Wtorek, 8 września 2015 r.

P8_TA(2015)0288

Prawa człowieka a technologia w państwach trzecich

Rezolucja Parlamentu Europejskiego z dnia 8 września 2015 r. w sprawie „Prawa człowieka a technologia: wpływ systemów inwigilacji i nadzoru na prawa człowieka w państwach trzecich" (2014/2232(INI))

(2017/C 316/03)

Parlament Europejski,

— uwzględniając Powszechną deklarację praw człowieka oraz Międzynarodowy pakt praw obywatelskich i politycznych, w szczególności jego art. 19,

— uwzględniając ramy strategiczne Unii Europejskiej w dziedzinie praw człowieka i demokracji, przyjęte przez Radę w dniu 25 czerwca 2012 r. ([1]),

— uwzględniając wytyczne UE w sprawie praw człowieka dotyczące wolności wypowiedzi w internecie i poza nim, przyjęte przez Radę (do Spraw Zagranicznych) w dniu 12 maja 2014 r. ([2]),

— uwzględniając wytyczne dla sektora technologii informacyjno-komunikacyjnych dotyczące realizacji wytycznych ONZ dotyczących biznesu i praw człowieka, opublikowane przez Komisję w z czerwcu 2013 r.,

— uwzględniając sprawozdanie Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE) z dnia 15 grudnia 2011 r. zatytułowane „Wolność wypowiedzi w internecie" ([3]) oraz sprawozdanie specjalnego przedstawiciela ds. wolności mediów przy Stałej Radzie OBWE z dnia 27 listopada 2014 r. ([4]),

— uwzględniając sprawozdanie specjalnego sprawozdawcy ONZ w sprawie propagowania i ochrony praw człowieka i podstawowych wolności w warunkach walki z terroryzmem z dnia 23 września 2014 r. (A/69/397) ([5]),

— uwzględniając sprawozdanie Biura Wysokiego Komisarza NZ ds. Praw Człowieka z dnia 30 czerwca 2014 r. zatytułowane „Prawo do prywatności w erze cyfrowej" ([6]),

— uwzględniając sprawozdanie specjalnego sprawozdawcy ONZ ds. wolności opinii i wypowiedzi z dnia 17 kwietnia 2013 r. (A/HRC/23/40), zawierające analizę wpływu nadzorowania komunikacji przez państwa na poszanowanie praw człowieka w zakresie prywatności oraz wolności opinii i wypowiedzi,

— uwzględniając sprawozdanie Komisji Zagadnień Prawnych i Praw Człowieka Zgromadzenia Parlamentarnego Rady Europy z dnia 26 stycznia 2015 r. w sprawie „Masowego nadzoru" ([7]),

— uwzględniając swoją rezolucję z dnia 12 marca 2014 r. w sprawie realizowanych przez Agencję Bezpieczeństwa Narodowego Stanów Zjednoczonych 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 ([8]),

---

([1]) http://eeas.europa.eu/delegations/un_geneva/press_corner/focus/events/2012/20120625_en.htm.
([2]) http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf.
([3]) http://www.osce.org/fom/80723?download=true.
([4]) http://www.osce.org/fom/127656?download=true .
([5]) http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement.
([6]) http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc.
([7]) http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10-b7a2.
([8]) Teksty przyjęte, P7_TA(2014)0230.

— uwzględniając sprawozdanie specjalnego przedstawiciela Sekretarza Generalnego ONZ ds. respektowania praw człowieka przez korporacje transnarodowe i inne przedsiębiorstwa z dnia 21 marca 2011 r., zatytułowane „Wytyczne dotyczące biznesu i praw człowieka: wdrażanie ram Organizacji Narodów Zjednoczonych »Ochrona, poszanowanie i naprawa«" ([1]),

— uwzględniając wytyczne OECD dla przedsiębiorstw wielonarodowych ([2]) oraz sprawozdanie roczne z 2014 r. dotyczące wytycznych OECD dla przedsiębiorstw wielonarodowych ([3]),

— uwzględniając sprawozdanie roczne Internetowej Korporacji ds. Nadawania Nazw i Numerów z 2013 r. ([4]),

— uwzględniając komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów z dnia 12 lutego 2014 r. zatytułowany „Polityka wobec internetu i zarządzanie internetem: rola Europy w kształtowaniu przyszłości zarządzania internetem" ([5]),

— uwzględniając oświadczenie z konferencji wielostronnej NETmundial przyjęte w dniu 24 kwietnia 2014 r. ([6]),

— uwzględniając podsumowanie przewodniczącego dziewiątego Forum Zarządzania Internetem, które odbyło się w Stambule w dniach 2–5 września 2014 r.,

— uwzględniając obowiązujące środki ograniczające Unii Europejskiej, z których część obejmuje embarga na sprzęt telekomunikacyjny, technologie informacyjno-komunikacyjne i narzędzia służące do monitorowania,

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 599/2014 z dnia 16 kwietnia 2014 r. zmieniające rozporządzenie Rady (WE) nr 428/2009 ustanawiające wspólnotowy system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania ([7]),

— uwzględniając wspólne oświadczenie Parlamentu Europejskiego, Rady i Komisji w sprawie przeglądu systemu kontroli wywozu produktów podwójnego zastosowania z dnia 16 kwietnia 2014 r. ([8]),

— uwzględniając decyzje przyjęte na 19. posiedzeniu plenarnym Porozumienia z Wassenaar w sprawie kontroli eksportu broni konwencjonalnej oraz towarów i technologii podwójnego zastosowania, które odbyło się w Wiedniu w dniach 3–4 grudnia 2013 r.,

— uwzględniając komunikat Komisji do Rady i Parlamentu Europejskiego z dnia 24 kwietnia 2014 r., zatytułowany „Przegląd polityki kontroli wywozu: zapewnienie bezpieczeństwa i konkurencyjności w zmieniającym się świecie" ([9]),

— uwzględniając konkluzje Rady z dnia 21 listopada 2014 r. w sprawie przeglądu polityki kontroli wywozu,

— uwzględniając swoją rezolucję z dnia 11 grudnia 2012 r. w sprawie strategii wolności cyfrowej w polityce zagranicznej UE ([10]),

---

([1]) http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf?v=1392752313000/_/jcr:system/jcr:version-storage/12/52/13/125213a0-e4bc-4a15-bb96-9930bb8fb6a1/1.3/jcr:frozennode

([2]) http://www.oecd.org/daf/inv/mne/48004323.pdf

([3]) http://www.oecd-ilibrary.org/docserver/download/2014091e.pdf?expires=1423160236&id=id&accname=ocid194994&checksum=D1FC664FBCEA28FC856AE63932715B3C

([4]) https://www.icann.org/en/system/files/files/annual-report-2013-en.pdf

([5]) COM(2014)0072.

([6]) http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

([7]) Dz.U. L 173 z 12.6.2014, s. 79.

([8]) Dz.U. L 173 z 12.6.2014, s. 82.

([9]) COM(2014)0244.

([10]) Teksty przyjęte, P7_TA(2012)0470.

Wtorek, 8 września 2015 r.

— uwzględniając swoją rezolucję z dnia 13 czerwca 2013 r. w sprawie wolności prasy i mediów na świecie ([1]),

— uwzględniając swoje rezolucje w sprawie drastycznych przypadków łamania praw człowieka, demokracji i praworządności, budzących zaniepokojenie w sprawach dotyczących wolności cyfrowych,

— uwzględniając swoją rezolucję z dnia 12 marca 2015 r. w sprawie priorytetów UE w Radzie Praw Człowieka ONZ w 2015 r. ([2]),

— uwzględniając swoją rezolucję z dnia 11 lutego 2015 r. w sprawie przedłużenia mandatu Forum Zarządzania Internetem ([3]),

— uwzględniając swoją rezolucję z dnia 12 marca 2015 r. w sprawie rocznego sprawozdania dotyczącego praw człowieka i demokracji na świecie za rok 2013 oraz polityki Unii Europejskiej w tym zakresie ([4]),

— uwzględniając pisemne zeznania Edwarda Snowdena przekazane Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w marcu 2014 r. ([5]),

— uwzględniając europejską konwencję praw człowieka oraz trwające negocjacje dotyczące przystąpienia UE do tej konwencji,

— uwzględniając Kartę praw podstawowych Unii Europejskiej,

— uwzględniając art. 52 Regulaminu,

— uwzględniając sprawozdanie Komisji Spraw Zagranicznych (A8-0178/2015),

A. mając na uwadze, że rozwój technologii i dostęp do otwartego internetu mają coraz większe znaczenie dla umożliwiania i zapewniania wykonywania praw człowieka i podstawowych wolności oraz ich pełnego poszanowania, gdyż wywierają pozytywny wpływ, rozszerzając zakres wolności wypowiedzi, dostępu do informacji, prawa do prywatności oraz wolności zrzeszania się i zgromadzeń na całym świecie;

B. mając na uwadze, że systemy technologiczne mogą być niewłaściwie użyte jako narzędzia łamania praw człowieka przez cenzurę, nadzór, nieuprawniony dostęp do urządzeń, zagłuszanie, przechwytywanie, lokalizowanie i śledzenie informacji i osób;

C. mając na uwadze, że w celu łamania praw człowieka takie działania podejmują podmioty publiczne i prywatne, w tym rządy i organy ścigania, a także organizacje przestępcze i sieci terrorystyczne;

D. mając na uwadze, że kontekst, w jakim opracowywane i wykorzystywane są technologie informacyjno-komunikacyjne, w znacznym stopniu determinuje wpływ, jaki mogą one mieć na propagowanie lub łamanie praw człowieka; mając na uwadze, że technologie informacyjne, szczególnie oprogramowanie, rzadko służą jednemu celowi i zazwyczaj mają podwójne zastosowanie, jeżeli chodzi o potencjał łamania praw człowieka, przy czym oprogramowanie jest również formą wypowiedzi;

E. mając na uwadze, że technologie informacyjno-komunikacyjne były kluczowymi narzędziami, które pomogły zorganizować ruchy i protesty społeczne w różnych państwach, szczególnie tych, w których rządzy sprawował autorytarny reżim;

([1]) Teksty przyjęte, P7_TA(2013)0274.
([2]) Teksty przyjęte, P8_TA(2015)0079.
([3]) Teksty przyjęte, P8_TA(2015)0033.
([4]) Teksty przyjęte, P8_TA(2015)0076.
([5]) http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

F. mając na uwadze, że ocena wpływu kontekstu, w jakim stosowane będą dane technologie, na prawa człowieka jest uzależniona od siły krajowych i regionalnych ram prawnych regulujących stosowanie technologii, a także od zdolności instytucji politycznych i sądowniczych do nadzorowania stosowania tych technologii;

G. mając na uwadze, że podmioty prywatne odgrywają coraz istotniejszą rolę w domenie cyfrowej we wszystkich sferach życia społecznego, ale w dalszym ciągu nie wprowadzono środków ochronnych uniemożliwiających im nadmierne ograniczanie praw podstawowych i swobód; mając na uwadze, że w konsekwencji podmioty prywatne odgrywają aktywniejszą rolę w ocenie legalności treści oraz opracowywaniu systemów bezpieczeństwa cybernetycznego i systemów nadzoru, co może mieć szkodliwy wpływ na poszanowanie praw człowieka na całym świecie;

H. mając na uwadze, że internet to rewolucyjne narzędzie, jeśli chodzi o możliwości wymiany wszelkiego rodzaju danych, informacji i wiedzy;

I. mając na uwadze, że szyfrowanie to ważna metoda pomagająca zabezpieczać systemy łączności i chronić korzystające z nich osoby;

J. mając na uwadze, że wielostronny model podejmowania decyzji okazał się korzystny dla zarządzania internetem jako proces zapewniający istotny, niewykluczający nikogo i oparty na zasadzie odpowiedzialności udział wszystkich zainteresowanych stron, w tym rządów, społeczeństwa obywatelskiego, społeczności technicznych i naukowych, sektora prywatnego i użytkowników;

K. mając na uwadze, że agencje wywiadowcze regularnie obchodzą protokoły i produkty kryptograficzne, by móc śledzić komunikację i przechwytywać dane; mając na uwadze, że Agencja Bezpieczeństwa Narodowego USA (NSA) zgromadziła informacje o znacznej liczbie tzw. błędów zero-day, czyli słabości zabezpieczeń teleinformatycznych, o których nie wie jeszcze opinia publiczna ani sprzedawca produktu; mając na uwadze, że takie działania podważają światowe wysiłki na rzecz poprawy bezpieczeństwa teleinformatycznego;

L. mając na uwadze, że służby wywiadowcze zlokalizowane w UE uczestniczyły w działaniach naruszających prawa człowieka;

M. mając na uwadze, że nadzór sądowniczy i demokratyczny oraz środki ochronne są w dużej mierze zbyt słabo rozwinięte wobec zachodzącego dynamicznego postępu technologicznego;

N. mając na uwadze, że środki w zakresie (cyber)bezpieczeństwa i walki z terroryzmem obejmujące technologie informacyjno-komunikacyjne oraz monitorowanie internetu mogą mieć znaczny szkodliwy wpływ na przestrzeganie praw człowieka i wolności jednostki na całym świecie, w tym na prawa i wolności obywateli UE mieszkających lub podróżujących za granicą, zwłaszcza wobec braku podstawy prawnej wprowadzającej zasady konieczności, proporcjonalności oraz nadzoru demokratycznego i sądowniczego;

O. mając na uwadze, że filtrowanie internetu i nadzorowanie komunikacji podważają zdolność obrońców praw człowieka do czerpania korzyści z internetu i przekazywania newralgicznych informacji, a także naruszają postanowienia kilku artykułów Powszechnej deklaracji praw człowieka, która gwarantuje każdej osobie prawo do prywatności i wolności wypowiedzi;

P. mając na uwadze, że zarówno bezpieczeństwo cyfrowe, jak i wolność cyfrowa są niezbędne i nie można jednego zastąpić drugim, lecz powinny się wzajemnie wzmacniać;

Q. mając na uwadze, że w kwestii wolności cyfrowych Unia Europejska będzie wzorem tylko wtedy, gdy będą one zagwarantowane w samej UE; mając na uwadze, że kluczowe znaczenie ma w związku z tym przyjęcie unijnego pakietu ochrony danych;

Wtorek, 8 września 2015 r.

R. mając na uwadze, że stawką są w tym przypadku dalekosiężne interesy społeczne, takie jak ochrona praw podstawowych, które nie powinny zależeć wyłącznie od rynku, lecz wymagają regulacji;

S. mając na uwadze, że przestrzeganie praw podstawowych i zasad praworządności oraz skuteczny nadzór parlamentarny nad służbami wywiadowczymi korzystającymi z cyfrowych technologii nadzoru to ważny element współpracy międzynarodowej;

T. mając na uwadze, że przedsiębiorstwa z siedzibą w UE mają znaczny udział w światowym rynku technologii informacyjno-komunikacyjnych, zwłaszcza jeśli chodzi o wywóz technologii służących do nadzoru, śledzenia, naruszania prywatności i monitoringu;

U. mając na uwadze, że wprowadzenie kontroli wywozu nie powinno mieć negatywnego wpływu na uzasadnione badania nad bezpieczeństwem teleinformatycznym ani na opracowywanie narzędzi zapewniających takie bezpieczeństwo, nieprowadzone w celach przestępczych;

1. uznaje, że prawa człowieka i podstawowe wolności są powszechne i muszą być chronione na całym świecie, niezależnie od tego, w jakiej formie się wyrażają; podkreśla, że nadzorowanie komunikacji samo w sobie stanowi ingerencję w prawo do prywatności i wypowiedzi, jeżeli taki nadzór wykracza poza odpowiednie ramy prawne;

2. wzywa Komisję do zapewnienia spójności między działaniami zewnętrznymi UE a jej wewnętrzną polityką dotyczącą technologii informacyjno-komunikacyjnych;

3. uważa, że ujawniony przez Edwarda Snowdena aktywny współudział niektórych państw członkowskich UE w masowej inwigilacji obywateli i szpiegowaniu przywódców politycznych przez NSA poważnie zaszkodził wiarygodności unijnej polityki praw człowieka i podważył globalne zaufanie do korzyści płynących z technologii informacyjno-komunikacyjnych;

4. przypomina państwom członkowskim i zainteresowanym agencjom UE, w tym Europolowi i Eurojustowi, o obowiązkach nałożonych na nie w Karcie praw podstawowych Unii Europejskiej oraz o obowiązku przestrzegania międzynarodowego prawa praw człowieka i celów polityki zewnętrznej UE, co oznacza nieudostępnianie danych wywiadowczych, które mogą prowadzić do łamania praw człowieka w państwie trzecim, i niewykorzystywanie informacji uzyskanych na skutek złamania praw człowieka, takiego jak bezprawny nadzór, poza granicami UE;

5. podkreśla, że wpływ technologii na poprawę przestrzegania praw człowieka powinien być uwzględniany we wszystkich stosownych dziedzinach polityki i programach UE, aby propagować ochronę praw człowieka oraz zasady demokracji, praworządności i dobrych rządów, jak również pokojowe rozwiązywanie konfliktów;

6. wzywa do aktywnego rozwijania i rozpowszechniania technologii, które pomagają chronić prawa człowieka i ułatwiają korzystanie z praw i wolności cyfrowych oraz bezpieczeństwa, jednocześnie propagując najlepsze praktyki i odpowiednie ramy prawne, a zarazem gwarantują bezpieczeństwo i nienaruszalność danych osobowych; wzywa UE i państwa członkowskie w szczególności, by aktywnie wspierały wykorzystywanie i rozwijanie na świecie otwartych standardów oraz wolnego i opartego na otwartych źródłach oprogramowania i technologii kryptograficznych;

7. wzywa UE do zwiększenia wsparcia dla podmiotów działających na rzecz poprawy bezpieczeństwa i standardów ochrony prywatności w technologiach informacyjno-komunikacyjnych na wszystkich poziomach, w tym standardów dotyczących sprzętu komputerowego, oprogramowania i komunikacji, jak również opracowywania sprzętu komputerowego i oprogramowania zgodnie z zasadą uwzględniania prywatności na etapie projektowania;

8. wzywa do utworzenia funduszu na rzecz praw człowieka i technologii w ramach Europejskiego Instrumentu na rzecz Wspierania Demokracji i Praw Człowieka (EIDHR);

9. wzywa samą UE, a w szczególności Europejską Służbę Działań Zewnętrznych (ESDZ), do stosowania technologii szyfrowania w komunikacji z obrońcami praw człowieka, aby uniknąć ich narażania i chronić własną komunikację z podmiotami zewnętrznymi przed inwigilacją;

10. wzywa UE, by przyjęła wolne i oparte na otwartych źródłach oprogramowanie oraz by zachęcała do tego inne podmioty, ponieważ tego typu oprogramowanie zapewnia większe bezpieczeństwo i większe poszanowanie praw człowieka;

11. zwraca uwagę na znaczenie rozwoju technologii informacyjno-komunikacyjnych na obszarach dotkniętych konfliktami z myślą o wspieraniu działań na rzecz budowania pokoju przez zapewnienie bezpiecznej komunikacji między stronami zaangażowanymi w pokojowe rozwiązywanie konfliktów;

12. wzywa do wdrożenia warunków, wskaźników i procedur sprawozdawczych służących zapewnieniu, że wsparcie finansowe i techniczne UE przeznaczone na rozwój nowych technologii w państwach trzecich nie jest wykorzystywane w sposób stanowiący łamanie praw człowieka;

13. wzywa Komisję i Radę, by aktywnie współpracowały z rządami państw trzecich oraz by wykorzystały istniejące europejskie mechanizmy wsparcia i instrumenty polityczne do wspierania, szkolenia i umacniania pozycji obrońców praw człowieka, działaczy społeczeństwa obywatelskiego i niezależnych dziennikarzy w bezpieczny sposób wykorzystujących w swoich działaniach technologie informacyjno-komunikacyjne, a także by propagowały powiązane prawa podstawowe, takie jak nieograniczony dostęp do informacji w internecie, prawo do prywatności i ochrony danych osobowych, wolność wypowiedzi, wolność zgromadzeń i stowarzyszeń oraz wolność prasy i wolność publikowania informacji w internecie;

14. zwraca uwagę na trudną sytuację osób zgłaszających przypadki naruszenia i ich zwolenników, w tym dziennikarzy, po ogłoszeniu doniesień o nieuczciwych praktykach nadzorczych w państwach trzecich; uważa, że takie osoby powinny być uznawane za obrońców praw człowieka, co oznacza, że zasługują one na ochronę ze strony UE, zgodnie z wytycznymi UE w sprawie obrońców praw człowieka; ponawia apel do Komisji i państw członkowskich o szczegółowe rozpatrzenie możliwości przyznania osobom zgłaszającym przypadki naruszeń międzynarodowej ochrony przed ściganiem;

15. ubolewa, że środki bezpieczeństwa, w tym środki służące do walki z terroryzmem, są coraz częściej wykorzystywane jako pretekst do naruszania prawa do prywatności i do ograniczania uzasadnionych działań obrońców praw człowieka, dziennikarzy i działaczy politycznych; ponownie wyraża zdecydowane przekonanie, że bezpieczeństwo narodowe nie może nigdy uzasadniać programów nieukierunkowanej, tajnej lub masowej inwigilacji; apeluje, by takie środki były realizowane w ścisłej zgodności z zasadami praworządności i standardami praw człowieka, w tym z prawem do prywatności i ochrony danych;

16. wzywa ESDZ i Komisję, by w politycznym dialogu z państwami trzecimi oraz w programach współpracy rozwojowej propagowała demokratyczny nadzór nad służbami bezpieczeństwa i służbami wywiadowczymi; wzywa Komisję do wspierania organizacji społeczeństwa obywatelskiego i organów ustawodawczych w państwach trzecich działających na rzecz wzmocnienia kontroli, przejrzystości i odpowiedzialności krajowych służb bezpieczeństwa; wzywa do ujęcia konkretnych zobowiązań w tym zakresie w przyszłym planie działań UE na rzecz praw człowieka i demokratyzacji;

17. wzywa Radę i Komisję, by we wszystkich formach kontaktu z państwami trzecimi, w tym w ramach negocjacji akcesyjnych, negocjacji handlowych, dialogów dotyczących praw człowieka i w kontaktach dyplomatycznych, propagowały wolności cyfrowe i nieograniczony dostęp do internetu;

18. zauważa, że internet stał się przestrzenią publiczną i miejscem prowadzenia handlu, którego nieodłącznymi elementami są swobodny przepływ informacji i dostęp do technologii informacyjno-komunikacyjnych; podkreśla w związku z tym, że należy jednocześnie propagować i chronić wolności cyfrowe i wolny handel;

19. apeluje, by do wszystkich porozumień z państwami trzecimi włączano klauzule warunkowości jednoznacznie odnoszące się do konieczności propagowania, gwarantowania i poszanowania wolności cyfrowych, neutralności sieci, niecenzurowanego i nieograniczonego dostępu do internetu, prawa do prywatności i ochrony danych;

20. wzywa UE, by przeciwdziałała uznawaniu za przestępstwo stosowania przez obrońców praw człowieka technologii kryptograficznych, narzędzi pomijania cenzury i narzędzi ochrony prywatności, odmawiając ograniczania stosowania technologii kryptograficznych na terytorium UE, oraz by kwestionowała postępowanie rządów państw trzecich, które stawiają takie obrońcom praw człowieka;

21. wzywa UE, by przeciwdziałała uznawaniu za przestępstwo stosowania przez obrońców praw człowieka technologii kryptograficznych, narzędzi pomijania cenzury i narzędzi ochrony prywatności, odmawiając ograniczania stosowania technologii kryptograficznych na terytorium UE, oraz by kwestionowała postępowanie rządów państw trzecich, które uznają stosowanie takich narzędzi za przestępstwo;

22. podkreśla, że skuteczna polityka rozwojowa UE i polityka w dziedzinie praw człowieka wymaga upowszechnienia technologii informacyjno-komunikacyjnych i wyeliminowanie przepaści cyfrowej przez zapewnienie podstawowej infrastruktury technologicznej i ułatwienie dostępu do wiedzy i informacji z myślą o propagowaniu umiejętności cyfrowych, a w stosownych przypadkach również przez propagowanie stosowania otwartych standardów w dokumentach oraz wolnego i opartego na otwartych standardach oprogramowania, by zapewnić otwartość i przejrzystość (zwłaszcza w instytucjach publicznych) – w tym ochronę danych w sferze cyfrowej na całym świecie – oraz lepsze zrozumienie potencjalnych niebezpieczeństw i korzyści płynących z technologii informacyjno-komunikacyjnych;

23. apeluje do Komisji o wspieranie likwidacji barier cyfrowych, jakie muszą pokonywać osoby niepełnosprawne; uznaje za niezwykle ważne, by polityka rozwojowa UE i jej polityka w dziedzinie rozwoju i promocji praw człowieka na świecie zmierzały do zmniejszenia wykluczenia cyfrowego osób niepełnosprawnych oraz do oferowania szerszego zakresu praw, zwłaszcza jeśli chodzi o dostęp do wiedzy, udział w świecie cyfrowym i dostęp do nowych możliwości ekonomicznych i społecznych oferowanych przez internet;

24. podkreśla, że zgodne z prawem cyfrowe gromadzenie i rozpowszechnianie dowodów na łamanie praw człowieka może się przyczynić do ogólnoświatowej walki z bezkarnością i terroryzmem; jest zdania, że w przypadkach należycie uzasadnionych na mocy międzynarodowego prawa (karnego) materiały takie powinny być dopuszczane jako dowody w postępowaniach sądowych, zgodnie z międzynarodowymi, regionalnymi i konstytucyjnymi klauzulami ochronnymi; zaleca ustanowienie w dziedzinie międzynarodowego prawa karnego mechanizmów wprowadzania procedur potwierdzania i zbierania takich danych o celów dowodowych w postępowaniach sądowych;

25. wyraża ubolewanie, że niektóre technologie i usługi informacyjno-komunikacyjne wytworzone w UE są sprzedawane i mogą być wykorzystywane w państwach trzecich przez osoby prywatne, przedsiębiorstwa i władze do łamania praw człowieka przez cenzurę, masowy nadzór, zagłuszanie, przechwytywanie, monitorowanie, lokalizowanie i śledzenie obywateli i ich działań w sieciach telefonii (komórkowej) i internecie; jest zaniepokojony faktem, że niektóre przedsiębiorstwa z siedzibą w UE dostarczają być może technologii i świadczą usługi umożliwiające tego rodzaju łamanie praw człowieka;

26. zauważa, że zagrożenia dla bezpieczeństwa Unii Europejskiej, jej państw członkowskich i państw trzecich często pochodzą od pojedynczych osób lub małych grup korzystających z sieci komunikacji cyfrowej do planowania i przeprowadzania ataków, a narzędzia i taktyki niezbędne do obrony przed takimi zagrożeniami wymagają nieustannych przeglądów i aktualizacji;

27. uważa, że masowy nadzór nieuzasadniony zwiększonym ryzykiem ataków i zagrożeń terrorystycznych narusza zasady konieczności i proporcjonalności, a zatem stanowi złamanie praw człowieka;

28. wzywa państwa członkowskie do propagowania pełnego nadzoru demokratycznego nad działaniami służb wywiadowczych w państwach trzecich oraz do sprawdzania, czy służby te działają przy pełnym poszanowaniu zasad praworządności, i do pociągania do odpowiedzialności służb i osób działających niezgodnie z prawem;

29. zachęca państwa członkowskie, by wobec zwiększonej współpracy i wymiany informacji między państwami członkowskimi a państwami trzecimi (w tym z wykorzystaniem cyfrowych środków nadzoru) zagwarantowały demokratyczną kontrolę nad takimi służbami i ich działaniami przez odpowiedni wewnętrzny nadzór ze strony władz wykonawczych i sądowniczych oraz niezależnych organów parlamentarnych;

30. podkreśla, że w prawie UE należy przyjąć zasady społecznej odpowiedzialności przedsiębiorstw i kryteria dotyczące projektowania z uwzględnieniem praw człowieka jako innowacyjne rozwiązania techniczne umożliwiające ochronę praw człowieka, aby zapewnić, że dostawcy usług internetowych, twórcy oprogramowania, producenci sprzętu, usługi i media społecznościowe, operatorzy telefonii komórkowej oraz inne podmioty będą uwzględniały prawa człowieka przynależne użytkownikom końcowym na całym świecie;

31. wzywa UE do zapewnienia większej przejrzystości w relacjach między operatorami telefonii komórkowej lub dostawcami usług internetowych a rządami, a także do apelowania o to w stosunkach z państwami trzecimi, przez wymaganie od operatorów i dostawców usług internetowych corocznego publikowania szczegółowych sprawozdań na temat przejrzystości, w tym sprawozdań dotyczących działań nakazanych przez władze, jak również powiązań finansowych między organami publicznymi a operatorami i dostawcami usług internetowych;

32. przypomina przedsiębiorcom o odpowiedzialności za przestrzeganie praw człowieka w działaniach prowadzonych na całym świecie, niezależnie od tego, gdzie są zlokalizowani ich użytkownicy i czy państwo przyjmujące wypełnia własne zobowiązania w zakresie praw człowieka; wzywa przedsiębiorstwa z sektora technologii informacyjno-komunikacyjnych, szczególnie przedsiębiorstwa mające siedzibę na terytorium UE, do wdrożenia wytycznych ONZ dotyczących biznesu i praw człowieka, w tym przez wprowadzenie polityki należytej staranności i mechanizmów ochronnych dotyczących zarządzania ryzykiem, a także przez zapewnienie skutecznych środków zaradczych na wypadek, gdyby ich działania spowodowały naruszenie praw człowieka lub przyczyniły się do niego;

33. podkreśla konieczność skuteczniejszego wdrożenia i monitorowania unijnych regulacji i sankcji dotyczących technologii informacyjno-komunikacyjnych, w tym wykorzystania mechanizmów uniwersalnych, aby zapewnić, że wszystkie strony, w tym państwa członkowskie przestrzegały prawodawstwa i by utrzymano równe warunki działania;

34. podkreśla, że poszanowanie praw podstawowych jest niezbędnym elementem skutecznej polityki antyterrorystycznej, w tym stosowania cyfrowych technologii nadzoru;

35. z zadowoleniem przyjmuje postanowienia Porozumienia z Wassenaar z grudnia 2013 r. w sprawie kontroli wywozu narzędzi służących do nadzoru, egzekwowania prawa i zbierania informacji wywiadowczych oraz sieciowych systemów nadzoru; przypomina, że unijny system dotyczący produktów o podwójnym zastosowaniu, zwłaszcza rozporządzenie UE w tej sprawie, są nadal bardzo niepełne, jeśli chodzi o skuteczną i systematyczną kontrolę wywozu szkodliwych technologii informacyjno-komunikacyjnych do państw niedemokratycznych;

36. w kontekście nadchodzącego przeglądu i aktualizacji polityki dotyczącej technologii podwójnego zastosowania wzywa Komisję do szybkiego przedstawienia wniosku dotyczącego inteligentnej i skutecznej polityki ograniczania i regulacji komercyjnego wywozu usług związanych z wdrażaniem i stosowaniem tzw. technologii podwójnego zastosowania, uwzględniającej potencjalnie szkodliwy wywóz produktów i usług informacyjno-komunikacyjnych do państw trzecich, zgodnie z uzgodnieniami zawartymi we wspólnym oświadczeniu Parlamentu Europejskiego, Rady i Komisji z kwietnia 2014 r.; wzywa Komisję do ujęcia w tej polityce skutecznych środków ochronnych, by takie kontrole wywozu nie zaszkodziły badaniom, w tym badaniom naukowym i badaniom w obszarze bezpieczeństwa teleinformatycznego;

37. podkreśla, że Komisja powinna w krótkim czasie być w stanie przekazywać przedsiębiorstwom mającym wątpliwości, czy powinny złożyć wniosek o wydanie pozwolenia na wywóz, aktualne informacje o legalności lub potencjalnie szkodliwych skutkach ewentualnych transakcji;

38. wzywa Komisję do przedłożenia wniosków dotyczących przeglądu metod wykorzystywania norm UE dotyczących technologii informacyjno-komunikacyjnych do zapobiegania potencjalnie szkodliwym skutkom wywozu takich technologii lub innych usług do państw trzecich, w których pojęć takich, jak „uprawnione przechwytywanie", nie można uznać za równoważne z pojęciami stosowanymi przez Unię Europejską, lub np. w przeszłości nie przestrzegano praw człowieka albo nie są stosowane zasady praworządności;

39. ponownie stwierdza, że standardy unijne, w szczególności Karta praw podstawowych Unii Europejskiej, powinny mieć decydujące znaczenie w ocenie przypadków wykorzystywania technologii podwójnego zastosowania w sposób, który może ograniczać prawa człowieka;

40. wzywa do opracowania polityki umożliwiającej regulację sprzedaży programów wykorzystujących słabości i błędy „zero-day exploit", aby uniknąć wykorzystywania ich do cyberataków lub uzyskiwania nieuprawnionego dostępu do urządzeń, prowadzącego do łamania praw człowieka, przy czym regulacje takie nie mogą mieć istotnego wpływu na prowadzone w uczciwych zamiarach badania naukowe i inne nadania nad bezpieczeństwem;

41. ubolewa, że niektóre europejskie i międzynarodowe przedsiębiorstwa działające w UE, które handlują technologiami podwójnego zastosowania mającymi potencjalnie szkodliwy wpływ na poszanowanie praw człowieka, aktywnie współpracują z reżimami łamiącymi prawa człowieka;

42. z naciskiem wzywa Komisję, by publicznie wykluczyła przedsiębiorstwa angażujące się w takie działania z unijnych procedur przetargowych, finansowania badań i rozwoju i wszelkich innych form wsparcia finansowego;

43. wzywa Komisję do zwrócenia szczególnej uwagi na aspekt praw człowieka w procedurach zamówień publicznych na sprzęt technologiczny, szczególnie w państwach stosujących niewiarygodne praktyki w tej dziedzinie;

44. wzywa Komisję i Radę, by na forach zarządzania internetem aktywnie broniły otwartego internetu, wielostronnych procedur decyzyjnych, neutralności internetu, wolności cyfrowych i gwarancji ochrony danych osobowych w państwach trzecich;

45. potępia osłabianie oraz podważanie protokołów i produktów kryptograficznych, zwłaszcza przez służby wywiadowcze chcące przechwytywać zaszyfrowane informacje;

46. przestrzega przed prywatyzacją egzekwowania prawa przez przedsiębiorstwa internetowe i dostawców usług internetowych;

47. wzywa do doprecyzowania norm i standardów stosowanych przed podmioty prywatne przy opracowywaniu ich systemów;

48. przypomina o znaczeniu oceny kontekstu, w jakim wykorzystywane są technologie, dla dokonania pełnej oceny ich wpływu na poszanowanie praw człowieka;

49. jednoznacznie wzywa do propagowania narzędzi umożliwiających anonimowe korzystanie z internetu lub używanie pseudonimu oraz kwestionuje jednostronny pogląd, zgodnie z którym takie narzędzia umożliwiają tylko prowadzenie działań przestępczych, a nie wzmacniają pozycji osób działających na rzecz praw człowieka w UE i poza jej granicami;

50. wzywa Radę, Komisję i ESDZ do opracowania inteligentnej i skutecznej polityki regulującej wywóz technologii podwójnego zastosowania i dotyczącej potencjalnie szkodliwego wywozu produktów i usług informacyjno-komunikacyjnych, na szczeblu międzynarodowym, w wielostronnych systemach kontroli wywozu i w innych organach międzynarodowych;

51. podkreśla, że wszelkie zmiany regulacyjne mające na celu zwiększenie skuteczności kontroli wywozu w odniesieniu do transferu niematerialnych technologii nie mogą ograniczać uzasadnionych badań ani dostępu do informacji i ich wymiany oraz że wszelkie potencjalne działania, np. stosowanie generalnych wspólnotowych zezwoleń na wywóz w przypadku badań nad produktami podwójnego zastosowania, nie powinny wywierać efektu zniechęcającego w stosunku do osób prywatnych oraz małych i średnich przedsiębiorstw (MŚP);

52. wzywa państwa członkowskie do zapewnienia, że obecna i przyszła polityka kontroli wywozu nie będzie ograniczać działań naukowców prowadzących zasadne badania nad bezpieczeństwem, a kontrole wywozu będą prowadzone w dobrej wierze i wyłącznie w odniesieniu do jasno określonych technologii wykorzystywanych do masowej inwigilacji, cenzury, zagłuszania, przechwytywania informacji, monitorowania oraz śledzenia i lokalizowania obywateli i ich działań w sieciach telefonii (komórkowej);

53. przypomina, że bezprzewodowe technologie komunikacji w topologii siatki mają wysoki potencjał jako sieci zabezpieczające na obszarach, gdzie dostęp do internetu jest nieosiągalny lub zablokowany, i mogą pomóc w propagowaniu praw człowieka;

54. wzywa Komisję do powołania niezależnej grupy ekspertów mogących przeprowadzić ocenę wpływu istniejących norm UE w dziedzinie technologii informacyjno-komunikacyjnych na wykonywanie praw człowieka w celu sformułowania zaleceń dotyczących dostosowań, które zwiększą ochronę praw człowieka, szczególnie w przypadku wywozu systemów;

55. uznaje, że rozwój technologiczny stanowi wyzwanie dla systemów prawnych, które należy dostosować do nowych okoliczności; podkreśla, że podmioty kształtujące prawo powinny zwracać większą uwagę na kwestie związane z gospodarką cyfrową;

56. wzywa Komisję do zaangażowania społeczeństwa obywatelskiego i niezależnych ekspertów ds. technologii informacyjno-komunikacyjnych, w tym naukowców zajmujących się sprawami bezpieczeństwa, aby zapewnić dostęp do aktualnej wiedzy fachowej, co powinno umożliwić kształtowanie przyszłościowej polityki;

57. podkreśla konieczność unikania niezamierzonych konsekwencji, takich jak ograniczanie naukowych i innych działań badawczo-rozwojowych prowadzonych w dobrej wierze, wymiany informacji i dostępu do nich, opracowywania wiedzy o technologiach służących zdobywaniu koniecznych kompetencji cyfrowych i propagowaniu praw człowieka lub wywozu takich technologii, albo zniechęcanie do takich działań;

58. uważa, że współpraca między rządami a podmiotami prywatnymi w domenie cyfrowej na całym świecie, w tym Forum Zarządzania Internetem, wymaga wyraźnej kontroli i równowagi i nie może prowadzić do podważania nadzoru demokratycznego i sądowniczego;

59. zauważa, że podejście dobrowolne nie jest wystarczające i że należy wprowadzić wiążące środki, by zachęcić przedsiębiorstwa do uwzględnienia praktyk danego państwa w dziedzinie praw człowieka, zanim sprzedadzą mu swoje produkty, oraz do przeprowadzenia oceny wpływu ich technologii na sytuację obrońców praw człowieka i osób krytykujących rząd;

60. jest zdania, że należy sprawdzać wywóz towarów szczególnie newralgicznych, zanim opuszczą one terytorium UE, oraz że niezbędne są sankcje na wypadek naruszeń;

61. apeluje o przyznanie każdej osobie prawa do szyfrowania informacji oraz o stworzenie niezbędnych warunków umożliwiających szyfrowanie; uważa, że kontrola powinna leżeć w gestii użytkownika końcowego, który powinien mieć umiejętności niezbędne do właściwego przeprowadzenia takiej kontroli;

62. apeluje o wdrożenie kompleksowych standardów szyfrowania i o uznanie ich za normę we wszystkich usługach komunikacyjnych, aby utrudnić rządom, służbom wywiadowczym i organom nadzoru odczyt treści komunikatów;

63. podkreśla szczególną odpowiedzialność służb wywiadowczych za budowanie zaufania i wzywa do zaprzestania masowej inwigilacji; uważa, że trzeba zająć się problemem inwigilacji obywateli europejskich przez wewnętrzne i zewnętrzne służby wywiadowcze i położyć jej kres;

64. sprzeciwia się sprzedaży i rozpowszechnianiu europejskich technologii nadzoru i narzędzi cenzury w państwach o ustroju autorytarnym, w których nie obowiązują zasady praworządności;

65. apeluje o umożliwienie osobom zgłaszającym przypadki nadużyć skorzystania z ochrony międzynarodowej i zachęca państwa członkowskie do przedstawienia projektów przepisów dotyczących ochrony takich osób;

66. apeluje o mianowanie przedstawiciela ONZ ds. wolności cyfrowych i ochrony danych oraz wzywa do rozszerzenia zakresu działań Europejskiego Rzecznika Praw Człowieka, by również na technologie spojrzano z punktu widzenia praw człowieka;

67. apeluje o przyjęcie środków gwarantujących ochronę prywatności działaczy, dziennikarzy i obywateli na całym świecie oraz zapewniających im możliwość podłączenia się do internetu;

68. podkreśla, że należy uznać dostęp do internetu za prawo człowieka, i apeluje o przyjęcie środków mających na celu wyeliminowanie przepaści cyfrowej;

69. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie, Komisji, wiceprzewodniczącej Komisji/wysokiej przedstawiciel Unii Europejskiej do spraw zagranicznych i polityki bezpieczeństwa oraz ESDZ.