

Torek, 8. september 2015

P8_TA(2015)0288

Človekove pravice in tehnologija: učinek sistemov za odkrivanje vdorov in sistemov nadzora na človekove pravice v tretjih državah

Resolucija Evropskega parlamenta z dne 8. septembra 2015 o človekovih pravicah in tehnologiji: učinek sistemov za odkrivanje vdorov in sistemov nadzora na človekove pravice v tretjih državah (2014/2232(INI))

(2017/C 316/03)

Evropski parlament,

- ob upoštevanju Splošne deklaracije o človekovih pravicah in Mednarodnega pakta o državljanskih in političnih pravicah, zlasti člena 19 tega pakta,
- ob upoštevanju strateškega okvira Evropske unije za človekove pravice in demokracijo, ki ga je Svet sprejel 25. junija 2012 ⁽¹⁾,
- ob upoštevanju smernic EU o človekovih pravicah glede svobode izražanja na spletu in drugje, ki jih je Svet za zunanje zadeve sprejel 12. maja 2014 ⁽²⁾,
- ob upoštevanju sektorskih smernic za izvajanje vodilnih načel ZN o podjetništvu in človekovih pravicah za sektor informacijskih in komunikacijskih tehnologij, ki jih je Evropska komisija objavila junija 2013,
- ob upoštevanju poročila Organizacije za varnost in sodelovanje v Evropi (OVSE) z dne 15. decembra 2011, ki nosi naslov Svoboda izražanja na internetu ⁽³⁾, in rednega poročila posebnega predstavnika OVSE njegovemu Stalnemu svetu z dne 27. novembra 2014 o svobodi medijev ⁽⁴⁾,
- ob upoštevanju poročila posebnega poročevalca OZN za spodbujanje in varstvo človekovih pravic in temeljnih svoboščin v boju proti terorizmu z dne 23. septembra 2014 (A/69/397) ⁽⁵⁾,
- ob upoštevanju poročila Urada visokega komisarja Združenih narodov za človekove pravice z dne 30. junija 2014, ki nosi naslov Pravica do zasebnosti v digitalni dobi ⁽⁶⁾,
- ob upoštevanju poročila posebnega poročevalca ZN z dne 17. aprila 2013 o pravici do svobode izražanja in mnenja (A/HRC/23/40), ki obravnava posledice nadzora držav nad komunikacijo za uresničevanje človekovih pravic do zasebnosti ter svobode mnenja in izražanja,
- ob upoštevanju poročila o množičnem nadzoru Odbora za pravne zadeve in človekove pravice pri parlamentarni skupščini Sveta Evrope z dne 26. januarja 2015 ⁽⁷⁾,
- ob upoštevanju svoje resolucije z dne 12. marca 2014 o programu nadzora Agencije Združenih držav za nacionalno varnost, organih nadzora v različnih državah članicah ter njihovem učinku na temeljne pravice državljanov EU in o čezatlantskem sodelovanju na področju pravosodja in notranjih zadev ⁽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-e903af10b7a2>.

⁽⁸⁾ Sprejeto besedilo P7_TA(2014)0230.

Torek, 8. september 2015

- ob upoštevanju poročila posebnega predstavnika generalnega sekretarja OZN z dne 21. marca 2011 o človekovih pravicah in transnacionalnih družbah ter drugih podjetjih z naslovom Vodilna načela o podjetništvu in človekovih pravicah: izvajanje okvira Združenih narodov za varovanje, spoštovanje in pomoč ⁽¹⁾,
- ob upoštevanju smernic OECD za večnacionalne družbe ⁽²⁾ in letnega poročila za leto 2014 o navedenih smernicah ⁽³⁾,
- ob upoštevanju letnega poročila organizacije za dodeljevanje spletnih imen in števil za leto 2013 ⁽⁴⁾,
- ob upoštevanju Sporočila Komisije z dne 12. februarja 2014, Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij – Internetna politika in upravljanje interneta – Vloga Evrope pri oblikovanju prihodnosti upravljanja interneta ⁽⁵⁾,
- ob upoštevanju izjave deležnikov NETmundial, sprejete 24. aprila 2014 ⁽⁶⁾,
- ob upoštevanju predsednikovega povzetka devetega foruma o upravljanju interneta, ki je potekal v Istanbulu od 2. do 5. septembra 2014,
- ob upoštevanju uvedbe omejevalnih ukrepov Evropske unije, ki v nekaterih primerih vključujejo embargo na telekomunikacijsko opremo, informacijsko in komunikacijsko tehnologijo (IKT) ter orodje za spremljanje,
- ob upoštevanju Uredbe (EU) št. 599/2014 Evropskega parlamenta in Sveta z dne 16. aprila 2014 o spremembi Uredbe Sveta (ES) št. 428/2009 o vzpostavitvi režima Skupnosti za nadzor izvoza, prenosa, posredovanja in tranzita blaga z dvojno rabo ⁽⁷⁾,
- ob upoštevanju skupne izjave Evropskega parlamenta, Sveta in Komisije o pregledu sistema za nadzor izvoza blaga z dvojno rabo z dne 16. aprila 2014 ⁽⁸⁾,
- ob upoštevanju sklepov 19. plenarnega zasedanja o Wassenaarskem sporazumu o nadzoru izvoza konvencionalnega orožja ter blaga in tehnologije z dvojno rabo, ki je potekalo na Dunaju 3. in 4. decembra 2013,
- ob upoštevanju Sporočila Komisije Svetu in Evropskemu parlamentu – Pregled politike nadzora izvoza: zagotavljanje varnosti in konkurenčnosti v spreminjajočem se svetu z dne 24. aprila 2014 ⁽⁹⁾,
- ob upoštevanju sklepov Sveta z dne 21. novembra 2014 o pregledu politike nadzora izvoza,
- ob upoštevanju svoje resolucije z dne 11. decembra 2012 o strategiji digitalne svobode v zunanji politiki EU ⁽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:frozensnode.

⁽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⁾ UL L 173, 12.6.2014, str. 79.

⁽⁸⁾ UL L 173, 12.6.2014, str. 82.

⁽⁹⁾ COM(2014)0244.

⁽¹⁰⁾ Sprejeta besedila, P7_TA(2012)0470.

Torek, 8. september 2015

- ob upoštevanju svoje resolucije z dne 13. junija 2013 o svobodi tiska in medijev ⁽¹⁾,
 - ob upoštevanju svojih resolucij o nujnih primerih kršitev človekovih pravic, demokratičnih načel in načel pravne države, ki vzbujajo skrb glede digitalne svobode,
 - ob upoštevanju svoje resolucije z dne 12. marca 2015 o prednostnih nalogah EU za Svet za človekove pravice v letu 2015 ⁽²⁾,
 - ob upoštevanju svoje resolucije z dne 11. februarja 2015 o podaljšanju mandata foruma o upravljanju interneta ⁽³⁾,
 - ob upoštevanju svoje resolucije z dne 12. marca 2015 o letnem poročilu o človekovih pravicah in demokraciji v svetu v letu 2013 ter politiki Evropske unije na tem področju ⁽⁴⁾,
 - ob upoštevanju pisne izjave Edwarda Snowdna odboru LIBE iz marca 2014 ⁽⁵⁾,
 - ob upoštevanju Evropske konvencije o človekovih pravicah in potekajočih pogajanj o pristopu EU k tej konvenciji,
 - ob upoštevanju Listine Evropske unije o temeljnih pravicah,
 - ob upoštevanju člena 52 Poslovnika,
 - ob upoštevanju poročila Odbora za zunanje zadeve (A8-0178/2015),
- A. ker imata tehnološki razvoj in dostop do odprtega interneta vse pomembnejšo vlogo pri tem, da se v celoti omogoči in zagotovi izpolnjevanje in spoštovanje človekovih pravic in temeljnih svoboščin, ter pozitiven učinek, saj spodbujata večjo svobodo izražanja, dostop do informacij ter pravico do zasebnosti in do svobode zbiranja in združevanja po vsem svetu;
- B. ker se tehnološki sistemi lahko zlorabijo kot pripomoček za kršitve človekovih pravic s cenzuro, nadzorom, nepooblaščenim dostopom do naprav, motenjem signala, prestrezanjem ter izsleditvijo in sledenjem informacijam in posameznikom;
- C. ker javni in zasebni akterji, tudi vlade in organi kazenskega pregona, pa tudi hudodelske združbe in teroristične mreže s tem kršijo človekove pravice;
- D. ker so lahko informacijske in komunikacijske tehnologije gonilo napredka ali spodbuda h kršenju človekovih pravic, njihov učinek pa je v veliki meri odvisen od okoliščin, v katerih nastajajo ali se uporabljajo; ker informacijska tehnologija, zlasti programska oprema, le redko služi enemu samemu namenu in ima ponavadi vojno rabo, kar zadeva možnost za kršenje človekovih pravic, programska oprema pa je tudi oblika govora;
- E. ker je informacijska tehnologija ključni instrument, ki ljudem pomaga organizirati družbena gibanja in proteste v različnih državah, zlasti tistih z avtoritarnimi režimi;

⁽¹⁾ Sprejeta besedila, P7_TA(2013)0274.

⁽²⁾ Sprejeta besedila, P8_TA(2015)0079.

⁽³⁾ Sprejeta besedila, P8_TA(2015)0033.

⁽⁴⁾ Sprejeta besedila, P8_TA(2015)0076.

⁽⁵⁾ <http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf>.

Torek, 8. september 2015

- F. ker oceno posledic, ki jo imajo okoliščine, v katerih se tehnologija uporablja, za človekove pravice, določata trdnost nacionalnih in regionalnih zakonodajnih okvirov, ki urejajo uporabo tehnologij, in možnost političnih in pravosodnih institucij, da nadzirajo takšno uporabo;
- G. ker imajo zasebni akterji vse pomembnejšo vlogo na digitalnem področju, in sicer na vseh področjih družbenih dejavnosti, vendar še vedno niso uvedeni zaščitni ukrepi, ki bi jim preprečili pretirano omejevanje temeljnih pravic in svoboščin; ker zasebni akterji zato igrajo dejavnejšo vlogo pri ocenjevanju zakonitosti vsebine in razvoju sistemov za kibernetško varnost in nadzor, ki lahko škodljivo vplivajo na spoštovanje človekovih pravic po vsem svetu;
- H. ker internet predstavlja revolucijo v smislu možnosti, ki jih ponuja za izmenjavo vseh vrst podatkov, informacij in znanja;
- I. ker je šifriranje pomembna metoda, ki pripomore k varnosti komunikacij in ljudi, ki jih uporabljajo;
- J. ker je model odločanja s sodelovanjem več deležnikov koristen za upravljanje interneta, saj ta postopek zagotavlja pomembno, vključujoče in odgovorno sodelovanje vseh zainteresiranih strani, tudi vlad, civilne družbe, tehničnih in akademskih skupnosti, zasebnega sektorja in uporabnikov;
- K. ker so obveščevalne agencije sistematično spodkopavale kriptografske protokole in izdelke, da bi lahko prestrezale sporočila in podatke; ker je Agencija ZDA za nacionalno varnost zbrala veliko število varnostnih vrzeli v informacijski tehnologiji (t.i. „zero-day exploits“), ki javnosti ali prodajalcu izdelka še niso znane; ker takšne dejavnosti spodkopavajo svetovna prizadevanja za izboljšanje varnosti informacijske tehnologije;
- L. ker so obveščevalne službe s sedežem v EU izvajale dejavnosti, ki škodijo človekovim pravicam;
- M. ker so sodni in demokratični nadzor ter zaščitni ukrepi glede na hiter tehnološki razvoj v veliki meri premalo razviti;
- N. ker lahko ukrepi na področju (kibernetške) varnosti in boja proti terorizmu, ki predvidevajo rabo IKT in nadzor interneta, zelo negativno vplivajo na spoštovanje človekovih pravic in svoboščin posameznikov po vsem svetu, tudi državljanov EU, ki prebivajo ali potujejo v tujino, zlasti če ni pravne podlage, ki bi temeljila na načelih nujnosti, sorazmernosti ter demokratičnega in sodnega nadzora;
- O. ker internetni filtri in nadzor komunikacij spodkopavajo zmožnost zagovornikov človekovih pravic, da bi izkoristili internet in sporočali občutljive podatke, ter kršijo več členov Splošne deklaracije o človekovih pravicah, ki vsakemu posamezniku zagotavlja pravico do zasebnosti in svobode izražanja;
- P. ker sta digitalna varnost in svoboda bistveni in druga druge ne moreta nadomestiti;
- Q. ker je Evropska unija na področju digitalnih svoboščin lahko za vzor le, če jih ščiti znotraj svojih meja; in je zato bistveno, da se sprejme sveženj EU za varstvo podatkov;

Torek, 8. september 2015

- R. ker gre za daljnosežne družbene interese, kot je varstvo temeljnih pravic, ki jih ne bi smeli prepustiti samo trgu in ki jih je treba urediti s predpisi;
- S. ker so spoštovanje temeljnih pravic in pravne države ter učinkovit parlamentarni nadzor obveščevalnih služb, ki uporabljajo tehnologijo za digitalni nadzor, pomembni elementi mednarodnega sodelovanja;
- T. ker imajo podjetja s sedežem v EU pomemben svetovni tržni delež na področju IKT, zlasti ko gre za izvoz tehnologije za nadzor, sledenje, poseganje v zasebnost in spremljanje;
- U. ker uvedba nadzora izvoza ne bi smela škoditi zakonitim raziskavam o vprašanih informacijsko-tehnološke varnosti ali razvoju orodij za informacijsko-tehnološko varnost, če ne gre za namen storitve kaznivega dejanja;
1. se zaveda, da so človekove pravice in temeljne svoboščine univerzalne in bi jih morali zaščititi po vsem svetu v vseh razsežnostih njihovega uresničevanja; poudarja, da nadzor komunikacij kot tak posega v pravici do zasebnosti in izražanja, če se izvaja zunaj ustreznega pravnega okvira;
 2. poziva Komisijo, naj zagotovi skladnost med zunanjim delovanjem EU in njenimi notranjimi politikami na področju IKT;
 3. meni, da je dejavno sodelovanje nekaterih držav članic EU pri množičnem nadzoru državljanov in vohunjenjem za političnimi voditelji ameriške Agencije za nacionalno varnost, kot ju je razkril Edward Snowden, resno škodila verodostojnosti evropske politike človekovih pravic in spodbujala globalno zaupanje v prednosti IKT;
 4. države članice in ustrezne agencije EU, vključno z Europolom in Eurojustom, opozarja na obveznosti iz Listine Evropske unije o temeljnih pravicah in spoštovanje mednarodne zakonodaje o človekovih pravicah ter na zunanjepolitične cilje EU, naj ne izmenjujejo obveščevalnih podatkov, če bi to lahko privedlo do kršitev človekovih pravic v tretji državi, ali uporabljajo informacij, pridobljenih s kršenjem človekovih pravic, kot je nezakonit nadzor, zunaj EU;
 5. poudarja, da bi bilo treba vpliv tehnologij na izboljšanje človekovih pravic po potrebi vključiti v vse politike in programe EU, da bi s tem dosegli napredek pri varovanju človekovih pravic ter spodbujali demokracijo, pravno državo in dobro upravljanje ter mirno reševanje sporov;
 6. poziva k dejavnemu razvoju in širjenju tehnologij, ki bodo pripomogle k varstvu človekovih pravic in spodbujale digitalne pravice in svoboščine ljudi, kakor tudi njihovo varnost, in ki bodo spodbujale najboljšo prakso in ustrezne zakonodajne okvire, hkrati pa zagotavljale varnost in celovitost osebnih podatkov; poziva zlasti EU in države članice, naj spodbujajo uporabo in razvoj odprtih standardov, brezplačne odprtokodne programske opreme in tehnologij šifriranja po svetu;
 7. poziva EU, naj poveča podporo akterjem, ki si prizadevajo za krepitev standardov varnosti in varstva zasebnosti v IKT na vseh ravneh, vključno s strojno in programsko opremo ter komunikacijskimi standardi, kakor tudi za razvoj strojne in programske opreme v okvirih vgrajene zasebnosti;
 8. poziva k ustanovitvi sklada za človekove pravice in tehnologijo v okviru evropskega instrumenta za demokracijo in človekove pravice;
 9. poziva samo EU in še zlasti Evropsko službo za zunanje delovanje, naj pri komuniciranju z zagovorniki človekovih pravic uporabljata šifriranje, da ne bi ogrozili zagovornikov in da bi lastno komunikacijo z zunanjim svetom zaščitili pred nadzorom;

Torek, 8. september 2015

10. poziva EU, naj začne uporabljati brezplačno in odprtokodno programsko opremo ter tudi druge akterje spodbuja k enakemu ravnanju, saj ta programska oprema zagotavlja večjo varnost in spoštovanje človekovih pravic;
11. opozarja, da je razvoj IKT na konfliktnih območjih pomemben za spodbujanje dejavnosti za vzpostavitev miru, da bi zagotovili varno komunikacijo med stranmi, ki sodelujejo v mirnem reševanju sporov;
12. poziva k uporabi pogojev, meril in postopkov poročanja z namenom zagotavljanja, da se finančna in tehnična podpora EU za razvoj novih tehnologij v tretjih državah ne uporabljata tako, da bi kršili človekove pravice;
13. poziva Komisijo in Svet, naj se aktivno povežeta z vladami tretjih držav in s pomočjo obstoječih evropskih mehanizmov podpore in instrumentov še naprej podpirata in usposabljata zagovornike človekovih pravic, aktiviste civilne družbe in neodvisne novinarje, ki pri svoji dejavnosti uporabljajo varno informacijsko in komunikacijsko tehnologijo, ter krepita njihovo vlogo in naj spodbujata s tem povezane temeljne pravice do zasebnosti, kot so neomejen dostop do informacij na spletu, pravica do zasebnosti in varstva podatkov ter pravice do svobodnega izražanja, svobode zbiranja in združevanja ter objavljanja na spletu;
14. opozarja na težak položaj prijaviteljev nepravilnosti in njihovih zagovornikov, vključno z novinarji, po razkritjih zlorab nadzora v tretjih državah; meni, da bi bilo treba te posameznike šteti za zagovornike človekovih pravic in da si zato zaslužijo zaščito EU, kot določajo smernice EU o zagovornikih človekovih pravic; ponovno poziva Komisijo in države članice, naj temeljito preučijo možnost, da se prijaviteljem nepravilnosti dodeli mednarodna zaščita pred pregonom;
15. obžaluje, da se varnostni ukrepi, vključno s protiterorističnimi ukrepi, vse večkrat uporabljajo kot izgovor za kršenje pravice do zasebnosti in preprečevanje legitimnih dejavnosti zagovornikov človekovih pravic, novinarjev in političnih aktivistov; poudarja svoje trdno prepričanje, da nacionalna varnost nikoli ne sme biti opravičilo za programe neciljnega, tajnega ali množičnega nadzora; vztraja, naj se takšni ukrepi izvajajo strogo v skladu s standardi pravne države in človekovih pravic, vključno s pravico do zasebnosti in varstva podatkov;
16. poziva Evropsko službo za zunanje delovanje in Komisijo, naj spodbujata demokratični nadzor varnostnih in obveščevalnih služb v svojem političnem dialogu s tretjimi državami, kakor tudi pri razvoju programov čezmejnega sodelovanja; poziva Komisijo, naj podpre organizacije civilne družbe in zakonodajne organe v tretjih državah, ki si prizadevajo o krepiti nadzor, preglednost in odgovornost domačih varnostnih služb; poziva, naj se konkretne zaveze v zvezi s tem vključijo v prihodnji akcijski načrt EU za človekove pravice in demokratizacijo;
17. poziva Svet in Komisijo, naj pri vseh stikih s tretjimi državami, tudi pri pristopnih pogajanjih, trgovinskih pogajanjih in dialogih o človekovih pravicah in v diplomatskih odnosih spodbujata digitalne svoboščine ter neomejen dostop do interneta;
18. se zaveda, da je internet postal javni prostor in trg, za katera sta prost pretok informacij in dostop do informacijske in komunikacijske tehnologije nepogrešljiva; zato poudarja, da je treba sočasno pospeševati in zaščititi digitalno svobodo in prosto trgovino;
19. poziva, naj se v vse sporazume s tretjimi državami vključijo klavzule, v katerih bo izrecno navedeno, da je treba spodbujati, zagotoviti in spoštovati digitalne svoboščine, nevtralnost omrežja, necenzuriran in neomejen dostop do interneta, pravico do zasebnosti in varstvo podatkov;

Torek, 8. september 2015

20. poziva EU, naj nasprotuje kriminalizaciji uporabe orodij za šifriranje, izogibanje cenzuri in zasebnost s strani zagovornikov človekovih pravic, tako da zavrne omejitve uporabe šifriranja znotraj EU, in naj oporeka vladam tretjih držav, ki vlagajo takšne obtožbe proti zagovornikom človekovih pravic;

21. poziva EU, naj nasprotuje kriminalizaciji uporabe orodij za šifriranje, proti cenzuri in za zasebnost, tako da zavrne omejitve uporabe šifriranja znotraj EU in oporeka vladam tretjih držav, ki takšna orodja kriminalizirajo;

22. poudarja, da je treba za učinkovito razvojno politiko EU in politiko EU na področju človekovih pravic vanju vključiti informacijsko in komunikacijsko tehnologijo ter premostiti digitalno vrzel, tako da se zagotovi osnovna tehnološka infrastruktura, poenostavi dostop do znanja in informacij in tako spodbudijo digitalne veščine ter spodbudi uporaba odprtih standardov v dokumentih in uporaba brezplačne in odprtokodne programske opreme, če je to primerno, da se zagotovita odprtost in preglednost (zlasti v javnih institucijah), vključno z zaščito varstva podatkov na digitalnem področju po vsem svetu, kot tudi boljše razumevanje morebitnih tveganj in koristi informacijskih in komunikacijskih tehnologij;

23. poziva Komisijo, naj podpre odpravo digitalnih ovir za invalide; meni, da je zelo pomembno, da so politike EU na področju razvoja in spodbujanja človekovih pravic v svetu namenjene zmanjšanju digitalnega razkoraka za invalide in zagotavljanju širšega okvira pravic, zlasti kar zadeva dostop do znanja, digitalno udeležbo in vključenost v nove gospodarske in socialne priložnosti, ki jih ustvarja internet;

24. poudarja, da lahko zakonito digitalno zbiranje in širjenje dokazov o kršitvah človekovih pravic prispeva k vsesplošnemu boju zoper nekaznovanost in terorizem; meni, da bi morale biti to gradivo v skladu z mednarodnim (kazenskim) pravom v utemeljenih primerih dopusten dokaz v sodnih postopkih, in sicer v skladu z mednarodnimi, regionalnimi in ustavnimi zaščitnimi mehanizmi; priporoča, naj se na področju mednarodnega kazenskega prava oblikujejo mehanizmi za uvedbo postopkov, s katerimi se takšni podatki overijo in zberejo kot dokaz za uporabo v sodnih postopkih;

25. obžaluje, da se nekatere informacijske in komunikacijske tehnologije ter storitve iz EU prodajajo in jih lahko posamezniki, podjetja in organi v tretjih državah uporabljajo za namene, ki kršijo človekove pravice s cenzuriranjem, množičnim nadzorom, motenjem, prestrezanjem in spremljanjem ter z sledenjem državljanov in njihove uporabe (mobilnih) telefonskih omrežij in interneta; je zaskrbljen, ker bi lahko nekatera podjetja s sedežem v EU zagotavljale tehnologije in storitve, ki omogočajo tako kršenje človekovih pravic;

26. ugotavlja, da grožnje za varnost Evropske unije, njenih držav članic in tretjih držav pogosto prihajajo od posameznikov ali majhnih skupin, ki za načrtovanje in izvedbo napadov uporabljajo omrežja za digitalno komunikacijo, in da je treba orodja in taktike za izničenje takšnih groženj nenehno pregledovati in posodabljati;

27. meni, da je množični nadzor, ki ni upravičen s povečanim tveganjem zaradi terorističnih napadov in groženj, v nasprotju z načeloma nujnosti in sorazmernosti, zato predstavlja kršitev človekovih pravic;

28. poziva države članice, naj spodbujajo poln demokratični nadzor nad operacijami obveščevalnih služb v tretjih državah, da preveri, ali te službe pri svojem delovanju v celoti spoštujejo načelo pravne države, ter kaznuje službe in posameznike, ki nezakonito delujejo;

29. glede na povečano sodelovanje in izmenjavo informacij med državami članicami in tretjimi državami – vključno z uporabo digitalnega nadzora – spodbuja države članice, naj zagotovijo demokratični nadzor nad temi službami in njihovimi dejavnostmi s pomočjo ustreznega notranjega, izvršnega, sodnega in neodvisnega parlamentarnega nadzora;

Torek, 8. september 2015

30. poudarja, da bi bilo treba v okviru prava EU sprejeti načela družbene odgovornosti gospodarskih družb in merila „vgrajenih človekovih pravic“, pri katerih gre za tehnološke rešitve in inovacije za zaščito človekovih pravic, s čimer bi zagotovili, da bodo ponudniki internetnih storitev, razvijalci programske opreme, proizvajalci strojne opreme, družabna omrežja/mediji, ponudniki mobilne telefonije in drugi upoštevali človekove pravice končnih uporabnikov na svetovni ravni;

31. poziva EU, naj zagotovi večjo preglednost v odnosu med mobilnimi operaterji in ponudniki internetnih storitev ter vladami ter naj k temu poziva v svojih odnosih s tretjimi državami z zahtevo, da operaterji in ponudniki internetnih storitev letno objavljajo podrobna poročila o preglednosti, vključno s poročili o dejavnostih, ki so jih zahtevale oblasti, in finančnimi povezavami med javnimi organi in operaterji/ponudniki internetnih storitev;

32. opozarja korporativne akterje, da so odgovorni za spoštovanje človekovih pravic pri vsem svojem delovanju po svetu, ne glede na to, kje se nahajajo njihovi uporabniki in ali država gostiteljica izpolnjuje svoje obveznosti s področja človekovih pravic; poziva podjetja IKT, zlasti tista s sedežem v EU, naj izvajajo vodilna načela ZN o podjetništvu in človekovih pravicah, tudi z vzpostavitvijo politike potrebne skrbnosti in zaščitnih ukrepov za upravljanje tveganja ter zagotavljanjem učinkovitih protiukrepov v primeru, da so njihove dejavnosti povzročile negativne učinke na področju človekovih pravic ali prispevale k takim učinkom;

33. poudarja, da je treba na ravni EU učinkoviteje izvajati in spremljati uredbe EU in sankcije, ki zadevajo IKT, vključno z uporabo vseobsegajočih mehanizmov, in s tem zagotoviti, da bodo države članice spoštovale zakonodajo in se bodo ohranili enaki konkurenčni pogoji;

34. poudarja, da je spoštovanje temeljnih pravic bistvena sestavina uspešnih protiterorističnih politik, tudi z uporabo tehnologij za digitalni nadzor;

35. pozdravlja sklep zasedanja o Wassenaarskem sporazumu decembra 2013 o nadzoru izvoza na področjih orodij za nadzor, kazenski pregon in zbiranje obveščevalnih podatkov ter sistemov za mrežni nadzor; opozarja, da je ureditev EU za blago z dvojno rabo, tj. uredba EU o dvojni rabi, še vedno nepopolna, ko gre za učinkovit in sistematičen nadzor izvoza škodljivih tehnologij IKT v nedemokratične države;

36. poziva Komisijo, naj glede na bližnji pregled in prenavo politike glede dvojne rabe hitro pripravi predloge za pametne in učinkovite politike za omejitev in urejanje komercialnega izvoza storitev na področju uvajanja in uporabe tako imenovanih tehnologij z dvojno rabo, ki bodo obravnavale potencialno škodljivi izvoz izdelkov in storitev IKT v tretje države, kot je bilo aprila 2014 dogovorjeno v skupni izjavi Evropskega parlamenta, Sveta in Komisije; poziva Komisijo, naj vanj vključi učinkovite zaščitne ukrepe, da bi preprečili morebitne škodljive učinke tega nadzora izvoza na raziskave, vključno z znanstvenimi raziskavami in raziskavami na področju informacijsko-tehnološke varnosti;

37. poudarja, da bi morala biti Komisija zmožna čim prej zagotoviti pravilne in najnoveše informacije o zakonitosti ali morebitnih škodljivih učinkih potencialnih transakcij podjetjem, ki se sprašujejo, ali naj zaprosijo za izvozno dovoljenje;

38. poziva Komisijo, naj predstavi predloge o pregledu, kako bi lahko standarde EU glede IKT uporabili za preprečevanje morebitnih škodljivih posledic izvoza teh tehnologij ali drugih storitev v tretje države, kjer konceptov, kot je „zakonito prestrezanje“, ni mogoče obravnavati kot enakovredne tistim v Evropski uniji ali kjer so na primer razmere na področju človekovih pravic slabe ali ne veljajo načela pravne države;

Torek, 8. september 2015

39. znova potrjuje, da morajo standardi EU, zlasti Listina EU o temeljnih pravicah, prevladati pri ocenjevanju incidentov, pri katerih se tehnologije z dvojno rabo uporabljajo tako, da se lahko omejujejo človekove pravice;
40. poziva k oblikovanju politik, s katerimi bi uredili prodajo varnostnih vrzeli v informacijski tehnologiji (t. i. „zero-day exploits“) in preprečili njihovo uporabo za kibernetске napade ali za nepooblaščen dostop do naprav, ki bi vodil do kršenja človekovih pravic, ne da bi takšni predpisi pomembno vplivali na akademske ali druge raziskave varnosti, ki se izvajajo v dobri veri;
41. obžaluje, da so nekatera evropska podjetja in mednarodna podjetja, ki trgujejo s tehnologijami z dvojno rabo s potencialno škodljivimi učinki na človekove pravice in poslujejo v EU, dejavna v državah z režimi, ki kršijo človekove pravice;
42. poziva Komisijo, naj podjetja, ki sodelujejo pri takšnih dejavnostih, izključi iz postopkov javnih naročil EU, financiranja raziskav in razvoja ter vsakršne druge finančne podpore;
43. poziva Komisijo, naj posebno pozornost posveti vidikom človekovih pravic v postopkih javnih naročil za tehnološko opremo, zlasti v državah z nezanesljivimi praksami na tem področju;
44. poziva Komisijo in Svet, naj na forumih o upravljanju interneta dejavno zagovarjata odprti internet, procese odločanja z več deležniki, nevtralnost omrežja, digitalne svoboščine in zaščitne ukrepe za varstvo podatkov v tretjih državah;
45. obsoja slabljenje in spodkopavanje protokolov in izdelkov za šifriranje, zlasti s strani obveščevalnih služb, ki želijo prestrezati šifrirana sporočila;
46. svari pred privatizacijo kazenskega pregona prek internetnih podjetij in ponudnikov internetnih storitev;
47. poziva k pojasnitvi predpisov in standardov, ki jih zasebni akterji uporabljajo za razvoj svojih sistemov;
48. opozarja na pomembnost ocenjevanja okoliščin, v katerih se tehnologije uporabljajo, da bi v celoti razumeli njihov vpliv na človekove pravice;
49. izrecno poziva k širjenju orodij, ki omogočajo anonimno in/ali psevdonimno uporabo interneta, in oprekanju enostranskemu pogledu, da takšna orodja služijo edino kriminalnim dejavnostim, ne omogočajo pa delovanja aktivistov za človekove pravice zunaj in znotraj EU;
50. poziva Svet, Komisijo in Evropsko službo za zunanje delovanje, naj na mednarodni ravni in v okviru večstranskih izvoznih nadzornih režimov in drugih mednarodnih organov razvijejo pametne in učinkovite politike za urejanje izvoza tehnologij z dvojno rabo, ki bodo obravnavale potencialno škodljiv izvoz izdelkov in storitev IKT;
51. poudarja, da regulativne spremembe, namenjene povečanju učinkovitosti nadzora izvoza prenosa nematerialne tehnologije, ne smejo ovirati zakonitih raziskav in dostopa do informacij ter njihove izmenjave in da morebitni ukrepi, kot je uporaba splošnih izvoznih dovoljenj EU za raziskave tehnologij z dvojno rabo, ne smejo negativno vplivati na posameznike in MSP;

Torek, 8. september 2015

52. poziva države članice, naj zagotovijo, da sedanje in prihodnje politike nadzora izvoza ne bodo omejevale dejavnosti zakonitih raziskovalcev varnosti in da se bo nadzor izvoza uporabljal v dobri veri ter izključno za jasno opredeljene tehnologije, namenjene množičnemu nadzoru, cenzuri, motenju signala, prestrezanju ali spremljanju, ter sledenju državljanom in njihovim aktivnostim v (mobilnih) telefonskih omrežjih;
53. opozarja, da brezžične tehnologije zankastih omrežij ad hoc ponujajo velik potencial za zagotavljanje podpornih omrežij na območjih, kjer internet ni na voljo ali je blokiran, in lahko pripomorejo k spodbujanju človekovih pravic;
54. poziva Komisijo, naj določi neodvisno skupino strokovnjakov, ki lahko izvede oceno učinka človekovih pravic na obstoječe standarde EU za IKT z namenom oblikovanja priporočil za prilagoditve, ki bodo okrepile varstvo človekovih pravic, zlasti ko gre za izvoz sistemov;
55. priznava, da tehnološki razvoj predstavlja izziv za pravne sisteme, ki se morajo prilagoditi novim razmeram; poudarja pomembnost tega, da zakonodajalci namenijo več pozornosti vprašanjem, ki so povezana z digitalnim gospodarstvom;
56. poziva Komisijo, naj vključi civilno družbo in neodvisne strokovnjake s področja IKT v tretjih državah, tudi raziskovalce na področju varnosti, saj se bo tako zagotovilo najnovejše strokovno znanje, kar naj bi privedlo do oblikovanja politik, pripravljenih na izzive prihodnosti;
57. poudarja, da se je treba izogibati neželenim posledicam, kot je omejevanje ali oviranje znanstvenih in drugih vrst raziskav in razvoja, ki se izvajajo v dobri veri, izmenjave informacij in dostopa do njih, razvoja znanja o varnosti ali izvoza tehnologij, ki so v interesu pridobivanja potrebnih digitalnih znanj in spretnosti ter spodbujanja človekovih pravic;
58. meni, da sodelovanje na digitalnem področju med vladami in zasebnimi akterji po vsem svetu zahteva jasen sistem nadzora in ravnotežja, ki vključuje Forum o upravljanju interneta, ter ne sme privedi do spodkopavanja demokratičnega in sodnega nadzora;
59. ugotavlja, da prostovoljni pristop ne zadostuje in so potrebni zavezujoči ukrepi, da bi podjetja spodbudili, naj upoštevajo stanje na področju človekovih pravic v državi, preden začnejo v njej prodajati svoje izdelke, in naj ocenijo, kako bodo njihove tehnologije vplivale na zagovornike človekovih pravic in kritike vlade;
60. meni, da je treba izvoz zelo občutljivega blaga preveriti, preden zapusti EU, in da so v primeru kršitev potrebne kazni;
61. poziva, naj ima vsak posameznik pravico do šifriranja in naj se ustvarijo pogoji, ki so potrebni za izvajanje šifriranja; meni, da mora biti nadzor stvar končnega uporabnika, pri čemer bi moral biti ta tudi usposobljen za ustrezno izvajanje takšnega nadzora;
62. poziva k uvedbi standardov šifriranja brez posrednikov, ki naj postanejo samoumevni za vse komunikacijske storitve, da bi vladam, obveščevalnim službam in nadzornim organom otežili branje vsebine;
63. poudarja posebno odgovornost vladnih obveščevalnih služb za izgradnjo zaupanja in poziva k prenehanju množičnega nadzora; meni, da je treba spremljanje evropskih državljanov prek domačih in tujih obveščevalnih služb obravnavati ter ga ustaviti;
64. nasprotuje prodaji in distribuciji evropske tehnologije za nadzor in orodij za cenzuro avtoritarnim režimov, v katerih načelo pravne države ne velja;

Torek, 8. september 2015

65. poziva k razširitvi možnosti za mednarodno zaščito prijaviteljev nepravilnosti in spodbuja tudi države članice, naj predlagajo zakone za njihovo zaščito;
 66. poziva, naj se imenuje odposlanec ZN za digitalne svoboščine in varstvo podatkov ter naj se razširijo pristojnosti posebnega predstavnika EU za človekove pravice, tako da bo tudi tehnologija obravnavana z vidika človekovih pravic;
 67. poziva k ukrepom za zagotovitev, da bo zasebnost aktivistov, novinarjev in državljanov varovana povsod po svetu in da se bodo lahko povezovali prek interneta;
 68. vztraja, da je treba pravico dostopa do interneta priznati kot človekovo pravico, in poziva k ukrepom za odpravo digitalnega razkoraka;
 69. naroči svojemu predsedniku, naj to resolucijo posreduje Svetu in Komisiji ter podpredsednici Komisije/visoki predstavnici Unije za zunanje zadeve in varnostno politiko, in ESZD.
-