Droits de l'homme et technologies: incidences des systèmes de détection des intrusions et de surveillance sur les droits de l'homme dans les pays tiers

2014/2232(INI) - 08/09/2015 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 371 voix pour, 293 voix contre et 43 abstentions, une résolution 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.

Le Parlement rappelle que les avancées technologiques et l'accès à l'internet ouvert jouent un rôle de plus en plus important pour assurer l'épanouissement et le plein respect des droits de l'homme et la liberté d'expression.

Les Technologies de l'Information de la Communication (TIC) constituent toutefois un outil de renseignement qui permet d'intercepter des communications et des données comme l'a fait l'Agence de sécurité nationale des États-Unis (National Security Agency - NSA). Ces activités de surveillance des communications ont interféré avec le droit au respect de la vie privée et avec la liberté d'expression. En conséquence, le Parlement indique que la complicité active de certains États membres de l'Union dans la surveillance de masse des citoyens et l'espionnage de responsables politiques par la NSA 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.

Il appelle à plus de cohérence en la matière par l'UE 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. Il 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 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.

Pour des logiciels cryptés : le Parlement prie l'Union, et en particulier le Service européen pour l'action extérieure (SEAE), de crypter les communications avec les défenseurs des droits de l'homme, afin d'éviter de les mettre en danger et d'empêcher que les propres communications du SEAE avec des tiers ne soient surveillées. Il invite parallèlement l'Union à adopter des logiciels libres et ouverts, ainsi qu'à encourager d'autres acteurs à faire de même.

Le Parlement appelle en outre à la formation des défenseurs des droits de l'homme, des militants de la société civile et des journalistes, aux TIC.

Lanceurs d'alerte : le Parlement 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. Il estime qu'il convient de les considérer comme des défenseurs des droits de l'homme et 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.

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

Lutte contre la terrorisme et protection de la vie privée : le Parlement 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. Pour le Parlement, **la sécurité nationale ne saurait en aucun cas justifier des programmes de surveillance non ciblés, secrets ou de masse**.

Le Parlement 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. Il 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.

Lutter contre la pénalisation des outils de cryptage : le Parlement presse l'Union de 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.

Contrôle démocratique : le Parlement 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. Il exhorte dès lors les États membres à favoriser **un contrôle démocratique rigoureux des opérations des services de renseignement dans les pays tiers**.

Il presse également 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, en exigeant des opérateurs et des fournisseurs d'accès qu'ils publient des rapports annuels détaillés sur la transparence.

Il 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. D’une manière générale, le Parlement souligne que le respect des droits fondamentaux est essentiel au succès des dispositifs de lutte contre le terrorisme, notamment des technologies de surveillance numérique.

Biens à double usage : le Parlement exhorte la Commission à proposer 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** . Il 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.

Il 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. Il déplore que des entreprises européennes ainsi que des entreprises internationales actives sur le territoire de l'Union qui vendent des technologies à double usage coopèrent avec des régimes qui ne respectent pas les droits de l'homme. Il appelle la Commission à **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.

Neutralité d’internet : le Parlement 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. Il 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.

Il 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 renforcer les droits de l'homme.

Cryptage pour tous : le Parlement demande l'autorisation du **cryptage pour tous**, ainsi que la mise en place des conditions nécessaires à l'autorisation du cryptage. Les contrôles devraient être assurés par l'utilisateur final, qui devrait disposer des compétences requises pour ce faire. Il demande en outre 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. Il 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**.

Il condamne enfin 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.