Mardi 8 septembre 2015

P8_TA(2015)0288

Droits de l'homme et technologies dans les pays tiers

Résolution du Parlement européen du 8 septembre 2015 concernant les droits de l'homme et la technologie: incidences des systèmes d'intrusion et de surveillance sur les droits de l'homme dans les pays tiers (2014/2232(INI))

(2017/C 316/03)

Le Parlement européen,

— vu la Déclaration universelle des droits de l'homme et le Pacte international relatif aux droits civils et politiques, en particulier son article 19,

— vu le cadre stratégique de l'Union européenne en matière de droits de l'homme et de démocratie, adopté par le Conseil le 25 juin 2012 ([1]),

— vu les orientations de l'Union relatives à la liberté d'expression en ligne et hors ligne adoptées par le Conseil «Affaires étrangères» le 12 mai 2014 ([2]),

— vu le guide à destination du secteur des TIC sur la mise en œuvre des principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, publié par la Commission en juin 2013,

— vu le rapport de l'Organisation pour la sécurité et la coopération en Europe (OSCE) du 15 décembre 2011 intitulé «*Freedom of Expression on the Internet*» (Liberté d'expression sur l'internet) ([3]) et le rapport régulier du représentant spécial de l'OSCE pour la liberté des médias au Conseil permanent de l'OSCE du 27 novembre 2014 ([4]),

— vu le rapport du rapporteur spécial des Nations unies pour la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte contre le terrorisme du 23 septembre 2014 (A/69/397) ([5]),

— vu le rapport du haut-commissariat des Nations Unies aux droits de l'homme du 30 juin 2014 intitulé «Le droit à la vie privée à l'ère du numérique» ([6]),

— vu le rapport du rapporteur spécial des Nations unies sur le droit à la liberté d'expression et d'opinion du 17 avril 2013 (A/HRC/23/40) sur les implications de la surveillance des communications par les États sur l'exercice des droits de l'homme relatifs à la vie privée et à la liberté d'opinion et d'expression,

— vu le rapport de la commission des questions juridiques et des droits de l'homme de l'assemblée parlementaire du Conseil de l'Europe du 26 janvier 2015 intitulé «Les opérations massives de surveillance» ([7]),

— vu sa résolution du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures ([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-FR.pdf/ec460a49-b709-4099-b53c-194761ec8621.
([8]) Textes adoptés de cette date, P7_TA(2014)0230.

— vu le rapport du représentant spécial du Secrétaire général des Nations unies pour les droits de l'homme et les sociétés transnationales et autres entreprises du 21 mars 2011 intitulé «Principes directeurs relatifs aux entreprises et aux droits de l'homme: mise en œuvre du cadre de référence "protéger, respecter et réparer" des Nations unies» ([1]),

— vu les principes directeurs de l'Organisation de coopération et de développement économiques (OCDE) à l'intention des entreprises multinationales ([2]) et le rapport annuel 2014 sur les principes directeurs de l'OCDE à l'intention des entreprises multinationales ([3]),

— vu le rapport annuel 2013 de la Société pour l'attribution des noms de domaine et des numéros sur Internet ([4]),

— vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 12 février 2014 intitulée «Politique et gouvernance de l'internet: le rôle de l'Europe à l'avenir» ([5]),

— vu la déclaration multipartite de NetMundial adoptée le 24 avril 2014 ([6]),

— vu le résumé du président relatif au neuvième forum sur la gouvernance de l'internet, qui s'est tenu à Istanbul du 2 au 5 septembre 2014,

— vu les mesures restrictives mises en place par l'Union européenne, lesquelles incluent notamment des embargos sur les équipements de télécommunication, les technologies de l'information et de la communication (TIC) et les outils de surveillance,

— vu le règlement (UE) n° 599/2014 du Parlement européen et du Conseil du 16 avril 2014 portant modification du règlement (CE) n° 428/2009 du Conseil instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage ([7]),

— vu la déclaration commune du Parlement européen, du Conseil et de la Commission du 16 avril 2014 sur l'examen du système de contrôle des exportations de biens à double usage ([8]),

— vu les décisions de la 19e réunion plénière de l'Arrangement de Wassenaar relatif au contrôle des exportations des armes conventionnelles et des biens et technologies à double usage, organisée à Vienne les 3 et 4 décembre 2013,

— vu la communication de la Commission au Conseil et au Parlement européen du 24 avril 2014 intitulée «Réexamen de la politique de contrôle des exportations: garantir la sécurité et la compétitivité dans un monde en mutation» ([9]),

— vu les conclusions du Conseil du 21 novembre 2014 sur le réexamen de la politique de contrôle des exportations,

— vu sa résolution du 11 décembre 2012 sur une stratégie pour la liberté numérique dans la politique étrangère de l'Union ([10]),

---

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

([2]) http://www.oecd.org/fr/daf/inv/mne/48004355.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]) JO L 173 du 12.6.2014, p. 79.

([8]) JO L 173 du 12.6.2014, p. 82.

([9]) COM(2014)0244.

([10]) Textes adoptés de cette date, P7_TA(2012)0470.

Mardi 8 septembre 2015

— vu sa résolution du 13 juin 2013 sur la liberté de la presse et des médias dans le monde ([1]),

— vu ses résolutions concernant des cas urgents de violation des droits de l'homme, de la démocratie et de l'état de droit, où il fait part de ses préoccupations quant aux libertés numériques,

— vu sa résolution du 12 mars 2015 sur les priorités de l'Union européenne en 2015 pour le Conseil des droits de l'homme de l'Organisation des Nations unies ([2]),

— vu sa résolution du 11 février 2015 sur le renouvellement du mandat du Forum sur la gouvernance de l'internet ([3]),

— vu sa résolution du 12 mars 2015 sur le rapport annuel 2013 sur les droits de l'homme et la démocratie dans le monde et la politique de l'Union européenne en la matière ([4]),

— vu la déclaration écrite d'Edward Snowden devant la commission LIBE en mars 2014 ([5]),

— vu la Convention européenne des droits de l'homme et les négociations en cours sur l'adhésion de l'Union européenne à cette dernière,

— vu la charte des droits fondamentaux de l'Union européenne,

— vu l'article 52 de son règlement,

— vu le rapport de la commission des affaires étrangères (A8-0178/2015),

A. considérant que les avancées technologiques et l'accès à l'internet ouvert jouent un rôle de plus en plus important s'agissant de permettre et d'assurer l'épanouissement et le plein respect des droits de l'homme et des libertés fondamentales, et qu'ils exercent une influence positive en élargissant le champ de la liberté d'expression, l'accès à l'information, le droit à la protection de la vie privée et la liberté de réunion et d'association à travers le monde;

B. considérant que les systèmes technologiques peuvent être détournés pour enfreindre les droits de l'homme au travers de la censure, de la surveillance, de l'accès non autorisé à des appareils, du brouillage, de l'interception, du repérage et du traçage d'informations et de personnes;

C. considérant que ces systèmes sont utilisés par des acteurs privés et publics, notamment les pouvoirs publics et les autorités répressives, ainsi que par des organisations criminelles et des réseaux terroristes pour porter atteinte aux droits de l'homme;

D. considérant que le contexte dans lequel les TIC sont conçues et utilisées détermine dans une large mesure leur incidence en tant que facteur de renforcement — ou de violation — des droits de l'homme; que les technologies informatiques, en particulier les logiciels, sont rarement à usage unique et généralement à double usage du point de vue de leur capacité à porter atteinte aux droits de l'homme, et que les logiciels constituent également une forme d'expression;

E. considérant que les TIC ont joué un rôle déterminant dans l'organisation de manifestations et de mouvements sociaux dans plusieurs pays, en particulier des pays soumis à des régimes autoritaires;

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

F. considérant que l'évaluation des répercussions pour les droits de l'homme du contexte dans lequel des technologies seront utilisées est déterminée par la rigueur des cadres juridiques nationaux et régionaux qui réglementent l'utilisation de ces technologies et par la capacité des institutions politiques et judiciaires à contrôler cette utilisation;

G. considérant que, dans le domaine du numérique, les acteurs privés jouent un rôle de plus en plus important dans toutes les sphères d'activité sociale mais que des mesures de sauvegarde n'ont pas encore été mises en place pour les empêcher de restreindre excessivement les droits de l'homme et les libertés fondamentales; que les acteurs privés jouent, dès lors, un rôle plus actif dans l'évaluation de la légalité du contenu et dans le développement de systèmes de cybersécurité et de surveillance qui peuvent être préjudiciables aux droits de l'homme à l'échelle mondiale;

H. considérant que l'internet révolutionne l'échange de données, d'informations et de connaissances de toutes sortes;

I. considérant que le cryptage s'avère être une importante méthode de sécurisation des moyens de communication et de leurs utilisateurs;

J. considérant que la gestion de l'internet a bénéficié d'un processus décisionnel multipartite garantissant une participation réelle, ouverte et responsable de l'ensemble des parties prenantes, notamment des pouvoirs publics, de la société civile, des communautés techniques et universitaires, des entreprises et des utilisateurs;

K. considérant que les services de renseignement contournent systématiquement les protocoles et les produits cryptographiques afin de pouvoir intercepter des communication et des données; que l'agence de sécurité nationale des États-Unis (*National Security Agency*) a répertorié un grand nombre de failles de sécurité informatique encore inconnues du public et des fournisseurs des produits concernés (des failles dites «*zero-day*»); que ces activités mettent à mal les efforts déployés à l'échelle mondiale pour améliorer la sécurité informatique;

L. considérant que les services de renseignement basés dans l'Union européenne participent à des activités qui portent atteinte aux droits de l'homme;

M. considérant qu'au vu de la rapidité des avancées technologiques, les mesures de contrôle et de protection judiciaires et démocratiques sont largement sous-développées;

N. considérant que les mesures de (cyber)sécurité et de lutte contre le terrorisme qui s'appuient sur les TIC ou sur la surveillance de l'internet peuvent avoir des répercussions sensibles sur les droits de l'homme et sur les libertés individuelles des citoyens à l'échelle mondiale, y compris pour les citoyens de l'Union qui résident ou voyagent à l'étranger, particulièrement en l'absence d'un fondement juridique découlant des principes de nécessité, de proportionnalité et de contrôle démocratique et judiciaire;

O. considérant que le filtrage d'internet et la surveillance des communications empêchent les défenseurs des droits de l'homme de recourir à l'internet et de communiquer des informations sensibles, et que ces techniques enfreignent plusieurs articles de la déclaration universelle des droits de l'homme, qui garantit à toute personne le droit à la vie privée et la liberté d'expression;

P. considérant que la sécurité et la liberté numériques sont toutes deux essentielles et qu'elles ne peuvent pas se substituer l'une à l'autre, mais doivent se renforcer mutuellement;

Q. considérant qu'en matière de libertés numériques, l'Union européenne ne peut donner l'exemple que si celles-ci sont garanties au sein-même de l'Union; que l'adoption du train de mesures de l'Union sur la protection des données est par conséquent indispensable;

R. considérant que l'enjeu réside dans d'importants intérêts sociaux, comme la protection des droits fondamentaux, qui ne peuvent être régis par le seul marché et doivent être réglementés;

S. considérant que le respect des droits fondamentaux et de l'état de droit, ainsi qu'un contrôle parlementaire effectif des services de renseignement qui utilisent des technologies de surveillance numérique sont des aspects importants de la coopération internationale;

T. considérant que des entreprises installées dans l'Union européenne détiennent une part importante du marché mondial des technologies de l'information et de la communication, en particulier pour ce qui concerne l'exportation de technologies de surveillance, de repérage, d'intrusion et de contrôle;

U. considérant que le contrôle des exportations ne doit pas entraver la recherche légitime en matière de sécurité informatique ni le développement d'outils de sécurité informatique en l'absence d'intention délictueuse;

1. reconnaît que les droits de l'homme et les libertés fondamentales sont universels et qu'il convient d'en défendre tous les aspects à l'échelle mondiale; insiste sur le fait que la surveillance des communications, en tant que telle, interfère avec le droit au respect de la vie privée et à la liberté d'expression lorsqu'elle ne s'inscrit pas dans un cadre juridique adapté;

2. demande à la Commission de veiller à la cohérence des actions extérieures de l'Union et de ses politiques internes en matière de TIC;

3. estime que la complicité active de certains États membres de l'Union européenne dans la surveillance de masse des citoyens et l'espionnage de responsables politiques par l'agence de sécurité nationale américaine révélés par Edward Snowden ont gravement décrédibilisé la politique de l'Union en matière de droits de l'homme et ébranlé la confiance dans les avantages des TIC à l'échelle mondiale;

4. rappelle aux États membres et aux agences européennes concernées, notamment Europol et Eurojust, qu'ils sont tenus par les obligations découlant de la charte des droits fondamentaux de l'Union européenne et qu'ils ne peuvent, conformément au droit international en matière de droits de l'homme et aux objectifs de l'Union en matière de politique étrangère, ni partager d'informations susceptibles d'entraîner une violation des droits de l'homme dans un pays tiers ni utiliser des informations obtenues par le truchement d'une telle violation en dehors de l'Union, au moyen d'une surveillance illégale, par exemple;

5. souligne que le rôle des technologies dans le renforcement des droits de l'homme devrait être intégré dans l'ensemble des politiques et programmes de l'Union, s'il y a lieu, afin de promouvoir la protection des droits de l'homme, la démocratie, l'état de droit et la bonne gouvernance, ainsi que la résolution pacifique des conflits;

6. préconise l'élaboration et la diffusion actives de technologies qui contribuent à protéger les droits de l'homme et à favoriser les droits, les libertés et la sécurité numériques des citoyens, à promouvoir des pratiques exemplaires et des dispositifs législatifs appropriés ainsi qu'à garantir la sécurité et l'intégrité des données personnelles; exhorte, en particulier, l'Union et ses États membres à promouvoir activement l'utilisation et le développement de normes ouvertes ainsi que de logiciels et de technologies cryptographiques libres et ouverts;

7. invite l'Union à soutenir davantage les acteurs qui s'efforcent d'améliorer les normes de sécurité et de protection de la vie privée en matière de TIC, et ce à tous les niveaux, notamment du matériel, des logiciels et des normes de communication, ainsi que de développer du matériel et des logiciels qui intègrent les principes de protection des données dès la phase de conception;

8. préconise la création d'un fonds pour les droits de l'homme et les technologies dans le cadre de l'instrument européen pour la démocratie et les droits de l'homme;

9. prie instamment l'Union, et en particulier le Service européen pour l'action extérieure, de crypter ses communications avec les défenseurs des droits de l'homme, afin d'éviter de les mettre en danger et d'empêcher que ses propres communications avec des tiers ne soit surveillées;

10. invite l'Union à adopter des logiciels libres et ouverts, ainsi qu'à encourager d'autres acteurs à faire de même, ces logiciels permettant de renforcer la sécurité et d'améliorer le respect des droits de l'homme;

11. souligne qu'il importe, dans une perspective de pacification, de développer les TIC dans les zones de conflits afin d'assurer la sécurité des communications entre les parties impliquées dans la résolution pacifique des conflits;

12. demande que des conditions, des critères de référence et des procédures de déclaration soient appliqués pour veiller à ce que le soutien financier et technique de l'Union au développement de nouvelles technologies dans des pays tiers ne soit pas utilisé en contradiction avec les droits de l'homme;

13. demande à la Commission et au Conseil de coopérer activement avec les pouvoirs publics de pays tiers, d'utiliser les mécanismes de soutien et les instruments stratégiques dont dispose l'Union pour soutenir, former et doter de moyens d'action les défenseurs des droits de l'homme, les militants de la société civile et les journalistes indépendants tributaires de la sécurité des TIC dont ils se servent dans le cadre de leurs activités, ainsi que de promouvoir, dans ce contexte, les droits fondamentaux liés à la vie privée, tels que le libre accès à l'information sur internet, le respect de la vie privée et de la protection des données, la liberté d'expression, la liberté de réunion, la liberté de la presse et la liberté de publication en ligne;

14. attire l'attention sur la situation critique des lanceurs d'alerte et de ceux qui les soutiennent, notamment des journalistes, lorsqu'ils dénoncent des pratiques de surveillance abusives dans des pays tiers; estime qu'il convient de les considérer comme des défenseurs des droits de l'homme qui peuvent, à ce titre, prétendre à la protection de l'Union, conformément aux orientations de l'UE concernant les défenseurs des droits de l'homme; réitère son appel à la Commission et aux États membres pour qu'ils envisagent sérieusement la possibilité d'accorder aux lanceurs d'alertes une protection internationale contre toutes poursuites;

15. déplore que les mesures de sécurité, notamment les mesures de lutte contre le terrorisme, soient de plus en plus fréquemment prétextes à la violation du droit à la vie privée et à la répression des activités légitimes de défenseurs des droits de l'homme, de journalistes et d'activistes politiques; réaffirme sa conviction profonde que la sécurité nationale ne saurait en aucun cas justifier des programmes de surveillance non ciblés, secrets ou de masse; insiste sur le fait que les mesures de surveillance doivent être strictement conformes à l'état de droit et aux droits de l'homme, notamment au respect de la vie privée et à la protection des données;

16. invite le Service européen pour l'action extérieure et la Commission à promouvoir le contrôle démocratique des services de sécurité et de renseignement dans son dialogue politique avec les pays tiers, ainsi que dans ses programmes de coopération au développement; exhorte la Commission à soutenir les organisations de la société civile et les organes législatifs des pays tiers qui œuvrent au renforcement du contrôle, de la transparence et de la responsabilisation de leurs services de sécurité nationaux; préconise l'intégration d'engagements spécifiques en ce sens dans le futur plan d'action de l'Union européenne en matière de droits de l'homme et de démocratisation;

17. prie instamment le Conseil et la Commission de promouvoir les libertés numériques et le libre accès à l'internet dans toutes ses relations avec des pays tiers, y compris dans le cadre des négociations d'adhésion, des négociations commerciales, des dialogues relatifs aux droits de l'homme et des relations diplomatiques;

18. reconnaît que l'internet est devenu un espace public en même temps qu'un espace commercial, au sein duquel la liberté de circulation de l'information et d'accès aux TIC est indispensable; insiste dès lors sur l'importance de promouvoir et, dans le même temps, de protéger la liberté numérique et le libre-échange;

19. préconise l'intégration, dans tous les accords conclus avec des pays tiers, de clauses faisant explicitement référence à la nécessité de promouvoir, de garantir et de respecter les libertés numériques, la neutralité d'internet, le libre accès à l'internet sans aucune forme de censure ni de restriction, le respect de la vie privée et la protection des données;

20. presse l'Union européenne de lutter contre la pénalisation de l'utilisation par les défenseurs des droits de l'homme d'outils de cryptage, de contournement de la censure et de protection de la vie privée, en refusant de restreindre le recours au cryptage au sein de l'Union européenne et en s'opposant aux gouvernements de pays tiers qui engagent des poursuites à ce titre contre des défenseurs des droits de l'homme;

21. exhorte l'Union européenne à lutter contre la pénalisation de l'utilisation d'outils de cryptage, de contournement de la censure et de protection de la vie privée en refusant de restreindre le recours au cryptage au sein de l'Union européenne et en s'opposant aux gouvernements de pays tiers qui pénalisent ces outils;

22. souligne que la politique de l'Union en matière de développement et de droits de l'homme doit, pour être efficace, prendre en compte les TIC à tous les niveaux, et résorber la fracture numérique en fournissant les infrastructures techniques de base, en facilitant l'accès aux connaissances et aux informations nécessaires à l'acquisition des compétences numériques, ainsi qu'en favorisant, s'il y a lieu, l'utilisation de formats de fichier ouverts et de logiciels libres et ouverts afin de garantir l'ouverture et la transparence (des institutions publiques en particulier), y compris en ce qui concerne la protection des données dans la sphère numérique à l'échelle mondiale, ainsi qu'une meilleure compréhension des risques et avantages potentiels liés aux TIC;

23. invite la Commission à contribuer à lever les barrières numériques auxquelles font face les personnes handicapées; considère qu'il est extrêmement important que les politiques de l'Union en faveur du développement et des droits de l'homme dans le monde visent à atténuer la fracture numérique qui touche les personnes handicapées et à étendre les droits de ces dernières, en particulier en ce qui concerne l'accès à la connaissance, la participation numérique et l'accès aux perspectives économiques et sociales qu'ouvre l'internet;

24. insiste sur le fait que la collecte numérique et la diffusion légales de données attestant des violations des droits de l'homme peuvent contribuer à la lutte contre l'impunité et le terrorisme dans le monde; estime que ces données devraient, dans des cas dûment justifiés, être recevables en droit (pénal) international en tant que moyens de preuve devant les tribunaux, dans le respect des garanties internationales, régionales et constitutionnelles; recommande la mise en place, dans le domaine du droit pénal international, de procédures permettant d'authentifier de telles données et de les recueillir en tant que moyens de preuve dans le cadre de procédures judiciaires;

25. déplore que des technologies et services d'information et de communication provenant de l'Union soient vendus dans des pays tiers et puissent y être utilisés par des particuliers, des entreprises ou des autorités dans le but précis de porter atteinte aux droits de l'homme par la censure, la surveillance de masse, le brouillage, l'interception et la surveillance, ou encore le repérage et le suivi des activités de citoyens sur les réseaux de téléphonie (mobile) et sur l'internet; est préoccupé par le fait que des entreprises ayant leur siège dans l'Union puissent fournir des technologies et des services qui permettent de telles violations des droits de l'homme;

26. constate que les menaces de sécurité auxquelles l'Union européenne et ses États membres ainsi que des pays tiers font face émanent souvent d'individus isolés ou de petits groupes qui utilisent les réseaux de communication numériques pour planifier et exécuter des attentats, et que les outils et les tactiques requis pour contrer ces menaces doivent être constamment réexaminés et actualisés;

27. estime que toute surveillance de masse qui n'est pas justifiée par une recrudescence du risque ou des menaces d'attentat est contraire aux principes de nécessité et de proportionnalité et, partant, constitue une violation des droits de l'homme;

28. exhorte les États membres à favoriser un contrôle démocratique rigoureux des opérations des services de renseignement dans les pays tiers afin de veiller à ce qu'ils opèrent dans le strict respect de l'état de droit et à ce que les services et les personnes responsables d'agissements illégaux répondent de leurs actes;

29. encourage les États membres, à la lumière du renforcement de la coopération et de l'échange d'informations avec des pays tiers (y compris en lien avec la surveillance numérique), à assurer un contrôle démocratique des organes compétents en la matière et de leurs activités au moyen d'une supervision appropriée par une entité interne, par le pouvoir exécutif, par le pouvoir judiciaire et par une instance parlementaire indépendante;

30. souligne qu'il convient de définir dans le droit de l'Union des principes de responsabilité sociale des entreprises et des critères de prise en compte des droits de l'homme dès la phase de conception des produits, qui permettent d'élaborer des innovations et des solutions technologiques respectueuses des droits de l'homme, afin de garantir que les fournisseurs de services internet, les développeurs de logiciels, les fabricants de matériel, les services et les médias de réseautage social et les opérateurs de téléphonie mobile, entre autres, tiennent compte des droits fondamentaux des utilisateurs finaux au niveau mondial;

31. presse l'Union d'assurer une plus grande transparence dans la relation entre les opérateurs de téléphonie mobile ou les fournisseurs de services internet et les pouvoirs publics, et d'y inciter les pays tiers dans les relations qu'elle entretient avec eux, en exigeant des opérateurs et des fournisseurs d'accès qu'ils publient des rapports annuels détaillés sur la transparence, notamment sur les mesures que devraient prendre les autorités, ainsi que sur les liens financiers qu'ils entretiennent avec les autorités;

32. rappelle aux entreprises les responsabilités qui leur incombent en matière de respect des droits de l'homme dans l'ensemble de leurs activités à l'échelle mondiale, indépendamment du lieu où se trouvent leurs utilisateurs et du fait que le pays hôte respecte ou non ses obligations en la matière; invite les entreprises du secteur des TIC, notamment celles qui sont implantées dans l'Union européenne, à mettre en œuvre les principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, notamment en mettant en place des procédures de diligence raisonnable, des mécanismes de gestion des risques, ainsi que des procédures permettant de remédier à toutes les incidences négatives sur les droits de l'homme qu'elles peuvent avoir ou auxquelles elles contribuent;

33. insiste sur la nécessité d'accroître l'efficacité de la mise en œuvre et du suivi de la réglementation et des sanctions prévues par le droit de l'Union en matière de TIC, y compris par l'utilisation de clauses dites «attrape-tout» (*catch-all*), de manière à garantir le respect de la législation par toutes les parties, notamment les États membres, ainsi que le maintien de conditions équitables;

34. souligne que le respect des droits fondamentaux est essentiel au succès des dispositifs de lutte contre le terrorisme, notamment des technologies de surveillance numérique;

35. salue les dispositions de l'Arrangement de Wassenaar de décembre 2013 relatives au contrôle des exportations de dispositifs de surveillance, de répression et de collecte d'informations ainsi que de systèmes de surveillance des réseaux; rappelle que le régime de contrôle des biens et technologies à double usage, plus précisément la réglementation européenne y afférente, sont encore très incomplets s'agissant de contrôler efficacement et systématiquement les exportations de TIC sensibles vers des pays non démocratiques;

36. exhorte la Commission, dans le contexte de la révision et de la mise à jour prochaines du régime de contrôle des biens à double usage, à proposer dans les meilleurs délais des stratégies intelligentes et efficaces de limitation et de réglementation des exportations commerciales de services relatifs à la mise en œuvre et à l'utilisation de technologies à double usage, afin de résoudre la question des exportations potentiellement dommageables vers des pays tiers de produits et de services dans le domaine des TIC, conformément à la déclaration commune du Parlement européen, du Conseil et de la Commission d'avril 2014; demande à la Commission d'y inclure des mesures de sauvegarde efficaces afin d'empêcher que le contrôle des exportations ne nuise à la recherche, notamment à la recherche scientifique et à la recherche dans le domaine de la sécurité informatique;

37. souligne que la Commission devrait être à même de fournir rapidement aux entreprises qui s'interrogent sur l'opportunité de demander une autorisation d'exportation, des informations précises et à jour sur la légalité ou les possibles effets dommageables de transactions éventuelles;

38. demande à la Commission de présenter des propositions pour déterminer de quelle manière les normes de l'Union en matière de TIC peuvent être utilisées pour prévenir les effets potentiellement dommageables de l'exportation de ces technologies ou d'autres services vers des pays tiers dans lesquels des notions telles que celle d'«interception légale» ne peuvent être considérées comme équivalentes à celles qui ont cours dans l'Union européenne ou dans lesquels, par exemple, l'état de droit n'est pas appliqué;

Mardi 8 septembre 2015

39. réaffirme que les normes de l'Union, en particulier sa charte des droits fondamentaux, doivent prévaloir lors de l'évaluation d'incidents au cours desquels des technologies à double usage sont utilisées d'une manière susceptible de porter atteinte aux droits de l'homme;

40. préconise d'élaborer des dispositifs de réglementation de la commercialisation des failles «*zero day*» et des moyens de les exploiter afin d'éviter qu'ils ne soient utilisés pour mener des cyberattaques ou pour accéder à des appareils sans autorisation, en violation des droits de fondamentaux, dispositifs qui ne devront toutefois pas avoir d'incidence sensible sur les travaux légitimes de recherche, universitaire notamment, en matière de sécurité;

41. déplore que des entreprises européennes ainsi que des entreprises internationales actives sur le territoire de l'Union qui vendent des technologies à double usage potentiellement préjudiciables aux droits fondamentaux coopèrent activement avec des régimes qui ne respectent pas les droits de l'homme;

42. presse la Commission d'exclure publiquement les entreprises qui se livrent à de telles activités des procédures de passation de marchés de l'Union, des aides au financement de la recherche-développement ainsi que de tout autre soutien financier;

43. invite la Commission à accorder une attention particulière aux droits de l'homme lors de la passation de marchés publics pour l'acquisition d'équipements technologiques, en particulier dans les pays dont les pratiques en la matière ne sont pas fiables;

44. demande à la Commission et au Conseil de s'engager activement en faveur de l'internet ouvert, de procédures décisionnelles multipartites, de la neutralité d'internet, des libertés numériques et de dispositifs de protection des données dans les pays tiers par le truchement de forums sur la gestion de l'internet;

45. condamne l'affaiblissement et l'altération des protocoles et des produits de cryptage, en particulier par les services de renseignement désireux d'intercepter les communications cryptées;

46. met en garde contre la privatisation de la mission de répression des infractions au bénéfice d'entreprises et de fournisseurs de services internet;

47. invite à clarifier les normes et les standards utilisés par les acteurs du secteur privé dans le développement de leurs systèmes;

48. rappelle qu'il importe d'évaluer le contexte dans lequel les technologies sont utilisées pour pouvoir évaluer précisément leurs répercussions sur les droits fondamentaux;

49. demande explicitement de diffuser des outils permettant l'utilisation anonyme ou sous pseudonyme de l'internet, et conteste la vision tronquée selon laquelle ces outils ne serviraient qu'à des fins criminelles et non à donner des moyens d'action aux défenseurs des droits de l'homme dans l'Union européenne et ailleurs;

50. prie instamment le Conseil, la Commission et le Service pour l'action extérieure d'élaborer des stratégies intelligentes et efficaces de réglementation de l'exportation de technologies à double usage, afin de résoudre la question des exportations potentiellement dommageables de produits et de services dans le domaine des TIC au niveau international, dans le cadre de régimes multilatéraux de contrôle des exportations et au sein d'autres instances internationales;

51. insiste sur le fait qu'aucune modification de la réglementation visant à renforcer l'efficacité du contrôle des exportations en lien avec les transferts intangibles de technologie ne doit entraver la recherche légitime ni l'accès à l'information et l'échange de données, et qu'aucune mesure telle que le recours à des autorisations générales d'exportation de l'UE pour la recherche duale ne doit avoir d'effet dissuasif sur les particuliers et les PME;

52. invite les États membres à veiller à ce que les politiques de contrôle des exportations existantes et futures ne restreignent pas les travaux de recherche légitimes en matière de sécurité, et à ce que ces contrôles soient mis en œuvre de bonne foi et uniquement pour l'exportation de technologies clairement définies destinées à être utilisées pour la surveillance de masse, la censure, le brouillage, l'interception et la surveillance, ou encore le repérage et le suivi des activités de citoyens sur les réseaux de téléphonie (mobile);

53. rappelle que les technologies ad hoc sans fil à structure maillée («*mesh*») se prêtent particulièrement à la mise en place de réseaux secondaires dans les zones où l'internet est indisponible ou bloqué, et qu'elles peuvent contribuer à l'action en faveur des droits de l'homme;

54. invite la Commission à désigner un groupe d'experts indépendants chargé d'évaluer l'incidence sur les droits de l'homme des normes européennes en matière de TIC et de formuler des recommandations en vue d'ajustements destinés à renforcer la protection des droits de l'homme, en particulier lors de l'exportation de systèmes;

55. reconnaît que le progrès technologique constitue un défi pour les systèmes juridiques, qui doivent s'adapter à des situations nouvelles; insiste sur la nécessité, pour les législateurs, de prendre davantage en considération les questions liées à l'économie numérique;

56. demande à la Commission de veiller à la participation de la société civile et d'experts indépendants dans le domaine des TIC dans les pays tiers, notamment de chercheurs en matière de sécurité, afin de s'adjoindre des compétences de pointe en vue de l'élaboration de politiques à l'épreuve du temps;

57. insiste sur la nécessité de prévenir tout effet indésirable, de restriction ou de dissuasion, par exemple, sur la recherche scientifique et d'autres activités légitimes de recherche et développement, sur l'échange d'informations ou l'accès à celles-ci, sur le développement des connaissances en matière de sécurité ou encore sur l'exportation de technologies nécessaires à l'acquisition des compétences numériques fondamentales et à l'action en faveur des droits de l'homme;

58. est convaincu que la coopération dans le domaine numérique entre les pouvoirs publics et les acteurs privés à l'échelle mondiale, notamment au sein du Forum sur la gouvernance de l'internet, nécessite un équilibre des pouvoirs clairement défini et ne doit pas nuire au contrôle démocratique et judiciaire;

59. relève que des dispositions facultatives sont insuffisantes et que des mesures contraignantes sont nécessaires pour inciter les entreprises à prendre en considération le bilan d'un pays donné en matière de droits de l'homme avant d'y vendre leurs produits, ainsi qu'à évaluer l'incidence de leurs technologies sur les défenseurs des droits de l'homme et les figures de l'opposition;

60. est d'avis que l'exportation de biens hautement sensibles doit être contrôlée avant que ceux-ci ne quittent le territoire de l'Union, et que des sanctions sont nécessaires en cas d'infraction;

61. demande l'autorisation du cryptage pour tous, ainsi que la mise en place des conditions nécessaires à l'autorisation du cryptage; estime que les contrôles devraient être assurés par l'utilisateur final, qui doit disposer des compétences requises pour ce faire;

62. demande la mise en place systématique de normes de cryptage de bout en bout pour tous les services de communication afin d'en rendre le contenu plus difficilement accessible pour les pouvoirs publics, les services de renseignement et les organismes de surveillance;

63. souligne qu'il incombe particulièrement aux services de renseignement de restaurer la confiance et demande qu'il soit mis un terme à la surveillance de masse; estime que des mesures doivent être prises pour mettre un terme à la surveillance des citoyens européens par des services de renseignement nationaux et étrangers;

64. s'oppose à ce que des technologies de surveillance et des outils de censure européens soient vendus et mis à la disposition de régimes autoritaires qui n'appliquent pas l'état de droit;

65. préconise d'étendre la protection internationale des lanceurs d'alerte et encourage les États membres à adopter des lois pour les protéger;

66. demande qu'un envoyé spécial de l'ONU pour les libertés numériques et la protection des données soit désigné et que le portefeuille du commissaire aux droits de l'homme du Conseil de l'Europe soit étendu afin que la technologie soit également abordée sous l'angle des droits de l'homme;

67. réclame des mesures garantissant la protection de la vie privée des militants, journalistes et citoyens dans le monde entier et leur permettant de constituer des réseaux via internet;

68. met l'accent sur le fait qu'il convient de reconnaître l'accès à internet comme un droit fondamental et réclame des mesures pour résorber la fracture numérique;

69. charge son Président de transmettre la présente résolution au Conseil, à la Commission, à la vice-présidente de la Commission/haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ainsi qu'au Service européen pour l'action extérieure.