Dinsdag 8 september 2015

P8_TA(2015)0288

Mensenrechten en technologie in derde landen

Resolutie van het Europees Parlement van 8 september 2015 over mensenrechten en technologie: het effect van inbreuk- en bewakingssystemen op de mensenrechten in derde landen (2014/2232(INI))

(2017/C 316/03)

Het Europees Parlement,

— gezien de Universele Verklaring van de Rechten van de Mens en het Internationaal Verdrag inzake burgerrechten en politieke rechten, met name artikel 19,

— gezien het strategisch EU-kader voor mensenrechten en democratie, aangenomen door de Raad op 25 juni 2012 ([1]),

— gezien de EU-mensenrechtenrichtsnoeren inzake vrijheid van meningsuiting online en offline, die op 12 mei 2014 ([2]) door de Raad Buitenlandse Zaken zijn vastgesteld,

— gezien de door de Commissie in juni 2013 gepubliceerde Gids voor de ICT-sector betreffende de toepassing van de leidende beginselen van de VN op het gebied van zakendoen en mensenrechten („ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights"),

— gezien het verslag van de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) van 15 december 2011 over de vrijheid van meningsuiting op het internet ([3]) en het regelmatige verslag van de speciale vertegenwoordiger van de OVSE voor de vrijheid van de media aan de Permanente Raad van de OVSE van 27 november 2014 ([4]),

— gezien het verslag van de speciale rapporteur van de VN van 23 september 2014 over het bevorderen en beschermen van mensenrechten en fundamentele vrijheden bij terrorismebestrijding (A/69/397) ([5]),

— gezien het verslag van het Bureau van de hoge commissaris van de VN voor de mensenrechten van 30 juni 2014 met als titel „Het recht op privacy in het digitale tijdperk" ([6]),

— gezien het verslag van de speciale rapporteur inzake de bevordering en bescherming van het recht op vrijheid van mening en meningsuiting van 17 april 2013 (A/HRC/23/40) met een analyse van de gevolgen van het aftappen van communicatie door staten voor de uitoefening van de rechten van de mens op privacy en op vrijheid van mening en meningsuiting,

— gezien het verslag van de Commissie juridische zaken en mensenrechten van de Parlementaire Vergadering van de Raad van Europa van 26 januari 2015 over grootschalig toezicht ([7]),

— gezien zijn resolutie van 12 maart 2014 over het surveillanceprogramma van de NSA in de VS, toezichthoudende instanties in verschillende lidstaten en gevolgen voor de grondrechten van EU-burgers en voor de trans-Atlantische samenwerking op het gebied van justitie en binnenlandse zaken ([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]) Aangenomen teksten, P7_TA(2014)0230.

— gezien het verslag van 21 maart 2011 van de bijzondere rapporteur van de VN over mensenrechten en transnationale ondernemingen en andere bedrijven, met als titel „Guiding Principles on Business and Human Rights: Implementing the United Nations „Protect, Respect and Remedy" Framework" ([1]),

— gezien de OESO-richtlijnen voor multinationale ondernemingen ([2]) en het jaarverslag 2014 over de OESO-richtlijnen voor multinationale ondernemingen ([3]),

— gezien het jaarverslag 2013 van de Internet Corporation for Assigned Names and Numbers ([4]),

— gezien de mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's van 12 februari 2014 met als titel „Internetbeleid en -governance: De rol van Europa bij het vormgeven van de toekomst van internetgovernance" ([5]),

— gezien de verklaring van de multistakeholderbijeenkomst van NetMundial, aangenomen op 24 april 2014 ([6]),

— gezien de samenvatting van de voorzitter van het 9e Forum voor internetbeheer, dat van 2 tot 5 september 2014 in Istanbul werd gehouden,

— gezien de beperkende maatregelen van de Europese Unie, waarvan sommige embargo's op telecommunicatieapparatuur, informatie- en communicatietechnologieën (ICT's) en toezichtsinstrumenten bevatten,

— gezien Verordening (EU) nr. 599/2014 van het Europees Parlement en de Raad van 16 april 2014 tot wijziging van Verordening (EG) nr. 428/2009 van de Raad tot instelling van een communautaire regeling voor controle op de uitvoer, de overbrenging, de tussenhandel en de doorvoer van producten voor tweeërlei gebruik ([7]),

— gezien de Gemeenschappelijke verklaring van 16 april 2014 van het Europees Parlement, de Raad en de Commissie over de toetsing van het controlesysteem voor de uitvoer van producten voor tweeërlei gebruik ([8]),

— gezien de besluiten van de 19e plenaire vergadering in het kader van de Overeenkomst van Wassenaar betreffende exportcontrole voor conventionele wapens en goederen en technologieën voor tweeërlei gebruik, gehouden te Wenen op 3 en 4 december 2013,

— gezien de mededeling van de Commissie aan de Raad en het Europees Parlement van 24 april 2014 met als titel „De herziening van het uitvoercontrolebeleid: waarborgen van veiligheid en concurrentievermogen in een veranderende wereld" ([9]),

— gezien de conclusies van de Raad van 21 november 2014 over de herziening van het uitvoercontrolebeleid,

— gezien zijn resolutie van 11 december 2012 over een strategie voor digitale vrijheid in het buitenlandbeleid van de EU ([10]),

---

([1]) http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN. pdf?v=1392752313000/_/jcr:system/jcr:versionstorage/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]) PB L 173 van 12.6.2014, blz. 79.

([8]) PB L 173 van 12.6.2014, blz. 82.

([9]) COM(2014)0244.

([10]) Aangenomen teksten, P7_TA(2012)0470.

Dinsdag 8 september 2015

— gezien zijn resolutie van 13 juni 2013 over de vrijheid van pers en media in de wereld ([1]),

— gezien zijn spoedresoluties over gevallen van schending van de mensenrechten, de democratie en de rechtstaat waarin kwesties met betrekking tot digitale vrijheden worden aangekaart,

— gezien zijn resolutie van 12 maart 2015 over de prioriteiten van de EU voor de VN-Mensenrechtenraad in 2015 ([2]),

— gezien zijn resolutie van 11 februari 2015 over de verlenging van het mandaat van het Forum voor internetbeheer ([3]),

— gezien zijn resolutie van 12 maart 2015 over het jaarverslag over de mensenrechten in de wereld in 2013 en het mensenrechtenbeleid van de Europese Unie ([4]),

— gezien de schriftelijke verklaring van Edward Snowden voor de LIBE-commissie in maart 2014 ([5]),

— gezien het Europees Verdrag tot bescherming van de rechten van de mens en de lopende onderhandelingen over de toetreding van de EU tot dat verdrag,

— gezien het Handvest van de grondrechten van de Europese Unie,

— gezien artikel 52 van zijn Reglement,

— gezien het verslag van de Commissie buitenlandse zaken (A8-0178/2015),

A. overwegende dat technologische ontwikkelingen en toegang tot het open internet een steeds belangrijkere rol spelen voor het mogelijk maken en het waarborgen van de naleving en de volledige eerbiediging van de mensenrechten en fundamentele vrijheden, en een positief effect hebben door de reikwijdte van de vrijheid van meningsuiting, de toegang tot informatie, het recht op privacy en de vrijheid van vergadering en vereniging in de hele wereld te vergroten;

B. overwegende dat technologische systemen kunnen worden misbruikt als middel voor mensenrechtenschendingen door middel van censuur, toezicht, onwettige toegang tot apparaten, blokkeren, onderscheppen en het volgen en opsporen van informatie en personen;

C. overwegende dat publieke en private actoren, met inbegrip van regeringen en rechtshandhavingsorganen, en criminele organisaties en terroristische netwerken deze middelen gebruiken om de mensenrechten te schenden;

D. overwegende dat de context waarbinnen ICT's worden ontworpen en gebruikt, in grote mate bepaalt welk effect ze kunnen hebben als middel om de mensenrechten te bevorderen of te schenden; overwegende dat informatietechnologie, met name software, gewoonlijk geschikt is voor tweeërlei gebruik wat hun potentieel voor mensenrechtenschendingen betreft en dat software ook een vorm van meningsuiting is;

E. overwegende dat ICT's belangrijke instrumenten zijn geweest om mensen te helpen bij de organisatie van sociale bewegingen en protesten in tal van, vooral autoritair geregeerde, landen;

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

F. overwegende dat de beoordeling van de gevolgen voor mensenrechten van de context waarin technologieën worden gebruikt, bepaald wordt door de mate waarin het gebruik van technologieën door nationale en regionale wetgevingskaders wordt gereguleerd en de politieke en justitiële autoriteiten toezicht kunnen houden op dat gebruik;

G. overwegende dat private actoren een steeds belangrijkere rol spelen in het digitale domein op alle gebieden van maatschappelijke activiteiten, maar dat nog steeds niet in waarborgen is voorzien om te voorkomen dat zij de grondenrechten en fundamentele rechten te zeer inperken; overwegende dat private actoren daarom een actievere rol spelen bij de beoordeling van de rechtmatigheid van inhoud en bij de ontwikkeling van systemen voor cyberveiligheid en bewakingssystemen, die overal ter wereld een nadelig effect kunnen hebben voor de mensenrechten;

H. overwegende dat het internet een ware revolutie van de mogelijkheden voor de uitwisseling van gegevens, informatie en allerhande kennis heeft teweeggebracht;

I. overwegende dat versleuteling een belangrijke methode is die ertoe bijdraagt communicatie te beveiligen en de mensen die van communicatiemiddelen gebruik maken te beschermen;

J. overwegende dat internetbeheer gebaat is bij een besluitvormingsmodel waarbij een groot aantal stakeholders is betrokken, een proces dat een zinvolle, inclusieve en verantwoordelijke participatie van alle stakeholders, regeringen, maatschappelijke organisaties, technische en academische gemeenschappen, de particuliere sector en gebruikers waarborgt;

K. overwegende dat inlichtingendiensten cryptografische protocollen en -producten systematisch hebben ondermijnd om communicatie en gegevens te kunnen onderscheppen; overwegende dat de National Security Agency (NSA) van de VS in groten getale „zero-day exploits" heeft verzameld — zwakke punten in de IT-beveiliging die het publiek of de verkoper van het product nog niet bekend zijn; overwegende dat dergelijke activiteiten de mondiale inspanningen ter verbetering van de IT-beveiliging ondermijnen;

L. overwegende dat in de EU gevestigde inlichtingendiensten activiteiten hebben ontplooid die indruisen tegen de mensenrechten;

M. overwegende dat juridische en democratische controles en waarborgen sterk onderontwikkeld zijn in vergelijking tot de snelle ontwikkelingen die plaatsvinden op technologisch gebied;

N. overwegende dat maatregelen voor (cyber)beveiliging of terrorismebestrijding op het vlak van ICT en monitoring van het internet grote negatieve gevolgen kunnen hebben voor de mensenrechten in de hele wereld, met inbegrip van EU-burgers die in het buitenland wonen of naar het buitenland reizen, en in het bijzonder bij gebrek aan rechtsgrondslag, noodzaak, proportionaliteit en democratisch en juridisch toezicht;

O. overwegende dat internetfilters en de bewaking van communicatie het mensenrechtenverdedigers moeilijker maken het internet voor hun doeleinden te gebruiken en gevoelige informatie te communiceren, en dat zij indruisen tegen verschillende artikelen van de Universele verklaring van de rechten van de mens, die het recht van eenieder op privacy en vrije meningsuiting garandeert;

P. overwegende dat zowel digitale veiligheid als digitale vrijheid essentieel zijn en dat ze elkaars plaats niet kunnen innemen, maar elkaar moeten versterken;

Q. overwegende dat de Europese Unie op het vlak van digitale vrijheden alleen het voortouw kan nemen als deze vrijheden in de EU zelf worden gewaarborgd; overwegende dat het EU-gegevensbeschermingspakket daarom van cruciaal belang is;

Dinsdag 8 september 2015

R. overwegende dat verstrekkende maatschappelijke belangen op het spel staan, zoals de bescherming van de grondrechten, die niet enkel aan de markt moeten worden overgelaten, maar die gereguleerd moeten worden;

S. overwegende dat de eerbiediging van de mensenrechten en de rechtsstaat en een doeltreffende parlementaire controle op inlichtingendiensten die gebruik maken van digitale bewakingstechnologie belangrijke elementen van internationale samenwerking vormen;

T. overwegende dat in de EU gevestigde ondernemingen een belangrijk deel van de mondiale markt voor ICT's in handen hebben, met name wanneer het gaat om de uitvoer van bewakings-, tracerings-, inbreuk- en monitoringtechnologie;

U. overwegende dat de invoering van uitvoercontroles geen afbreuk mag doen aan legitiem onderzoek op het gebied van IT-beveiliging en de ontwikkeling van IT-beveiligingsinstrumenten wanneer criminele bedoelingen ontbreken;

1. erkent dat mensenrechten en fundamentele vrijheden universeel zijn en in alle uitingsvormen wereldwijd moeten worden verdedigd; benadrukt dat de bewaking van communicatie als zodanig in strijd is met het recht op privacy en vrije meningsuiting indien zij buiten een passend wetgevingskader om plaatsvindt;

2. roept de Commissie op te zorgen voor samenhang tussen het externe optreden van de EU en de eigen beleidslijnen met betrekking tot ICT's;

3. is van mening dat de actieve medeplichtigheid van bepaalde EU-lidstaten aan de grootschalige bewaking van burgers door de NSA en de spionage tegen politieke leiders, zoals door Edward Snowden onthuld werd, de geloofwaardigheid van het mensenrechtenbeleid van de EU ernstige schade hebben berokkend en het wereldwijde vertrouwen in de voordelen van ICT's hebben ondermijnd;

4. herinnert de lidstaten en de betrokken EU-agentschappen, waaronder Europol en Eurojust, aan hun verplichtingen uit hoofde van het Handvest van de grondrechten van de Europese Unie en in lijn met internationale mensenrechtenwetgeving en de EU-doelstellingen voor extern beleid, die hun verbieden inlichtingen te delen die schendingen van de mensenrechten in een derde land tot gevolg zouden kunnen hebben of informatie te gebruiken die verkregen is als gevolg van een schending van de mensenrechten, zoals illegale surveillance, buiten de EU;

5. benadrukt dat de impact van technologieën op de verbetering van de mensenrechten in alle EU-beleidsdomeinen en -programma's moet worden geïntegreerd om de bescherming van de mensenrechten en de promotie van de democratie, de rechtsstaat, goed beheer en vreedzame conflictoplossing te bevorderen;

6. vraagt technologieën die bijdragen tot de bescherming van de mensenrechten en de digitale rechten en vrijheden en de veiligheid van mensen vergemakkelijken, actief te ontwikkelen en te verspreiden, en goede praktijken en geschikte wetgevingskaders te bevorderen en tegelijk de veiligheid en integriteit van persoonlijke gegevens te waarborgen; dringt er bij de EU en haar lidstaten met name op aan het wereldwijde gebruik en de ontwikkeling van open standaarden en vrije en opensourcesoftware en cryptografische technologieën te bevorderen;

7. roept de EU op haar steun op te voeren voor actoren die werken aan de verscherping van de standaarden voor veiligheid en bescherming van de privacy in ICT's op alle niveaus, waaronder hardware, software en communicatiestandaarden evenals de ontwikkeling van de hardware en software in structuren met „ingebouwde privacy";

8. vraagt dat een fonds voor mensenrechten en technologie wordt opgericht uit hoofde van het Europees instrument voor democratie en mensenrechten;

9. dringt er bij de EU zelf en met name bij de EDEO op aan versleuteling te gebruiken in de communicatie met mensenrechtenverdedigers, om hen niet in gevaar te brengen en om de communicatie met buitenstaanders te beschermen tegen bewaking;

10. roept de EU op vrije en opensourcesoftware in gebruik te nemen en andere actoren aan te moedigen hetzelfde te doen, daar zulke software zorgt voor verbeterde veiligheid en een betere eerbiediging van de mensenrechten;

11. vestigt de aandacht op het belang van de ontwikkeling van ICT's in conflictgebieden ter bevordering van vredesopbouwactiviteiten, om veilige communicatie mogelijk te maken tussen partijen die betrokken zijn bij vreedzame conflictresolutie;

12. vraagt dat voorwaarden, maatstaven en verslagprocedures worden ingevoerd om te waarborgen dat de financiële en technische EU-steun voor de ontwikkeling van nieuwe technologieën in derde landen niet gebruikt wordt op een manier die de mensenrechten schendt;

13. roept de Commissie en de Raad op actief met regeringen van derde landen te communiceren en mensenrechtenverdedigers, activisten uit het maatschappelijk middenveld en onafhankelijke journalisten die bij hun activiteiten veilig gebruik maken van ICT's, met de bestaande Europese ondersteuningsmechanismen en beleidsinstrumenten verder te steunen, op te leiden en hen in staat te stellen een actievere rol te spelen, en de daaraan gerelateerde fundamentele privacyrechten te bevorderen, zoals de ongehinderde toegang tot de informatiestromen op het internet, het recht op privacy en gegevensbescherming, vrije meningsuiting, vrijheid van vergadering en vrijheid van vereniging en de vrijheid van pers en publicatie op het internet;

14. vestigt de aandacht op het lot van klokkenluiders en hun medestanders, waaronder journalisten, na hun onthullingen over misbruik van surveillancepraktijken in derde landen; is van mening dat deze personen moeten worden beschouwd als mensenrechtenverdedigers en als dusdanig aanspraak moeten kunnen maken op bescherming door de EU zoals vereist door de EU-richtsnoeren over mensenrechtenverdedigers; roept de Commissie en de lidstaten nogmaals op tot een grondig onderzoek van de mogelijkheid om klokkenluiders internationale bescherming tegen vervolging te bieden;

15. betreurt het dat veiligheidsmaatregelen, waaronder maatregelen voor terrorismebestrijding, steeds vaker gebruikt worden als excuus voor de schending van het recht op privacy en de beteugeling van legitieme activiteiten van mensenrechtenverdedigers, journalisten en politieke activisten; spreekt nogmaals zijn sterke overtuiging uit dat de nationale veiligheid nooit als rechtvaardiging mag dienen voor niet-gerichte, geheime of grootschalige toezichtsprogramma's; staat erop dat zulke maatregelen uitsluitend toegepast worden volgens de regels van de rechtsstaat en de mensenrechtennormen, waaronder het recht op privacy en gegevensbescherming;

16. roept de EDEO en de Commissie op om in de politieke dialoog met derde landen en in de programma's voor ontwikkelingssamenwerking op te komen voor het democratisch toezicht op veiligheids- en inlichtingendiensten; dringt er bij de Commissie op aan organisaties uit het maatschappelijk middenveld en wetgevende organen in derde landen die ernaar streven het toezicht op en de transparantie en verantwoordingsplicht van binnenlandse veiligheidsdiensten te verscherpen, te ondersteunen; vraagt dat specifieke verbintenissen daaromtrent opgenomen worden in het toekomstige EU-actieplan over mensenrechten en democratisering;

17. dringt er bij de Raad en de Commissie op aan in alle vormen van betrekkingen met derde landen (ook toetredingsonderhandelingen, handelsonderhandelingen, mensenrechtendialogen en diplomatieke contacten) op te komen voor digitale vrijheden en de onbeperkte toegang tot het internet;

18. erkent dat internet zowel een openbare ruimte is geworden als een marktplaats, waarvoor een vrije informatiestroom en de toegang tot ICT's onmisbaar zijn; benadrukt derhalve dat digitale vrijheid en vrije handel gelijktijdig moeten worden bevorderd en beschermd;

19. vraagt dat in alle overeenkomsten met derde landen clausules worden opgenomen waarin expliciet wordt verwezen naar de noodzaak om digitale vrijheden, netneutraliteit, ongecensureerde en onbeperkte toegang tot het internet, privacyrechten en gegevensbescherming te bevorderen, waarborgen en eerbiedigen;

Dinsdag 8 september 2015

20. dringt er bij de EU op aan in te gaan tegen de criminalisering van het gebruik door mensenrechtenverdedigers van versleuteling, censuurontduiking en privacyinstrumenten, door te weigeren het gebruik van versleuteling in de EU te beperken, en overheden van derde landen die mensenrechtenverdedigers hiervan beschuldigen daarop aan te spreken;

21. dringt er bij de EU op aan in te gaan tegen de criminalisering van het gebruik van versleuteling, anticensuur- en privacyinstrumenten, door te weigeren het gebruik van versleuteling in de EU te beperken en door overheden van derde landen die deze instrumenten criminaliseren daarop aan te spreken;

22. benadrukt dat voor een effectief EU-beleid inzake ontwikkeling en mensenrechten ICT's moeten worden gemainstreamd en de digitale kloof moet worden overbrugd, door te zorgen voor technologische basisinfrastructuur en door de toegang tot kennis en informatie te vereenvoudigen teneinde digitale geletterdheid te bevorderen en door het gebruik van open standaarden en vrije en opensourcesoftware, waar gepast, te bevorderen, teneinde openheid en transparantie te waarborgen (vooral door openbare instellingen) — met inbegrip van het waarborgen van gegevensbescherming op het digitale vlak in heel de wereld — alsook te zorgen voor een beter inzicht in de potentiële risico's en voordelen van ICT;

23. roept de Commissie op initiatieven te ondersteunen om digitale hindernissen voor mensen met een handicap weg te nemen; is van mening dat het zeer belangrijk is dat het beleid van de EU ten aanzien van de ontwikkeling en bevordering van mensenrechten in de wereld is gericht op het dichten van de digitale kloof voor mensen met een handicap en op het bieden van een ruimer rechtskader, met name wat betreft de toegang tot kennis, de digitale participatie en de ontsluiting van de nieuwe economische en sociale mogelijkheden die het internet biedt;

24. benadrukt dat de legale digitale verzameling en verspreiding van bewijsmateriaal van schendingen van de mensenrechten kan helpen om straffeloosheid en terrorisme te bestrijden; is van mening dat dit materiaal in naar behoren gemotiveerde gevallen ontvankelijk moet zijn als bewijsmateriaal in rechtszaken in het kader van het internationaal (straf) recht overeenkomstig internationale, regionale en grondwettelijke waarborgen; beveelt aan om op het gebied van internationaal strafrecht mechanismen te creëren voor de invoering van procedures via welke deze gegevens als bewijsmateriaal in rechtszaken voor echt worden verklaard en verzameld;

25. betreurt het dat sommige in de EU ontwikkelde informatie- en communicatietechnologieën en -diensten in derde landen worden verkocht en door privépersonen, bedrijven en overheden kunnen worden gebruikt met als specifiek doel de mensenrechten te schenden door censuur, grootschalig toezicht, blokkeren, onderscheppen, controles, en het traceren en opsporen van burgers en hun activiteiten op (mobiele) telefoonnetwerken en het internet; is bezorgd over het feit dat sommige in de EU gevestigde bedrijven technologieën en diensten leveren die deze mensenrechtenschendingen mogelijk maken;

26. merkt op dat bedreigingen voor de veiligheid van de Europese Unie, haar lidstaten en derde landen vaak afkomstig zijn van individuele personen of kleine groeperingen die digitale communicatienetwerken gebruiken voor het plannen en uitvoeren van aanvallen, en dat de instrumenten en strategieën die nodig zijn voor het wegnemen van dergelijke bedreigingen continu moeten worden herzien en bijgewerkt;

27. is van mening dat grootschalig toezicht dat niet wordt verantwoord door een verhoogd risico van terroristische aanvallen en dreiging in strijd is met de beginselen van noodzaak en proportionaliteit en daarom een schending van de mensenrechten;

28. dringt er bij de lidstaten op aan om volledige democratische controle over de verrichtingen van inlichtingendiensten in derde landen te bevorderen, alsmede te verifiëren dat deze diensten met volledig respect voor de wet handelen, en om de diensten en personen verantwoordelijk voor onwettige verrichtingen rekenschap te laten afleggen;

29. moedigt de lidstaten aan om in het licht van de toegenomen samenwerking en informatie-uitwisseling tussen lidstaten en derde landen — met inbegrip van het gebruik van digitaal toezicht — democratische controle van deze diensten en hun verrichtingen te waarborgen door middel van toepasselijk intern, uitvoerend, gerechtelijk en onafhankelijk parlementair toezicht;

30. benadrukt dat de beginselen van maatschappelijk verantwoord ondernemerschap en de criteria van mensenrechten „by design" (die technologische oplossingen en innovaties ter bescherming van de mensenrechten zijn) in EU-wetgeving moeten worden opgenomen om ervoor te zorgen dat aanbieders van internetdiensten, softwareontwikkelaars, hardwareproducenten, socialenetwerkdiensten/media, aanbieders van mobiele telefonie en andere rekening houden met de mensenrechten van eindgebruikers wereldwijd;

31. dringt er bij de EU op aan om grotere transparantie te waarborgen in de relatie tussen aanbieders van mobiele telefonie of internetaanbieders en overheden, en om hiertoe in haar relatie met derde landen op te roepen door van aanbieders van mobiele telefonie en internetaanbieders te eisen dat zij jaarlijks gedetailleerde transparantieverslagen publiceren, waaronder verslagen over door overheden aangevraagde handelingen, alsmede in de financiële banden tussen de overheid en aanbieders van mobiele telefonie/internetaanbieders;

32. herinnert bedrijven aan hun verantwoordelijkheid de mensenrechten te respecteren bij hun wereldwijde activiteiten, ongeacht de woonplaats van hun gebruikers en onafhankelijk van de vraag of de ontvangende staat voldoet aan zijn verplichting tot het respecteren van de mensenrechten; roept ICT-bedrijven, in het bijzonder bedrijven die in de EU zijn gevestigd, op om de richtsnoeren van de VN inzake bedrijfsleven en mensenrechten toe te passen, onder andere door het instellen van een beleid van gepaste zorgvuldigheid en voorzorgsmaatregelen voor risicobeheer, en door voor doeltreffende rechtsmiddelen te zorgen als hun activiteiten een negatief effect op de mensenrechten hebben gecreëerd of hiertoe hebben bijgedragen;

33. benadrukt dat EU-regelgeving en -sancties met betrekking tot ICT's, met inbegrip van vangnetregelingen, doeltreffender moeten worden toegepast en gemonitord, om ervoor te zorgen dat alle partijen, met inbegrip van de lidstaten, de wetgeving naleven en een gelijk speelveld wordt behouden;

34. benadrukt dat respect voor fundamentele rechten een essentieel onderdeel is van een geslaagd beleid inzake terrorismebestrijding, waaronder het gebruik van technologieën voor digitaal toezicht;

35. is verheugd over het besluit van de Overeenkomst van Wassenaar van december 2013 over de controle op uitvoer op het gebied van toezicht, ordehandhaving en instrumenten voor het verzamelen van informatie en systemen voor netwerkbewaking; herinnert aan de grote onvolledigheid van de EU-regeling voor producten voor tweeërlei gebruik, te weten de EU-verordening voor tweeërlei gebruik, als het gaat om de effectieve en systematische controle op uitvoer van schadelijke ICT-technologieën naar niet-democratische landen;

36. dringt er bij de Commissie op aan in de context van de toekomstige herziening en vernieuwing van het beleid inzake producten voor tweeërlei gebruik spoedig een voorstel te doen voor intelligente en doeltreffende beleidslijnen om de commerciële uitvoer van diensten op het gebied van de toepassing en het gebruik van zogenaamde technologieën voor tweeërlei gebruik te beperken en te reguleren, waarbij de mogelijk schadelijke gevolgen van de uitvoer van ICT-producten en -diensten naar derde landen worden aangepakt, zoals overeengekomen in de Gemeenschappelijke verklaring van april 2014 van het Europees Parlement, de Raad en de Commissie; roept de Commissie op om doeltreffende waarborgen op te nemen om te voorkomen dat deze controle op de uitvoer op enige wijze schade kan toebrengen aan onderzoek, met inbegrip van wetenschappelijk onderzoek en onderzoek op het gebied van IT-veiligheid;

37. benadrukt dat de Commissie bedrijven die erover twijfelen of ze een uitvoervergunning moeten aanvragen nauwkeurige en bijgewerkte informatie moet kunnen aanbieden over de wettigheid of de mogelijk schadelijke gevolgen van potentiële transacties;

38. vraagt de Commissie voorstellen te doen om te toetsen hoe EU-normen in verband met ICT's kunnen worden gebruikt om de mogelijk schadelijke gevolgen te voorkomen van de uitvoer van deze technologieën of diensten naar derde landen waar concepten als „legale interceptie" niet kunnen worden gezien als gelijkwaardig aan die van de Europese Unie, of die een slechte reputatie op het gebied van mensenrechten hebben of waar bijvoorbeeld de rechtsstaat niet bestaat;

39. bevestigt opnieuw dat EU-normen, in het bijzonder het Handvest van de grondrechten van de EU, moeten prevaleren bij de beoordeling van incidenten als er technologieën voor tweeërlei gebruik op zo'n manier worden ingezet dat zij de mensenrechten zouden kunnen beperken;

40. vraagt dat beleid wordt ontwikkeld om de verkoop van „zero-day exploits" en kwetsbaarheden te reglementeren om te vermijden dat deze worden gebruikt voor cyberaanvallen of voor onwettige toegang tot apparaten, waardoor mensenrechten kunnen worden geschonden zonder dat dergelijke verordeningen een effect hebben dat van grote betekenis is voor academisch en in ander opzicht betrouwbaar veiligheidsonderzoek;

41. betreurt het dat bepaalde Europese ondernemingen en internationale ondernemingen die handel drijven in technologieën voor tweeërlei gebruik met potentiële negatieve gevolgen voor de mensenrechten terwijl zij in de EU actief zijn, actief samenwerken met landen waarvan de activiteiten de mensenrechten schenden;

42. dringt er publiekelijk bij de Commissie op aan ondernemingen die bij dergelijke activiteiten betrokken zijn, uit te sluiten van EU-aanbestedingsprocedures, onderzoeks- en ontwikkelingsfinanciering en van elke andere financiële steun;

43. vraagt de Commissie om extra aandacht te schenken aan mensenrechtenaspecten in de publieke aanbestedingsprocessen voor technologische apparatuur, met name in landen met onbetrouwbare praktijken op dit gebied;

44. vraagt de Commissie en de Raad het open internet, besluitvormingsprocedures waarbij veel belanghebbenden betrokken zijn, netneutraliteit, digitale vrijheden en gegevensbeschermingswaarborgen in derde landen actief te verdedigen in fora voor internetbeheer;

45. veroordeelt het verzwakken en ondermijnen van versleutelingsprotocollen en -producten, in het bijzonder door inlichtingendiensten die versleutelde communicatie willen onderscheppen;

46. waarschuwt voor de privatisering van wetshandhaving door internetbedrijven en internetserviceproviders;

47. vraagt om opheldering van normen en standaarden die private actoren gebruiken om hun systemen te ontwikkelen;

48. herinnert eraan om de context te beoordelen waarin technologieën worden gebruikt om hun effect op mensenrechten volledig te begrijpen;

49. vraagt expliciet om bij voorkeur middelen te promoten die het mogelijk maken om anoniem en/of pseudoniem internet te gebruiken en de strijd aan te gaan met de eenzijdige zienswijze dat zulke middelen criminele activiteiten toestaan, in plaats van het mondiger maken van mensenrechtenactivisten buiten en binnen de EU;

50. dringt er bij de Commissie en de EDEO op aan om intelligente en doeltreffende beleidslijnen te ontwikkelen om de uitvoer van technologieën voor tweeërlei gebruik te reguleren, waarbij de mogelijk schadelijke gevolgen van de uitvoer van ICT-producten en -diensten worden aangepakt, op internationaal niveau binnen multilaterale uitvoerregelingen en andere internationale instanties;

51. benadrukt dat wijzigingen in regelgeving om de effectiviteit van uitvoercontroles van immateriële technologieoverdracht te verhogen legitiem onderzoek en toegang tot en uitwisseling van informatie niet mogen verhinderen, en dat potentiële maatregelen zoals het gebruik van algemene uitvoertoelatingen van de EU voor onderzoek op het gebied van tweeërlei gebruik geen afschrikwekkend effect mogen hebben op individuen en kmo's;

52. vraagt de lidstaten om ervoor te zorgen dat het bestaande en toekomstige uitvoercontrolebeleid de activiteiten van legitieme veiligheidsonderzoekers niet beperkt en dat uitvoercontroles worden toegepast in goed vertrouwen en slechts op duidelijk gedefinieerde technologieën die bestemd zijn voor grootschalig toezicht, censuur, blokkeren, onderscheppen, controles en het opsporen van burgers en hun activiteiten op (mobiele) telefoonnetwerken;

53. herinnert eraan dat meshgebaseerde ad hoc draadloze technologieën een groot potentieel bieden voor het onderhoud van back-upnetwerken in gebieden waar internet niet beschikbaar of geblokkeerd is, en de mensenrechten kunnen bevorderen;

54. vraagt de Commissie een onafhankelijke groep deskundigen aan te stellen die een mensenrechteneffectiviteitsbeoordeling kan uitvoeren op bestaande EU-normen voor ICT's, met als doel het doen van aanbevelingen voor aanpassingen die de bescherming van de mensenrechten zullen verhogen, in het bijzonder als systemen worden uitgevoerd;

55. erkent dat technologische ontwikkeling een uitdaging vormt voor rechtssystemen die zich aan nieuwe omstandigheden moeten aanpassen; onderstreept het belang van wetgevers die meer aandacht moeten schenken aan de digitale economie;

56. vraagt de Commissie het maatschappelijk middenveld en onafhankelijke deskundigen, inclusief veiligheidsonderzoekers, op het vlak van ICT in derde landen te betrekken om voor actuele expertise te zorgen die moet leiden tot toekomstvaste beleidsvorming;

57. benadrukt dat ongewenste gevolgen moeten worden vermeden, zoals beperkingen of afschrikwekkende effecten op wetenschappelijk en andere soorten betrouwbaar onderzoek en ontwikkeling, op de uitwisseling van en toegang tot informatie, op de ontwikkeling van kennis op het gebied van veiligheid of op de uitvoer van technologieën die kunnen bijdragen tot het verwerven van de noodzakelijke digitale competenties en de bevordering van de mensenrechten;

58. is van mening dat de samenwerking tussen overheden en private actoren wereldwijd in het digitale domein, ook binnen het forum voor internetbeheer, onderhevig moet zijn aan controlemechanismen en niet mag leiden tot de ondermijning van democratisch en juridisch toezicht;

59. blijft bij zijn standpunt dat vrijwilligheid niet toereikend is, maar dat er bindende voorschriften nodig zijn om ondernemingen ertoe te brengen dat zij de staat van dienst van landen op het gebied van mensenrechten in overweging nemen voordat zij hun producten aan de desbetreffende landen verkopen, en dat zij een beoordeling van de gevolgen uitvoeren ten aanzien van het effect van hun technologieën op verdedigers van de mensenrechten en critici van regeringen;

60. is van mening dat de uitvoer van zeer gevoelige producten moet worden gecontroleerd, voordat deze producten de EU verlaten, en dat sancties bij overtredingen noodzakelijk zijn;

61. vraagt dat aan ieder individu het recht op encryptie wordt verleend en tevens dat de nodige voorwaarden worden geschapen om encryptie te kunnen uitvoeren; is van mening dat de controle bij de eindgebruiker moet liggen, die ook de vaardigheden nodig heeft om de controle op een zinvolle wijze uit te voeren;

62. vraagt om de invoering van „end-to-end" encryptiestandaarden als vanzelfsprekendheid bij alle communicatiediensten om het meelezen van inhoud door regeringen, geheime diensten en bewakingsdiensten te bemoeilijken;

63. benadrukt de bijzondere verantwoordelijkheid van de geheime diensten van staten om voor vertrouwen te zorgen en vraagt dat aan grootschalig toezicht een einde wordt gemaakt; is van mening dat het toezicht op Europese burgers door binnen- en buitenlandse geheime diensten moet worden aangepakt en gestaakt;

64. wijst de verkoop en verspreiding van Europese monitoringtechnologie en censuurhulpmiddelen aan autoritaire regimes zonder rechtsstaat af;

65. vraagt dat de internationale bescherming van klokkenluiders wordt uitgebreid en roept de lidstaten op om het initiatief te nemen tot wetgeving ter bescherming van klokkenluiders;

66. vraagt om een VN-gezant voor digitale vrijheden en gegevensbescherming en vraagt dat het werkgebied van de speciale vertegenwoordiger van de EU voor de mensenrechten dusdanig wordt uitgebreid dat ook technologie onder het mensenrechtenaspect valt;

67. vraagt om maatregelen die waarborgen dat de privacy van activisten, journalisten en burgers overal ter wereld wordt beschermd en dat zij via het internet onderlinge netwerken kunnen vormen;

68. benadrukt dat toegang tot het internet moet worden erkend als een mensenrecht en vraagt om maatregelen die een einde maken aan de digitale kloof;

69. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de Raad, de Commissie, de vicevoorzitter van de Commissie/hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid en de EDEO.