne i odpowiednie instrumenty prawne, ewidentnie wskazuje na to, że niezbędne jest działanie na szczeblu Unii w celu zapewnienia poszanowania zapisów traktatów i przepisów Unii z myślą o przestrzeganiu prawa obywateli do życia w bezpiecznym środowisku, w którym szanuje się godność ludzką i życie prywatne oraz chroni się dane osobowe i prawa własności, zgodnie z wymogami dyrektywy 2012/29/UE, według których każda ofiara przestępstwa ma prawo do otrzymania wsparcia i ochrony odpowiednio do indywidualnych potrzeb;

27. stwierdza, że doszło do poważnych niedociągnięć we wdrażaniu prawa Unii, gdy Komisja i Europejska Służba Działań Zewnętrznych (ESDZ) udzieliły wsparcia państwom niebędącym członkami UE, w tym między innymi 10 takim państwom w Sahelu, aby umożliwić im rozwój zdolności w zakresie nadzoru ([29]);

28. przyjmuje stanowisko, że handel oprogramowaniem szpiegowskim i jego stosowanie muszą być ściśle uregulowane; uznaje jednak, że proces legislacyjny może wymagać czasu, natomiast nadużycia muszą zostać natychmiast zaprzestane; wzywa do przyjęcia warunków dotyczących legalnego wykorzystywania, sprzedaży, nabywania i przekazywania oprogramowania szpiegowskiego; nalega, aby w celu dalszego korzystania z oprogramowania szpiegowskiego państwa członkowskie spełniły wszystkie następujące warunki do dnia 31 grudnia 2023 r.:

([29]) Decyzja w sprawie 1904/2021/MHZ, dostępna na stronie internetowej: https://www.ombudsman.europa.eu/en/decision/en/163491.

a) wszystkie przypadki domniemanego nadużycia oprogramowania szpiegowskiego zostaną w pełni zbadane i niezwłocznie rozwiązane przez odpowiednie organy ścigania oraz organy prokuratury i wymiaru sprawiedliwości,

b) udowodnią, że ramy regulujące stosowanie oprogramowania szpiegowskiego są zgodne ze standardami określonymi przez Komisję Wenecką i z odpowiednim orzecznictwem TSUE i ETPC,

c) wyraźnie zobowiążą się do włączenia Europolu na mocy art. 4, 5 i 6 rozporządzenia w sprawie Europolu w dochodzeń w dochodzenia w sprawie zarzutów nielegalnego stosowania oprogramowania szpiegowskiego, oraz

d) zostaną uchylone wszystkie pozwolenia na wywóz, które nie są w pełni zgodne z rozporządzeniem w sprawie produktów podwójnego zastosowania,

29. uważa, że spełnienie powyższych warunków musi zostać ocenione przez Komisję do dnia 30 listopada 2023 r.; uważa ponadto, że wyniki oceny powinny zostać opublikowane w ogólnodostępnym sprawozdaniu;

30. podkreśla, że choć walka z poważną przestępczością i terroryzmem oraz uznanie, że zdolność do tego są niezwykle ważne dla państw członkowskich, ochrona praw podstawowych i demokracji ma zasadnicze znaczenie; zwraca ponadto uwagę, że stosowanie oprogramowania szpiegowskiego przez państwa członkowskie musi być proporcjonalne, nie może być arbitralne, a nadzór może być dozwolony jedynie w ściśle określonych okolicznościach; uważa, że skuteczne mechanizmy *ex ante* zapewniające nadzór sądowy mają kluczowe znaczenie dla ochrony wolności jednostki; potwierdza, że zezwalanie na nieograniczone możliwości nadzoru nie może zagrażać indywidualnym prawom; podkreśla, że ważna jest również zdolność wymiaru sprawiedliwości do sprawowania znaczącego i skutecznego nadzoru *ex post* w dziedzinie wniosków o nadzór nad bezpieczeństwem narodowym, aby zapewnić możliwość kwestionowania nieproporcjonalnego korzystania z oprogramowania szpiegowskiego przez rządy;

31. podkreśla, że stosowanie oprogramowania szpiegowskiego na potrzeby egzekwowania prawa powinno być bezpośrednio regulowane środkami opartymi na tytule 5 rozdział 4 TFUE dotyczącym współpracy wymiarów sprawiedliwości w sprawach karnych; podkreśla, że konfiguracja oprogramowania szpiegowskiego, które jest importowane do UE i w inny sposób wprowadzane do obrotu, powinna być regulowana środkiem opartym na art. 114 TFUE; zwraca uwagę, że stosowanie oprogramowania szpiegowskiego do celów bezpieczeństwa narodowego może być regulowane jedynie pośrednio, na przykład za pomocą praw podstawowych i przepisów dotyczących ochrony danych;

32. uważa, że ze względu na ponadnarodowy i unijny wymiar stosowania oprogramowania szpiegowskiego konieczna jest skoordynowana i przejrzysta kontrola na szczeblu UE, aby zapewnić nie tylko ochronę obywateli UE, ale także ważność dowodów zebranych za pomocą oprogramowania szpiegowskiego w sprawach transgranicznych, oraz że istnieje wyraźna potrzeba opracowania – na podstawie tytułu 5 rozdział 4 TFUE regulującego stosowanie oprogramowania szpiegowskiego przez organy państw członkowskich oraz standardów określonych przez TSUE, ETPC, Komisję Wenecką i Agencję Praw Podstawowych Unii Europejskiej – wspólnych norm UE regulujących stosowanie oprogramowania szpiegowskiego przez organy państw członkowskich ([30]); uważa, że takie normy UE powinny obejmować co najmniej następujące elementy:

a) przewidywane użycie oprogramowania szpiegowskiego powinno być autoryzowane jedynie w wyjątkowych i szczególnych przypadkach w celu ochrony bezpieczeństwa narodowego i musi podlegać konieczności uzyskania skutecznej, wiążącej i znaczącej uprzedniej zgody wydanej przez bezstronny i niezależny organ sądowy lub inny niezależny demokratyczny organ nadzorczy mający dostęp do wszystkich istotnych informacji wskazujących na konieczność i proporcjonalność przewidywanego środka,

b) inwigilacja za pomocą oprogramowania szpiegowskiego powinna trwać nie dłużej, niż jest to absolutnie konieczne, uprzednia zgoda sądu powinna określać dokładny zakres i czas trwania w odniesieniu do każdego zastosowanego urządzenia, a inwigilację można przedłużyć jedynie po uzyskaniu kolejnej zgody organu sądowego na inny określony czas, zważywszy na charakter oprogramowania szpiegowskiego i możliwość inwigilacji wstecznej; organy państw członkowskich powinny ponadto prowadzić działania wyłącznie w odniesieniu do indywidualnych urządzeń lub kont użytkowników końcowych i nie inwigilować dostawców usług internetowych i technologicznych, aby uniknąć inwigilacji użytkowników nieobjętych daną operacją,

c) zgody na wykorzystanie oprogramowania szpiegowskiego można udzielić jedynie w wyjątkowych przypadkach w odniesieniu do dochodzeń w sprawie ograniczonego i zamkniętego wykazu jasno i precyzyjnie zdefiniowanych poważnych przestępstw stanowiących rzeczywiste zagrożenie dla bezpieczeństwa narodowego, a oprogramowanie szpiegowskie można wykorzystywać jedynie wobec osób, co do których istnieją wystarczające przesłanki pozwalające przypuszczać, że popełniły lub planują popełnić takie poważne przestępstwa;

([30]) Agencja Praw Podstawowych Unii Europejskiej, „Inwigilacja prowadzona przez służby wywiadowcze: środki zabezpieczające prawa podstawowe oraz środki prawne dostępne w Unii Europejskiej – część II – streszczenie", 2017, https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu.

d) za pomocą oprogramowania szpiegowskiego nie wolno dążyć do uzyskania danych, które są chronione przywilejami lub immunitetami dotyczącymi kategorii osób (takich jak politycy, lekarze itp.), szczególnie chronionych relacji (takich jak poufność wymiany informacji między prawnikiem a klientem) lub przepisów dotyczących określania i ograniczania odpowiedzialności karnej związanej z wolnością prasy i wolnością wypowiedzi w innych mediach, chyba że istnieją wystarczające powody ustalone pod nadzorem sądowym i potwierdzające udział w działalności przestępczej lub w sprawach związanych z bezpieczeństwem narodowym, które powinny podlegać wspólnym ramom;

e) należy opracować szczegółowe zasady inwigilacji za pomocą technologii szpiegowskiej, ponieważ umożliwia ona nieograniczony wsteczny dostęp do wiadomości, plików i metadanych;

f) państwa członkowskie powinny publikować co najmniej liczbę zatwierdzonych i odrzuconych wniosków o inwigilację, a także rodzaj i cel prowadzonego dochodzenia, oraz anonimowo rejestrować każde dochodzenie w rejestrze krajowym za pomocą niepowtarzalnego identyfikatora, tak aby można było zbadać daną sprawę w przypadku podejrzeń o nadużycie;

g) krajowe organy kontrolne powinny składać sprawozdania państwom członkowskim, a państwa członkowskie powinny następnie regularnie przekazywać te informacje Komisji; Komisja powinna uwzględniać te informacje w rocznych sprawozdaniach na temat praworządności, aby umożliwić porównanie wykorzystania oprogramowania szpiegowskiego w państwach członkowskich;

h) prawo inwigilowanej osoby do uzyskania informacji na temat inwigilacji: po zakończeniu inwigilacji organy powinny powiadomić daną osobę o tym, że była ona celem zastosowanego przez nie oprogramowania szpiegowskiego, w tym podać informacje dotyczące daty i czasu trwania inwigilacji, nakazu wydanego w związku z operacją inwigilacji i uzyskanych danych, informacje o tym, jak i przez jakie podmioty te dane zostały wykorzystane i kiedy zostały usunięte, a także informacje o prawie do administracyjnych i sądowych środków zaskarżenia przed właściwymi organami, jak i o kwestiach praktycznych związanych z korzystaniem z tego prawa; zauważa, że powiadomienie to należy wysłać bez zbędnej zwłoki, chyba że niezależny organ sądowy wyda zgodę na opóźnienie powiadomienia, jeśli natychmiastowe powiadomienie poważnie zagroziłoby celowi prowadzonej inwigilacji;

i) prawo osób nieobjętych inwigilacją, których dane udostępniono, do uzyskania informacji: po upływie okresu, w którym inwigilacja była dozwolona, organy powinny powiadomić osoby, których prawo do prywatności zostało poważnie naruszone w wyniku zastosowania oprogramowania szpiegowskiego, lecz które nie były celem operacji; organy powinny powiadomić tę osobę o tym, że ich dane zostały udostępnione organom, w tym podać informacje dotyczące daty i czasu trwania inwigilacji, nakazu wydanego w związku z operacją inwigilacji i uzyskanych danych, informacje o tym, jak i przez jakie podmioty te dane zostały wykorzystane i kiedy zostały usunięte; zauważa, że powiadomienie to należy wysłać bez zbędnej zwłoki, chyba że niezależny organ sądowy wyda zgodę na opóźnienie powiadomienia, jeśli natychmiastowe powiadomienie poważnie zagroziłoby celowi prowadzonej inwigilacji;

j) skuteczny, wiążący i niezależny nadzór *ex post* nad stosowaniem oprogramowania szpiegowskiego, w przypadku którego odpowiedzialne za nadzór organy muszą posiadać wszelkie wymagane środki i uprawnienia do sprawowania właściwego nadzoru oraz połączony z nadzorem parlamentarnym opartym na ponadpartyjnym członkostwie z odpowiednim upoważnieniem i pełnym dostępie do wystarczających informacji w celu stwierdzenia, że nadzór prowadzono zgodnie z prawem i w sposób proporcjonalny, a także nadzór parlamentarny nad szczególnie chronionymi informacjami poufnymi powinien być ułatwiany za pomocą niezbędnej infrastruktury, procesów i poświadczeń bezpieczeństwa; niezależnie od definicji lub zakresu koncepcji bezpieczeństwa narodowego, krajowe organy nadzoru muszą być właściwe w odniesieniu do pełnego zakresu bezpieczeństwa narodowego;

k) podstawowe zasady sprawiedliwości proceduralnej i nadzoru sądowego muszą mieć kluczowe znaczenie w systemie regulacji dotyczących oprogramowania szpiegowskiego do inwigilacji;

l) znaczący środek odwoławczy dla osób będących bezpośrednim i pośrednim celem inwigilacji, przy czym osoby, które twierdzą, że ucierpiały na skutek inwigilacji, muszą mieć możliwość dochodzenia zadośćuczynienia za pośrednictwem niezależnego organu; wzywa zatem do wprowadzenia obowiązku powiadamiania przez organy państwowe w odpowiednim terminie, przy czym powiadomienie następuje wówczas, gdy minęło już zagrożenie bezpieczeństwa;

m) środki odwoławcze muszą być skuteczne zarówno pod względem prawnym, jak i faktycznym oraz muszą być znane i dostępne; podkreśla, że takie środki wymagają szybkiego, dokładnego i bezstronnego dochodzenia prowadzonego przez niezależny organ nadzoru oraz że organ ten powinien mieć dostęp, a także wiedzę fachową i zdolności techniczne pozwalające na przetwarzanie wszystkich istotnych danych, aby móc stwierdzić, czy ocena bezpieczeństwa dokonana przez władze w odniesieniu do danej osoby jest wiarygodna i proporcjonalna; w przypadkach, w których zweryfikowano nadużycia, zastosowanie powinny mieć odpowiednie sankcje o charakterze karnym albo administracyjnym zgodnie z właściwymi przepisami krajowymi państw członkowskich;

n) poprawa bezpłatnego dostępu inwigilowanych osób do specjalistycznej wiedzy technologicznej na tym etapie, ponieważ większa dostępność i przystępność procesów technologicznych, takich jak analiza kryminalistyczna, umożliwiłaby inwigilowanym osobom przedstawienie silniejszych argumentów w sądzie i poprawiłaby reprezentację inwigilowanych osób w sądzie poprzez budowanie zdolności technologicznych w zakresie reprezentacji prawnej i sądownictwa, aby lepiej doradzać inwigilowanym osobom, identyfikować naruszenia oraz poprawić nadzór i rozliczalność za nadużywanie oprogramowania szpiegowskiego;

o) wzmocnienie prawa do obrony i prawa do rzetelnego procesu sądowego poprzez zapewnienie osobom oskarżonym o przestępstwa możliwości sprawdzenia prawidłowości, autentyczności, wiarygodności, a nawet legalności dowodów przeciwko nim, a tym samym odrzucenie ogólnego stosowania krajowych zasad dotyczących tajemnicy w kwestiach obronnych;

p) w trakcie inwigilacji organy powinny usuwać wszystkie dane nieistotne z punktu widzenia dochodzenia, na które udzielono zgody, a po zakończeniu inwigilacji i dochodzenia, na które udzielono zgody, organy powinny usunąć dane, jak również wszelkie związane z nimi dokumenty, takie jak notatki sporządzone w tym okresie, przy czym takie usunięcie musi zostać odnotowane i należy zapewnić możliwość skontrolowania go;

q) istotne informacje uzyskiwane za pomocą oprogramowania szpiegowskiego powinny być dostępne wyłącznie dla upoważnionych organów i wyłącznie do celów operacji; dostęp ten powinien być ograniczony do konkretnego okresu określonego w postępowaniu sądowym;

r) należy ustanowić minimalne standardy w odniesieniu do praw osób fizycznych w postępowaniu karnym, dotyczące dopuszczalności dowodów zgromadzonych za pomocą oprogramowania szpiegowskiego; w prawie karnym procesowym należy uwzględnić możliwość pojawienia się fałszywych lub zmanipulowanych informacji powstałych w wyniku zastosowania oprogramowania szpiegowskiego (posługiwanie się dokumentem stwierdzającym tożsamość innej osoby);

s) państwa członkowskie muszą się wzajemnie powiadamiać o inwigilacji obywateli lub mieszkańców innego państwa członkowskiego lub numeru telefonu komórkowego posiadacza w innym państwie członkowskim;

t) do oprogramowania służącego do nadzoru należy włączyć marker, tak aby organy nadzoru mogły jednoznacznie zidentyfikować podmiot wdrażający w przypadku podejrzenia o nadużycie; obowiązkowy podpis w przypadku każdego zastosowania oprogramowania szpiegowskiego powinien obejmować indywidualne oznaczenie działającego organu, rodzaj stosowanego oprogramowania szpiegowskiego oraz zanonimizowany numer sprawy;

33. wzywa państwa członkowskie do przeprowadzenia konsultacji publicznych z zainteresowanymi stronami, zapewnienia przejrzystości procesu legislacyjnego oraz uwzględnienia norm i zabezpieczeń UE przy opracowywaniu nowych przepisów dotyczących stosowania i sprzedaży oprogramowania szpiegowskiego;

34. podkreśla, że tylko oprogramowanie szpiegowskie, które jest zaprojektowane w taki sposób, by umożliwiać i ułatwiać funkcjonowanie oprogramowania szpiegowskiego zgodnie z ramami prawnymi określonymi w ust. 32 może być wprowadzane na rynek wewnętrzny, opracowywane lub wykorzystywane w Unii; potwierdza, że rozporządzenie dotyczące wprowadzania do obrotu oprogramowania szpiegowskiego zakładające uwzględnienie kwestii praworządności w fazie projektowania na podstawie art. 114 TFUE powinno zapewnić obywatelom Unii wyższy poziom ochrony; uważa za nieuzasadnione, że podczas gdy rozporządzenie w sprawie podwójnego zastosowania zapewnia obywatelom państw trzecich ochronę przed oprogramowaniem szpiegowskim eksportowanym z UE od 2021 r., obywatelom Unii nie zapewnia się równoważnej ochrony;

35. uważa, że jedynie sama technologia przechwytywania i ekstrakcji może być sprzedawana przez przedsiębiorstwa w UE i nabywana przez państwa członkowskie, a nie „hakowanie jako usługi", które obejmuje dostarczanie technicznego, operacyjnego i metodologicznego wsparcia technologii nadzoru i umożliwia dostawcy dostęp do nieproporcjonalnej ilości danych, co jest niezgodne z zasadami proporcjonalności, konieczności, legalności, zgodności z prawem i adekwatności; wzywa Komisję do przedstawienia wniosku ustawodawczego w tej sprawie;

36. podkreśla, że oprogramowanie szpiegowskie może być wprowadzane do obrotu wyłącznie po to, by mogło być zakupione i wykorzystane przez organy publiczne – według zamkniętej listy – których instrukcje obejmują dochodzenia w sprawie przestępstw lub ochronę bezpieczeństwa narodowego, w przypadku których można wydać zgodę na użycie oprogramowania szpiegowskiego; uważa, że agencja bezpieczeństwa powinny wykorzystywać oprogramowanie szpiegowskie jedynie wtedy, gdy wdrożyły wszystkie zalecenia Agencji Praw Podstawowych Unii Europejskiej ([31]);

37. podkreśla obowiązek stosowania takiej wersji oprogramowania szpiegowskiego zaprojektowanego w sposób, który minimalizuje dostęp do wszystkich danych przechowywanych na urządzeniu, lecz powinno być zaprojektowane w sposób, który ogranicza dostęp do danych do bezwzględnie koniecznego minimum dla celów dochodzenia, na które wydano zgodę;

38. stwierdza, że w przypadku zakupu przez państwo członkowskie oprogramowania szpiegowskiego, zakup ten musi być możliwy do skontrolowania przez niezależny i bezstronny organ kontrolny mający odpowiednie upoważnienie;

([31]) https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_en.pdf.

39. podkreśla, że podkreśla, że wszystkie podmioty wprowadzające oprogramowanie szpiegowskie na rynek wewnętrzny powinny przestrzegać rygorystycznych wymogów w zakresie należytej staranności, a przedsiębiorstwa ubiegające się o status dostawców w ramach procedury udzielania zamówień publicznych powinny przejść proces weryfikacji obejmujący reakcję przedsiębiorstwa na naruszenia praw człowieka popełnione za pomocą jego oprogramowania oraz to, czy na potrzeby danej technologii wykorzystuje się dane zgromadzone w wyniku niedemokratycznych i stanowiących nadużycie praktyk nadzoru; podkreśla, że właściwe krajowe organy nadzoru powinny składać Komisji coroczne sprawozdania dotyczące zgodności;

40. podkreśla, że przedsiębiorstwa oferujące technologie lub usługi nadzoru podmiotom państwowym powinny ujawniać właściwym krajowym organom nadzoru charakter pozwoleń na wywóz;

41. podkreśla, że państwa członkowskie powinny ustanowić okres karencji, aby tymczasowo uniemożliwić pracę byłych pracowników organów lub agencji rządowych dla firm zajmujących się oprogramowaniem szpiegowskim;

Potrzeba określenia granic bezpieczeństwa narodowego

42. jest zaniepokojony przypadkami nieuzasadnionego powoływania się na „bezpieczeństwo narodowe" w celu uzasadnienia rozmieszczenia i stosowania oprogramowania szpiegowskiego oraz zapewnienia absolutnej tajemnicy i brak odpowiedzialności; z zadowoleniem przyjmuje oświadczenie Komisji – zgodne z orzecznictwem TSUE ([32]) – w którym stwierdziła, że samo odniesienie do bezpieczeństwa narodowego nie może być interpretowane jako nieograniczone odstępstwo od stosowania prawa UE i powinno wymagać jasnego uzasadnienia, oraz wzywa Komisję do podjęcia działań w następstwie tego oświadczenia w przypadkach wskazujących na nadużycia; uważa, że w demokratycznym i przejrzystym społeczeństwie, które przestrzega zasad praworządności, takie ograniczenia w imię bezpieczeństwa narodowego będą raczej wyjątkiem niż regułą;

43. Uważa, że pojęcie bezpieczeństwa narodowego musi być przeciwstawiane bardziej ograniczonemu zakresowi w odniesieniu do bezpieczeństwa wewnętrznego, które ma szerszy zakres i obejmuje zapobieganie zagrożeniom dla obywateli, a w szczególności egzekwowanie prawa karnego;

44. wyraża ubolewanie z powodu trudności wynikających z braku wspólnej prawnej definicji bezpieczeństwa narodowego, określającej kryteria pozwalające ustalić, jaki system prawny może mieć zastosowanie w sprawach bezpieczeństwa narodowego, a także do wyraźnego rozgraniczenia obszaru, na którym taki specjalny system może mieć zastosowanie;

45. uważa, że użycie oprogramowania szpiegowskiego stanowi ograniczenie praw podstawowych; uważa ponadto, że w przypadku gdy pojęcia używa się w kontekście prawnym, co pociąga za sobą przeniesienie praw i nałożenie obowiązków (a w szczególności ograniczenia praw podstawowych osób fizycznych), pojęcie to musi być jasne i przewidywalne dla wszystkich osób, których dotyczy; przypomina, że Karta przewiduje, iż wszelkie ograniczenia praw podstawowych zgodnie z art. 52 ust. 1 muszą być zapisane w prawie; uważa zatem, że konieczne jest jasne zdefiniowanie pojęcia „bezpieczeństwo narodowe"; podkreśla, że niezależnie od precyzyjnego wyznaczenia zakresu, dziedzinę bezpieczeństwa narodowego należy objąć w całości niezależnym, wiążącym i skutecznym nadzorem;

46. podkreśla, że jeżeli organy powołują się na względy bezpieczeństwa narodowego jako uzasadnienie korzystania z oprogramowania szpiegowskiego, powinny one, oprócz ram określonych w ust. 29, wykazać zgodność z prawem UE, w tym przestrzeganie zasad proporcjonalności, konieczności, legitymacji, legalności i adekwatności; podkreśla, że uzasadnienie powinno być łatwo dostępne i udostępniane krajowemu organowi kontrolnemu do oceny;

47. przypomina w tym kontekście, że wszystkie państwa członkowskie podpisały konwencję 108+, która określa normy i obowiązki w zakresie ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych, w tym do celów bezpieczeństwa narodowego; zwraca uwagę, że konwencja 108+ stanowi wiążące ramy europejskie dotyczące przetwarzania danych przez służby wywiadu i służby bezpieczeństwa; wzywa wszystkie państwa członkowskie do bezzwłocznej ratyfikacji tej konwencji, do wdrożenia jej norm do prawa krajowego i podjęcia odpowiednich działań w zakresie bezpieczeństwa narodowego;

([32]) Wyrok z dnia 6 października 2020 r., sprawa C-623/17, Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs i in., ECLI.EU:C:2020:790, pkt 44 oraz wyroki z dnia 6 października 2020 r., sprawy połączone C-511/18, C-512/18 i C-520/18, La Quadrature du Net i in. przeciwko Premier ministre i in., ECLI.EU:C:2020:791, pkt 99: „[…] sam tylko fakt, że środek krajowy został podjęty w celu ochrony bezpieczeństwa narodowego, nie może powodować niemożności stosowania prawa Unii i zwolnienia państw członkowskich z konieczności przestrzegania tego prawa".

48. podkreśla, że wyjątki i ograniczenia od ograniczonej liczby postanowień konwencji są dopuszczalne tylko wtedy, gdy są zgodne z wymogami, o których mowa w art. 11 konwencji, co oznacza, że przy wdrażaniu konwencji 108+ każdy wyjątek i ograniczenie muszą być przewidziane ustawą, muszą respektować istotę podstawowych praw i wolności oraz muszą uzasadniać, że „stanowią niezbędny i proporcjonalny środek w społeczeństwie demokratycznym" w odniesieniu do jednej z uzasadnionych podstaw wymienionych w art. 11 ([33]) oraz że takie wyjątki i ograniczenia nie mogą kolidować z „niezależnym i skutecznym przeglądem i nadzorem na mocy ustawodawstwa krajowego danej Strony";

49. zauważa ponadto, że w konwencji 108+ podkreślono, że nadzór „ma uprawnienia do prowadzenia dochodzeń i podejmowania interwencji"; uważa, że skuteczny przegląd i nadzór oznacza wiążące uprawnienia tam, gdzie wpływ na prawa podstawowe jest największy, w szczególności na etapach dostępu, analizy i przechowywania procesu przetwarzania danych osobowych;

50. uważa, że brak wiążących uprawnień organów nadzoru w ramach dziedziny bezpieczeństwa narodowego jest niezgodny z kryterium określonym w konwencji 108+, zgodnie z którym w demokratycznym społeczeństwie stanowi to niezbędny i proporcjonalny środek;

51. zwraca uwagę, że w konwencji 108+ przewidziano bardzo ograniczoną liczbę wyjątków w odniesieniu do jej art. 15, ale nie dopuszcza się takich wyjątków, w szczególności w odniesieniu do ust. 2 [obowiązki w zakresie zwiększania świadomości], ust. 3 [konsultacje w sprawie środków ustawodawczych i administracyjnych], ust. 4 [wnioski i skargi od obywateli], ust. 5 [niezależność i bezstronność], ust. 6 [niezbędne zasoby umożliwiające skuteczną realizację zadań], ust. 7 [sprawozdawczość okresowa], ust. 8 [poufność], ust. 9 [możliwość wniesienia środka zaskarżenia] oraz ust. 10 [brak uprawnień dotyczących organów podczas sprawowania przez nie wymiaru sprawiedliwości];

Lepsze wdrażanie i egzekwowanie obowiązującego prawa

52. zwraca uwagę na braki w krajowych ramach prawnych oraz konieczność lepszego egzekwowania obowiązujących przepisów unijnych w celu przeciwdziałania tym brakom; wskazuje następujące przepisy unijne jako istotne, ale zbyt często niewłaściwie wdrażane lub egzekwowane: dyrektywa w sprawie przeciwdziałania praniu pieniędzy, dyrektywa o ochronie danych w sprawach karnych, zasady udzielania zamówień publicznych, rozporządzenie w sprawie produktów podwójnego zastosowania, orzecznictwo (orzeczenia w sprawie inwigilacji i bezpieczeństwa narodowego) oraz dyrektywa o ochronie sygnalistów; wzywa Komisję, by zbadała niedociągnięcia we wdrażaniu i egzekwowaniu oraz przygotowała sprawozdanie w tej sprawie, a najpóźniej do 1 sierpnia 2023 r. przedstawiła plan działania na rzecz wyeliminowania tych niedociągnięć;

53. uważa, że właściwie wdrożenie i ścisłe egzekwowanie unijnych ram prawnych w zakresie ochrony danych, w szczególności dyrektywy o ochronie danych w sprawach karnych, ogólnego rozporządzenia o ochronie danych i dyrektywy o e-prywatności, mają zasadnicze znaczenie; uważa, że równie ważne jest pełne wdrożenie odpowiednich orzeczeń TSUE – czego nadal brakuje w kilku państwach członkowskich; przypomina, że Komisja odgrywa główną rolę w egzekwowaniu prawa UE i zapewnianiu jego jednolitego stosowania w całej Unii oraz powinna korzystać z wszystkich dostępnych narzędzi, w tym z postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego w przypadkach uporczywego nieprzestrzegania prawa;

54. apeluje, aby porozumienie z Wassenaar stało się wiążące dla wszystkich jego uczestników z myślą o uczynieniu z niego międzynarodowego traktatu;

55. wzywa do tego, aby Cypr i Izrael stały się państwami uczestniczącymi w porozumieniu z Wassenaar; przypomina państwom członkowskim, że należy dołożyć wszelkich starań, aby umożliwić Cyprowi i Izraelowi przystąpienie do porozumienia z Wassenaar;

56. podkreśla, że porozumienie z Wassenaar powinno obejmować ramy w zakresie praw człowieka, zawierające postanowienia dotyczące pozwoleń na technologie szpiegowskie oraz zapewniające ocenę i monitorowanie przestrzegania przepisów przez firmy produkujące technologie szpiegowskie, oraz zwraca uwagę, że państwa uczestniczące powinny zakazać zakupu technologii nadzoru od państw, które nie uczestniczą w tym porozumieniu;

57. podkreśla, że w świetle ustaleń na temat oprogramowania szpiegowskiego Komisja i państwa członkowskie powinny zbadać szczegółowo pozwolenia na wywóz udzielone – na mocy rozporządzenia w sprawie produktów podwójnego zastosowania – na potrzeby korzystania z oprogramowania szpiegowskiego, a Komisja powinna udostępnić wyniki tej oceny Parlamentowi;

([33]) Ocenę tą przewidziano w orzecznictwie Europejskiego Trybunału Praw Człowieka, które nakłada ciężar dowodu na państwo/prawodawcę. Odpowiednie orzecznictwo Europejskiego Trybunału Praw Człowieka obejmuje: Roman Zacharow przeciwko Rosji (skarga nr 47143/06), 4 grudnia 2015 r.; Szabó i Vissy przeciwko Węgrom (skarga nr 37138/14), 12 stycznia 2016 r.; Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu (skargi nr 58170/13, 62322/14 i 24969/15), 25 maja 2021 r. i Centrum För rättvisa przeciwko Szwecji (skarga nr 35252/08), 25 maja 2021 r.

58. podkreśla potrzebę identyfikowalności i rozliczalności wywozu oprogramowania szpiegowskiego i przypomina, że przedsiębiorstwa z UE powinny mieć możliwość wywozu oprogramowania szpiegowskiego tylko, jeżeli ma ono wystarczające właściwości w zakresie identyfikowalności, aby zawsze można było przypisać odpowiedzialność;

59. podkreśla, że Komisja musi regularnie sprawdzać i odpowiednio egzekwować przekształcone rozporządzenie w sprawie produktów podwójnego zastosowania, aby uniknąć wybierania bardziej korzystnego systemu wywozu w całej Unii, co ma obecnie miejsce w Bułgarii i na Cyprze, oraz zwraca uwagę, że Komisja powinna dysponować odpowiednimi zasobami do realizacji tego zadania;

60. zwraca się do Komisji o zapewnienie wystarczającego zasobu kadrowego jednostek odpowiedzialnych za nadzór nad rozporządzeniem w sprawie produktów podwójnego zastosowania i egzekwowanie jego przepisów;

61. wzywa do wprowadzenia zmian do rozporządzenia w sprawie produktów podwójnego zastosowania w celu wyjaśnienia w art. 15, że nie wolno wydawać pozwoleń na wywóz towarów podwójnego zastosowania, jeżeli towary są lub mogą być wykorzystywane do stosowania represji wewnętrznych lub do działań stanowiących poważne naruszenie praw człowieka i międzynarodowego prawa humanitarnego; wzywa do pełnego wdrożenia kontroli praw człowieka i należytej staranności w procesie wydawania pozwoleń, a także do dalszych usprawnień, takich jak środki ochrony prawnej dla ofiar naruszeń praw człowieka i przejrzyste zgłaszanie przeprowadzonych działań w zakresie należytej staranności;

62. wzywa do wprowadzenia zmian do rozporządzenia w sprawie produktów podwójnego zastosowania w celu zapewnienia zakazu tranzytu w sytuacji, gdy towary są lub mogą być wykorzystywane do stosowania represji wewnętrznych lub do działań stanowiących poważne naruszenie praw człowieka i międzynarodowego prawa humanitarnego;

63. podkreśla, że – zgodnie z przyszłą zmianą rozporządzenia w sprawie produktów podwójnego zastosowania – wyznaczone organy krajowe odpowiedzialne za zatwierdzanie i odmowę udzielenia pozwoleń na wywóz produktów podwójnego zastosowania powinny dostarczać szczegółowe sprawozdania zawierające: informacje na temat danego produktu podwójnego zastosowania; liczbę pozwoleń, o które wnioskowano; nazwę kraju wywozu; opis przedsiębiorstwa wywożącego oraz informację, czy przedsiębiorstwo to jest jednostką zależną; opis użytkownika końcowego i miejsca przeznaczenia; wartość pozwolenia na wywóz oraz informację na temat tego, dlaczego pozwolenie na wywóz zostało zatwierdzone lub odmówiono jego udzielenia; podkreśla, że sprawozdania te powinny być co kwartał podawane do wiadomości publicznej; wzywa do utworzenia specjalnej stałej komisji parlamentarnej mającej dostęp do informacji niejawnych Komisji w celu sprawowania nadzoru parlamentarnego;

64. podkreśla, że w ramach przyszłej zmiany rozporządzenia w sprawie produktów podwójnego zastosowania należy znieść wyjątek od wymogu przekazywania informacji Komisji ze względu na szczególną ochronę informacji handlowych, politykę obronną i zagraniczną lub bezpieczeństwo narodowe; uważa natomiast, że aby zapobiec udostępnianiu informacji szczególnie chronionych państwom trzecim, Komisja może podjąć decyzję o utajnieniu niektórych informacji w swoim sprawozdaniu rocznym;

65. podkreśla, że znajdująca się w przekształconym rozporządzeniu w sprawie produktów podwójnego zastosowania definicja produktów służących do cyberinwigilacji nie może być interpretowana w sposób zawężający, lecz powinna obejmować wszystkie technologie w tej dziedzinie, takie jak urządzenia przechwytujące lub zakłócające telekomunikację mobilną; złośliwe oprogramowanie; systemy lub urządzenia do nadzorowania komunikacji w sieci z wykorzystaniem protokołu IP; oprogramowanie specjalnie zaprojektowane lub zmodyfikowane do celów monitorowania lub analizy przez organy ścigania; laserowe urządzenia do detekcji akustycznej; narzędzia kryminalistyczne, które pobierają surowe dane z urządzenia obliczeniowego lub komunikacyjnego i obchodzą mechanizmy kontroli „uwierzytelniania" lub upoważnienia urządzenia; systemy lub urządzenia elektroniczne zaprojektowane do nadzoru i monitorowania widma fal elektromagnetycznych do celów wywiadu wojskowego albo bezpieczeństwa; oraz bezzałogowe statki powietrzne zdolne do prowadzenia nadzoru;

66. wzywa do przyjęcia na szczeblu unijnym dodatkowych przepisów, które wymagałyby od przedsiębiorstw produkujących lub wywożących technologie nadzoru uwzględnienia ram w zakresie praw człowieka i należytej staranności zgodnie z Wytycznymi ONZ dotyczącymi biznesu i praw człowieka;

Współpraca międzynarodowa w celu ochrony obywateli

67. Wzywa do opracowania wspólnej strategii UE-USA w zakresie oprogramowania szpiegowskiego, w tym wspólnej białej lub czarnej listy dostawców oprogramowania szpiegowskiego, których narzędzi nadużywały zagraniczne rządy o niskim poziomie praw człowieka lub istnieje ryzyko takiego nadużycia, aby w złej wierze ukierunkować działania na urzędników państwowych, dziennikarzy i społeczeństwo obywatelskie, i którzy działają wbrew bezpieczeństwu i polityce zagranicznej Unii i którzy (nie) są upoważnieni do jego sprzedaży organom publicznym, do ustalenia wspólnych kryteriów dla dostawców, którzy mają być umieszczeni na którejkolwiek z tych list, do opracowania ustaleń dotyczących wspólnych sprawozdań UE-USA na temat tej branży, do wprowadzenia wspólnej kontroli, wspólnych obowiązków w zakresie należytej staranności dla dostawców oraz do kryminalizacji sprzedaży oprogramowania szpiegowskiego podmiotom niepaństwowym;

68. wzywa Radę UE–USA ds. Handlu i Technologii do przeprowadzenia szeroko zakrojonych i otwartych konsultacji ze społeczeństwem obywatelskim w celu opracowania wspólnej strategii i standardów UE-USA, w tym wspólnej białej listy lub czarnej listy;

69. wzywa do rozpoczęcia rozmów z innymi państwami, w szczególności z Izraelem, w celu ustalenia ram wprowadzania na rynek oprogramowania szpiegowskiego i udzielania pozwoleń na wywóz, w tym zasad dotyczących przejrzystości, listy krajów kwalifikujących się z uwzględnieniem standardów w zakresie praw człowieka i ustaleń dotyczących należytej staranności;

70. zauważa, że w porównaniu ze Stanami Zjednoczonymi, gdzie NSO zostało szybko wpisane na czarną listę, a prezydent USA podpisał dekret, zgodnie z którym firma ta nie może wykorzystywać w sposób operacyjny komercyjnego oprogramowania szpiegowskiego, które stwarza znaczące ryzyko dla kontrwywiadu lub bezpieczeństwa rządu Stanów Zjednoczonych lub znaczące ryzyko niewłaściwego wykorzystania przez zagraniczny rząd lub osobę zagraniczną, na szczeblu UE nie podjęto żadnych wystarczających działań w odniesieniu do przywozu oprogramowania szpiegowskiego i egzekwowania przepisów dotyczących wywozu;

71. stwierdza, że należy wzmocnić unijne przepisy dotyczące wywozu i ich egzekwowanie w celu ochrony praw człowieka w państwach trzecich oraz że potrzebne są niezbędne narzędzia, aby skutecznie wdrażać ich klauzule; przypomina, że UE powinna dążyć do połączenia sił ze Stanami Zjednoczonymi i innymi sojusznikami w celu uregulowania handlu oprogramowaniem szpiegowskim i wykorzystania ich łącznej siły rynkowej do wymuszenia zmian oraz ustanowić zestaw solidnych standardów przejrzystości, identyfikowalności i odpowiedzialności za wykorzystywanie technologii nadzoru, czego efektem powinna być inicjatywa na szczeblu Organizacji Narodów Zjednoczonych;

Luki zero-day

72. wzywa do uregulowania kwestii odkrywania, udostępniania, naprawiania i wykorzystywania luk oraz procedur ujawniania informacji, co uzupełni podstawę określoną w dyrektywie (UE) 2022/2555 ([34]) (dyrektywa NIS 2) i we wniosku dotyczącym aktu dotyczącego cyberodporności ([35]);

73. uważa, że naukowcy muszą mieć możliwość badania luk i dzielenia się wynikami bez odpowiedzialności cywilnej i karnej na mocy m.in. dyrektywy o cyberprzestępczości i dyrektywy o prawie autorskim;

74. wzywa najważniejsze podmioty z branży do stworzenia zachęt dla badaczy do udziału w badaniach nad lukami poprzez inwestowanie w plany naprawiania luk, praktyki ujawniania informacji w branży i społeczeństwu obywatelskiemu oraz prowadzenie programów wynagradzania za wykrywanie błędów;

75. wzywa Komisję, aby zwiększyła wsparcie i finansowanie programów wynagradzania za wykrywanie luk i innych projektów służących poszukiwaniu i naprawianiu luk w zabezpieczeniach oraz aby ustanowiła skoordynowane podejście do obowiązkowego ujawniania luk między państwami członkowskimi;

76. wzywa do wprowadzenia zakazu sprzedaży luk w zabezpieczeniach systemu w jakimkolwiek celu innym niż wzmocnienie bezpieczeństwa tego systemu oraz obowiązku ujawniania wyników wszystkich badań nad lukami w skoordynowany i odpowiedzialny sposób, promując bezpieczeństwo publiczne i minimalizując ryzyko wykorzystania luk w zabezpieczeniach;

77. wzywa podmioty publiczne i prywatne do utworzenia publicznie dostępnego punktu kontaktowego, w którym można zgłaszać luki w systemie w sposób skoordynowany i odpowiedzialny, a także do tego, by organizacje, które otrzymują informacje o lukach w swoim systemie, podejmowały natychmiastowe działania w celu ich naprawienia; uważa, że w przypadku gdy dostępna jest poprawka, należy upoważnić organizacje do wprowadzenia odpowiednich środków, aby zapewnić szybkie i gwarantowane wdrożenie w ramach skoordynowanego i odpowiedzialnego procesu ujawniania informacji;

78. uważa, że państwa członkowskie powinny przeznaczyć wystarczające zasoby finansowe, techniczne i ludzkie na badania nad bezpieczeństwem luk i ich naprawianie;

([34]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, Dz.U. L 333 z 27.12.2022, s. 80.

([35]) Wniosek z dnia 15 września 2022 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów w cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020 [COM(2022)0454].

79. wzywa państwa członkowskie do opracowania procesów ujawniania luk, określonych w przepisach prawa, które stanowią, że domyślnie luki należy ujawniać, a nie wykorzystywać, oraz że każda decyzja o odstąpieniu od tego podejścia musi stanowić wyjątek i podlegać ocenie zgodnie z wymogami konieczności i proporcjonalności, w tym rozważeniu, czy infrastruktura, której dotyczy luka, jest wykorzystywana przez dużą część populacji, oraz objąć ścisłym nadzorem niezależnego organu nadzorczego, a także przejrzystymi procedurami i decyzjami;

Sieci telekomunikacyjne

80. podkreśla, że należy cofnąć licencję każdemu dostawcy usług, co do którego stwierdzono, że ułatwia nieuprawniony dostęp do krajowej lub międzynarodowej infrastruktury sygnalizacji ruchomej we wszystkich generacjach (obecnie od 2G do 5G);

81. podkreśla, że procesy, za pomocą których podmioty działające w złej wierze mogą tworzyć nowe numery telefonów z całego świata, powinny być lepiej uregulowane, aby utrudnić ukrycie nielegalnych działań;

82. podkreśla potrzebę zapewnienia przez dostawców usług telekomunikacyjnych zdolności do wykrywania potencjalnych nadużyć w zakresie dostępu, kontroli lub skutecznego końcowego wykorzystania infrastruktury sygnalizacji uzyskanej przez strony trzecie w drodze umów handlowych lub innych umów w państwie członkowskim, w którym prowadzą działalność;

83. wzywa państwa członkowskie do zapewnienia, aby właściwe organy krajowe, zgodnie z przepisami dyrektywy NIS 2, oceniały poziom odporności dostawców usług telekomunikacyjnych na nieuprawnione włamania;

84. wzywa dostawców usług telekomunikacyjnych do podjęcia zdecydowanych i widocznych działań w celu złagodzenia różnych form emulacji bez zezwolenia ruchu telekomunikacyjnego generowanego przez element sieci w celu uzyskania dostępu do danych lub usług przeznaczonych dla legalnego użytkownika i innej działalności polegającej na manipulowaniu normalnymi operacjami elementów sieci ruchomej i infrastruktury do celów inwigilacji przez podmioty działające w złej wierze, w tym podmioty na szczeblu państwowym oraz grupy przestępcze;

85. wzywa państwa członkowskie do podjęcia działań w celu zapewnienia, aby podmioty państwowe spoza UE, które nie przestrzegają praw podstawowych, nie miały kontroli nad infrastrukturą strategiczną ani nie mogły z niej skutecznie korzystać oraz aby nie miały wpływu na decyzje dotyczące strategicznej infrastruktury w Unii, w tym infrastruktury telekomunikacyjnej;

86. wzywa wszystkie państwa członkowskie do priorytetowego traktowania większych inwestycji w ochronę infrastruktury krytycznej, takiej jak krajowe systemy telekomunikacyjne, aby naprawić luki w ochronie przed naruszeniami prywatności, zapobiegać wyciekom danych i nieuprawnionym włamaniom, aby bronić praw podstawowych obywateli;

87. wzywa właściwe organy krajowe do aktywnego promowania wzmacniania zdolności dostawców, a także zdolności reagowania, aby usprawnić identyfikację osób nielegalnie namierzonych, a także powiadamianie i zgłaszanie incydentów, w celu zapewnienia ciągłej, wymiernej pewności i łagodzenia skutków wykorzystywania luk w zabezpieczeniach przez krajowe i pozaunijne podmioty działające w złej wierze;

E-prywatność

88. wzywa do szybkiego przyjęcia rozporządzenia w sprawie e-prywatności w sposób, który w pełni odzwierciedla orzecznictwo dotyczące ograniczeń na potrzeby bezpieczeństwa narodowego oraz konieczność zapobiegania nadużywaniu technologii nadzoru, a także wzmacnia podstawowe prawo do prywatności oraz zapewnia silne zabezpieczenia o skuteczne egzekwowanie prawa; podkreśla, że zakres uprawnionego przechwytywania nie powinien wykraczać poza dyrektywę o e-prywatności (2002/58/WE);

89. wzywa do ochrony wszelkiej łączności elektronicznej, treści i metadanych przed nadużywaniem danych osobowych i prywatnej komunikacji przez prywatne przedsiębiorstwa i organy rządowe; zwraca uwagę, że nie należy osłabiać narzędzi bezpieczeństwa cyfrowego w fazie projektowania, takich jak pełne szyfrowanie transmisji;

90. wzywa Komisję do dokonania oceny wdrażania przez państwa członkowskie dyrektywy o e-prywatności w całej UE oraz do wszczęcia postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego w przypadku wystąpienia naruszeń;

Rola Europolu

91. zauważa, że w piśmie do przewodniczącego komisji PEGA z kwietnia 2023 r. Europol poinformował komisję, że skontaktował się z Bułgarią, Grecją, Hiszpanią, Węgrami i Polską w celu ustalenia, czy toczą się tam lub są planowane postępowania przygotowawcze lub inne postępowania na podstawie mających zastosowanie przepisów prawa krajowego, które Europol mógłby wesprzeć; podkreśla, że oferowanie pomocy państwom członkowskim nie stanowi wszczęcia, przeprowadzenia lub koordynowania postępowania przygotowawczego, o którym mowa w art. 6;

92. wzywa Europol do pełnego wykorzystania nowo nabytych uprawnień na mocy art. 6 ust. 1a rozporządzenia (UE) 2022/991, w ramach których Europol może zaproponować właściwym organom zainteresowanych państw członkowskich, w stosownych przypadkach, wszczęcie, przeprowadzenie lub koordynowanie postępowania przygotowawczego; przypomina, że zgodnie z art. 6 odrzucenie takiego wniosku należy do państw członkowskich;

93. wzywa wszystkie państwa członkowskie, aby zobowiązały się wobec Parlamentu Europejskiego i Rady do angażowania Europolu w dochodzenia w sprawie zarzutów nielegalnego korzystania z oprogramowania szpiegowskiego na szczeblu krajowym, w szczególności w przypadku propozycji, o której mowa w art. 6 ust. 1a rozporządzenia (UE) 2022/991;

94. wzywa państwa członkowskie do utworzenia w ramach Europolu rejestru krajowych operacji egzekwowania prawa z wykorzystaniem oprogramowania szpiegowskiego, w którym to rejestrze każda operacja powinna być oznaczona kodem, oraz do tego, by wykorzystanie oprogramowania szpiegowskiego przez rządy uwzględnić w rocznym sprawozdaniu Europolu z oceny zagrożenia zorganizowaną przestępczością internetową;

95. jest zdania, że należy zastanowić się nad rolą Europolu w przypadku, gdy organy krajowe nie wszczynają postępowań przygotowawczych lub odmawiają ich wszczęcia, a istnieją wyraźne zagrożenia dla interesów i bezpieczeństwa UE;

Unijna polityka rozwoju

96. wzywa Komisję i ESDZ do wdrożenia bardziej rygorystycznych mechanizmów kontroli w celu zagwarantowania, że w ramach unijnej pomocy rozwojowej, w tym przekazywania technologii nadzoru i szkoleń w zakresie wdrażania oprogramowania służącego do nadzoru, nie są finansowane ani wspierane narzędzia i działania, które mogłyby naruszać zasady demokracji, dobrych rządów, praworządności i poszanowania praw człowieka lub które stwarzają zagrożenie dla bezpieczeństwa międzynarodowego lub zasadniczego bezpieczeństwa Unii i jej państw członkowskich; zauważa, że oceny Komisji dotyczące zgodności z prawem Unii, w szczególności z rozporządzeniem finansowym, powinny zawierać specjalne kryteria kontroli i mechanizmy egzekwowania, aby zapobiec takim nadużyciom, w tym przewidywać ewentualne tymczasowe zawieszenie określonych projektów w przypadku wykrycia naruszenia tych zasad;

97. wzywa Komisję i ESDZ do uwzględnienia w każdej ocenie wpływu na prawa człowieka i prawa podstawowe procedury monitorowania pod kątem potencjalnego nadużywania nadzoru, która to procedura w pełni uwzględnia art. 51 Karty w terminie jednego roku [od publikacji zaleceń komisji PEGA]; podkreśla, że procedurę tę należy przedstawić Parlamentowi i Radzie, a ocenę wpływu należy przeprowadzić przed udzieleniem jakiegokolwiek wsparcia państwom niebędącym członkami UE;

98. wzywa ESDZ do uwzględnienia kwestii nadużywania oprogramowania szpiegowskiego wobec obrońców praw człowieka w rocznym sprawozdaniu UE na temat praw człowieka i demokracji;

Regulacje finansowe Unii

99. zwraca uwagę, że należy zwiększyć nacisk na poszanowanie praw człowieka przez sektor finansowy; podkreśla, że zalecenia UNGPs 10+ dotyczące biznesu i praw człowieka należy włączyć do prawa Unii oraz że dyrektywa w sprawie należytej staranności powinna mieć pełne zastosowanie do sektora finansowego, aby zapewnić poszanowanie demokracji, praw człowieka i praworządności w sektorze finansowym;

100. jest zaniepokojony konsekwencjami decyzji TSUE dotyczącej dyrektywy (UE) 2018/843 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu ([36]), zgodnie z którą informacje o beneficjentach rzeczywistych podmiotów o charakterze korporacyjnym i prawnym, wprowadzone do krajowego i publicznie dostępnego rejestru beneficjentów rzeczywistych, uznaje się za nieważne ([37]); podkreśla, że – biorąc pod uwagę decyzję TSUE – przyszła dyrektywa powinna umożliwiać jak największą publiczną dostępność, tak aby trudniej było ukryć zakup lub sprzedaż oprogramowania szpiegowskiego za pośrednictwem pełnomocników i spółek brokerskich;

([36]) Wyrok Trybunału z dnia 22 listopada 2022 r. w sprawach połączonych C-37/20 i C-601/20, ECLI.EU:C:2022:912.
([37]) TSUE. Komunikat prasowy nr 188/22, wyroku Trybunału w sprawach połączonych C-37/20 i C-601/20.

Postępowanie po przyjęciu rezolucji przez Parlament

101. wzywa do podjęcia niezwłocznych działań w następstwie rezolucji Parlamentu z 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych; podkreśla, że zalecenia zawarte we wspomnianej rezolucji należy wykonać w trybie pilnym;

102. podkreśla, że chociaż nadzór nad działaniami służb wywiadowczych powinien opierać się zarówno na legitymacji demokratycznej (silnych ramach prawnych, upoważnieniu *ex ante* i weryfikacji *ex post*), jak i na odpowiednich zdolnościach technicznych i wiedzy fachowej, większości obecnych unijnych i amerykańskich organów nadzoru zdecydowanie brakuje ich obu, zwłaszcza zdolności technicznych;

103. podobnie jak w przypadku Echelonu wzywa wszystkie parlamenty narodowe, które jeszcze tego nie uczyniły, do przyznania parlamentarzystom lub organom eksperckim kompetencji prawnych w zakresie prowadzenia dochodzeń w ramach znaczącego nadzoru nad działaniami wywiadowczymi; wzywa parlamenty narodowe do zapewnienia tego, aby takie komisje lub organy nadzoru posiadały wystarczające zasoby, fachową wiedzę techniczną i środki prawne, w tym prawo do prowadzenia kontroli na miejscu, umożliwiające im sprawowanie skutecznej kontroli nad służbami wywiadowczymi;

104. wzywa do powołania grupy wysokiego szczebla w celu zaproponowania, w sposób przejrzysty i we współpracy z parlamentami, zaleceń i dalszych kroków, jakie należy poczynić w kierunku nasilenia demokratycznej kontroli, w tym kontroli parlamentarnej nad służbami wywiadowczymi, oraz bardziej intensywnej współpracy w zakresie kontroli w UE, w szczególności w jej wymiarze transgranicznym;

105. uważa, że ta grupa wysokiego szczebla powinna:

a) określać minimalne europejskie normy lub wytyczne w zakresie nadzoru *ex ante* i *ex post* nad służbami wywiadowczymi w oparciu o obowiązujące sprawdzone wzorce postępowania i zalecenia organów międzynarodowych takich jak ONZ i Rada Europy, w tym w sprawie uznawania organów nadzorczych za osobę trzecią na podstawie „zasady osoby trzeciej" lub „zasady kontroli organu zastrzegającego", dotyczące sprawowania nadzoru nad wywiadem z państw obcych i pociągania go do odpowiedzialności;

b) opracowywać kryteria zwiększonej przejrzystości na podstawie ogólnej zasady dostępu do informacji i tak zwanych „zasad z Tshwane" ([38]);

106. zamierza zorganizować konferencję z krajowymi – parlamentarnymi lub niezależnymi – organami nadzoru;

107. wzywa państwa członkowskie do wykorzystania najlepszych praktyk, aby poprawić dostęp ich organów nadzoru do informacji na temat działań wywiadowczych, w tym informacji niejawnych i informacji pochodzących od innych służb, oraz ustanowienia uprawnień w zakresie przeprowadzania wizyt na miejscu, solidnego zbioru uprawnień w zakresie przesłuchań, odpowiednich zasobów i fachowej wiedzy technicznej, zdecydowanej niezależności od ich rządu oraz obowiązku sprawozdawczego wobec ich parlamentów;

108. wzywa państwa członkowskie do rozwoju współpracy między organami nadzoru;

109. wzywa Komisję do przedstawienia wniosku dotyczącego unijnej procedury sprawdzającej poświadczenia bezpieczeństwa wszystkich osób sprawujących urzędy w Unii, ponieważ obecny system, który opiera się na poświadczaniu bezpieczeństwa przez państwa członkowskie obywatelstwa, przewiduje różne wymogi i różną długość procedur w systemach krajowych, co powoduje różne traktowanie posłów do Parlamentu i ich pracowników w zależności od obywatelstwa;

110. przypomina postanowienia porozumienia międzyinstytucjonalnego między Parlamentem Europejskim a Radą w sprawie przekazywania Parlamentowi Europejskiemu i przetwarzania przez Parlament posiadanych przez Radę informacji niejawnych dotyczących spraw innych niż z dziedziny wspólnej polityki zagranicznej i bezpieczeństwa, które należy wykorzystać do poprawy nadzoru na szczeblu UE;

Unijne programy badawcze

111. wzywa do wdrożenia bardziej rygorystycznych i skutecznych mechanizmów kontroli w celu dopilnowania, by unijne fundusze badawcze nie były wykorzystywane do finansowania ani wspierania narzędzi naruszających wartości UE, w tym oprogramowania szpiegowskiego i narzędzi nadzoru; zauważa, że oceny zgodności z prawem Unii powinny zawierać specjalne kryteria kontroli w celu zapobiegania takim nadużyciom; wzywa do wstrzymania unijnych funduszy badawczych dla podmiotów, które są lub były zaangażowane w bezpośrednie lub pośrednie ułatwianie naruszeń praw człowieka za pomocą narzędzi nadzoru;

([38]) „The Global Principles on National Security and the Right to Information" [Globalne zasady obrony narodowej i prawa do informacji], czerwiec 2013 r.

112. podkreśla, że unijne finansowanie badań naukowych, takie jak umowy w sprawie programu „Horyzont Europa" z państwami niebędącymi członkami UE nie może być wykorzystywane do przyczyniania się do rozwoju oprogramowania szpiegowskiego i równoważnych technologii;

Unijne laboratorium technologiczne

113. wzywa Komisję, aby niezwłocznie zainicjowała stworzenie niezależnego europejskiego interdyscyplinarnego instytutu badawczego, koncentrującego się na badaniach i rozwoju na styku technologii informacyjnych i komunikacyjnych, praw podstawowych i bezpieczeństwa; podkreśla, że instytut ten powinien współpracować z ekspertami, środowiskiem akademickim i przedstawicielami społeczeństwa obywatelskiego, a także powinien być otwarty na uczestnictwo ekspertów i instytucji z państw członkowskich;

114. podkreśla, że instytut ten przyczyniłoby się to do zwiększenia świadomości, przypisania działań i odpowiedzialności w Europie i poza nią, a także do zwiększenia europejskiej bazy talentów i zrozumienia, w jaki sposób dostawcy oprogramowania szpiegowskiego rozwijają, utrzymują, sprzedają i świadczą usługi osobom trzecim;

115. uważa, że zadaniem instytutu powinno być wykrywanie i ujawnianie niezgodnego z prawem wykorzystywania oprogramowania do celów nielegalnej inwigilacji, zapewnianie dostępnego i bezpłatnego wsparcia prawnego i technologicznego, w tym badań przesiewowych smartfonów dla osób, które podejrzewają, że stały się celem oprogramowania szpiegowskiego, oraz narzędzi niezbędnych do wykrywania oprogramowania szpiegującego, przeprowadzanie analizy kryminalistycznej na potrzeby postępowań wstępnych oraz regularne składanie sprawozdania na temat wykorzystywania i niewłaściwego wykorzystywania oprogramowania szpiegującego w UE, z uwzględnieniem aktualizacji technologicznych; uważa, że sprawozdanie to powinno być udostępniane corocznie i przekazywane Komisji, Parlamentowi i Radzie;

116. zaleca, aby Komisja utworzyła unijne laboratorium technologiczne w ścisłej współpracy z zespołem reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE) i ENISA oraz konsultowała się przy tym z odpowiednimi ekspertami, tak aby wyciągnąć wnioski z najlepszych praktyk akademickich;

117. podkreśla znaczenie zapewnienia odpowiedniego finansowania unijnego laboratorium technologicznego;

118. zaleca, aby Komisja przedstawiła system certyfikacji w zakresie analizy i uwierzytelniania materiałów kryminalistycznych;

119. wzywa Komisję do wspierania zdolności społeczeństwa obywatelskiego na całym świecie w celu zwiększenia odporności na ataki oprogramowania szpiegowskiego oraz zapewnienia obywatelom pomocy i usług;

Praworządność

120. podkreśla, że skutki bezprawnego stosowania oprogramowania szpiegowskiego są znacznie dotkliwsze w państwach członkowskich, w których organy zajmujące się zwykle prowadzeniem dochodzeń i zapewnianiem osobom inwigilowanym prawa do zadośćuczynienia są zawłaszczane przez państwo, oraz że tam, gdzie istnieje kryzys praworządności i zagrożona jest niezależność wymiaru sprawiedliwości, nie można polegać na organach krajowych;

121. wzywa zatem Komisję, aby zapewniła skuteczne wdrożenie jej narzędzi w zakresie praworządności, w szczególności przez:

a) wprowadzenie bardziej kompleksowego monitorowania praworządności, w tym zalecenia dla poszczególnych krajów dotyczące niezgodnego z prawem wykorzystywania przez państwa członkowskie oprogramowania szpiegującego w rocznym sprawozdaniu Komisji na temat praworządności, ocenę reakcji instytucji państwowych, jeśli chodzi o zapewnienie zadośćuczynienia osobom inwigilowanym z użyciem oprogramowania szpiegowskiego oraz poprzez rozszerzenie zakresu rocznego sprawozdania na temat praworządności i uwzględnienie w nim wszystkich wyzwań dla demokracji, praworządności i praw podstawowych zawartych w art. 2 TUE, o co wielokrotnie zabiegał Parlament;

b) aktywne wszczynanie i łączenie postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego w związku z uchybieniami w zakresie praworządności, takimi jak zagrożenia dla niezależności sądownictwa oraz skutecznego funkcjonowania policji i prokuratury w kontekście współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych;

Unijny fundusz wsparcia finansowego w związku z postępowaniem sądowym

122. wzywa do ustanowienia, bez zbędnej zwłoki, unijnego funduszu wsparcia finansowego w związku z postępowaniem sądowym w celu pokrycia rzeczywistych kosztów procesowych i umożliwienia osobom inwigilowanym z użyciem oprogramowania szpiegowskiego dochodzenia odpowiedniego zadośćuczynienia, w tym za szkody związane z bezprawnym stosowaniem oprogramowania szpiegowskiego przeciwko nim, zgodnie z działaniem przygotowawczym przyjętym przez Parlament w 2017 r. w celu utworzenia „unijnego funduszu wsparcia finansowego dla postępowań w sprawach o naruszenia zasad demokracji, praworządności i praw podstawowych";

Instytucje UE

123. wyraża zaniepokojenie dotychczasowym brakiem działań ze strony Komisji i wzywa ją do pełnego wykorzystania wszystkich uprawnień przysługujących jej jako strażniczce traktatów oraz do kompleksowego i dogłębnego zbadania sprawy nadużywania oprogramowania szpiegowskiego i handlu nim w Unii;

124. wzywa Komisję do przeprowadzenia pełnego dochodzenia w sprawie wszystkich zarzutów i podejrzeń dotyczących wykorzystania oprogramowania szpiegowskiego przeciwko jej urzędnikom oraz do złożenia sprawozdania Parlamentowi, a w razie potrzeby właściwym organom ścigania;

125. wzywa Komisję do powołania specjalnej grupy zadaniowej (z udziałem krajowych komisji wyborczych) ds. ochrony wyborów europejskich w 2024 r. w całej Unii; przypomina, że zagrożeniem dla europejskich procesów wyborczych jest nie tylko ingerencja zagraniczna, ale również wewnętrzna; podkreśla, że niewłaściwe wykorzystanie wszechobecnych narzędzi nadzoru, takich jak Pegasus, może mieć wpływ na wybory;

126. zauważa, że zbiorcza odpowiedź Rady na zapytania Parlamentu skierowane do poszczególnych państw członkowskich wpłynęła do komisji PEGA dopiero w przeddzień publikacji projektu sprawozdania, czyli około cztery miesiące po pismach PE; wyraża zaniepokojenie brakiem działań Rady Europejskiej i Rady Unii Europejskiej oraz – zważywszy na skalę zagrożenia dla demokracji w Europie – wzywa do zorganizowania specjalnego szczytu Rady Europejskiej;

127. wzywa Radę UE, by zajęła się wydarzeniami związanymi ze stosowaniem oprogramowania szpiegowskiego i jego wpływem na wartości zapisane w art. 2 TUE podczas wysłuchań organizowanych na mocy art. 7 ust. 1 TUE;

128. wzywa Radę do stałego zapraszania Parlamentu Europejskiego na posiedzenia jej Komitetu ds. Bezpieczeństwa, zgodnie z art. 17 ust. 2 przepisów Rady z 2013 r. dotyczących bezpieczeństwa;

129. stoi na stanowisku, że Parlament powinien mieć pełne uprawnienia śledcze, w tym lepszy dostęp do informacji jawnych i niejawnych, prawo do wzywania świadków i do formalnego żądania od świadków zeznań pod przysięgą i dostarczania wymaganych informacji w określonych terminach; przypomina stanowisko Parlamentu w sprawie wniosku Parlamentu z dnia 23 maja 2012 r. dotyczącego rozporządzenia Parlamentu Europejskiego w sprawie szczegółowych przepisów regulujących wykonywanie przez Parlament Europejski uprawnień śledczych i zastępującego decyzję 95/167/WE, Euratom, EWWiS Parlamentu Europejskiego, Rady i Komisji ([39]); wzywa Radę do natychmiastowego rozpoczęcia prac nad tym wnioskiem dotyczącym rozporządzenia, aby zapewnić Parlamentowi Europejskiemu odpowiednie uprawnienia śledcze;

130. uznaje działania Parlamentu podejmowane na rzecz wykrywania infekcji oprogramowaniem szpiegowskim; uważa jednak, że należy wzmocnić ochronę personelu, uwzględniając przywileje i immunitety osób, które były szpiegowane; przypomina, że wszelkie ataki na prawa polityczne posłów stanowią atak na niezależność i suwerenność instytucji, jak również atak na prawa wyborców;

131. wzywa Prezydium do przyjęcia protokołu dotyczącego przypadków, w których członkowie lub personel Izby stali się bezpośrednim lub pośrednim celem inwigilacji z użyciem oprogramowania szpiegowskiego, oraz podkreśla, że wszystkie przypadki muszą być zgłaszane przez Parlament właściwym organom ścigania; podkreśla, że Parlament powinien zapewnić pomoc prawną i technicznej w takich przypadkach;

132. postanawia zapoczątkować konferencję międzyinstytucjonalną, w ramach której Parlament, Rada i Komisja muszą dążyć do reform zarządzania służących wzmocnieniu zdolności instytucjonalnej Unii do tego, by odpowiednio reagować na pochodzące z wewnątrz ataki na demokrację i praworządność oraz by zagwarantować, że Unia dysponuje skutecznymi ponadnarodowymi metodami egzekwowania traktatów i prawa wtórnego w przypadku nieprzestrzegania ich przez państwa członkowskie;

([39]) Dz.U. C 264 E z 13.9.2013, s. 41.

133. wzywa do szybkiego przyjęcia wniosku Komisji dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii (COM(2022)0122) oraz jego szybkiego wdrożenia, a następnie ścisłego egzekwowania w celu zmniejszenia ryzyka infekcji oprogramowaniem szpiegowskim urządzeń i systemów wykorzystywanych przez pracowników instytucji UE i polityków;

134. wzywa UE do przystąpienia do konwencji 108+;

135. wzywa Europejskiego Rzecznika Praw Obywatelskich do zainicjowania dyskusji w ramach europejskiej sieci rzeczników praw obywatelskich na temat wpływu nadużywania powszechnej inwigilacji na procesy demokratyczne i prawa obywateli; wzywa sieć do opracowania zaleceń dotyczących skutecznego i znaczącego dochodzenia roszczeń w całej UE;

Działania legislacyjne

136. wzywa Komisję do szybkiego wystąpienia z wnioskami ustawodawczymi na podstawie niniejszego zalecenia;

o

o o

137. zobowiązuje swoją przewodniczącą do przekazania niniejszego zalecenia państwom członkowskim, Radzie, Komisji oraz Europolowi.