



Résolution 1986 (2014)¹

Version finale

Améliorer la protection et la sécurité des utilisateurs dans le cyberspace

Assemblée parlementaire

1. L'Assemblée parlementaire craint que le développement et l'exploitation futurs du cyberspace se poursuivent sans une protection suffisante des droits et des intérêts de la partie intéressée la plus vulnérable: l'utilisateur individuel.
2. Les nombreuses intrusions des pouvoirs publics, de sociétés commerciales, mais aussi de particuliers dans les données à caractère personnel et la correspondance des utilisateurs de services en ligne suscitent des inquiétudes chez ces derniers. On peut citer, parmi les affaires très médiatisées, l'interception de communications et l'exploration de données d'utilisateurs par des services de sécurité nationale en Europe et aux Etats-Unis, l'extraction professionnelle de données sur des réseaux sociaux en ligne, le profilage commercial d'utilisateurs par des fournisseurs de services en ligne au moyen de données d'accès à internet et de données de géolocalisation, ainsi que le piratage à grande échelle de comptes et de mots de passe d'utilisateurs à des fins frauduleuses.
3. L'Assemblée regrette que ces attaques contre la sécurité et l'intégrité des services de communication en ligne et mobiles aient profondément ébranlé la confiance des utilisateurs dans les services internet. Par conséquent, elle invite tous les Etats membres et observateurs à lancer immédiatement, en coopération avec l'industrie de l'internet et en ligne, une initiative mondiale pour l'amélioration de la protection et de la sécurité des utilisateurs dans le cyberspace. L'internet n'a pas de frontières nationales, nous devons donc agir ensemble pour garantir le respect des droits de l'homme universels, ainsi que du droit national et de la souveraineté. L'objectif visé doit être un cadre juridique accepté internationalement, assorti de mécanismes de contrôle adéquats, dont la protection des donneurs d'alerte qui divulguent les violations commises.
4. L'Assemblée se félicite donc de la Résolution sur le droit à la vie privée à l'ère du numérique, adoptée par l'Assemblée générale des Nations Unies le 18 décembre 2013. L'Assemblée convient que les mêmes droits dont dispose toute personne à l'extérieur du cyberspace doivent également être protégés en ligne, en particulier le droit à la vie privée, ainsi qu'elle l'a exprimé dans sa [Résolution 1843 \(2011\)](#) sur la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne.
5. Se félicitant de la Déclaration de Montevideo du 7 octobre 2013 sur l'avenir de la coopération pour l'internet, l'Assemblée reconnaît que la mondialisation de l'Internet Corporation for Assigned Names and Numbers (ICANN) et son Internet Assigned Numbers Authority (IANA) doit être accélérée, vers un environnement dans lequel toutes les parties prenantes, y compris les gouvernements, participent sur un pied d'égalité. Les associations d'utilisateurs et de citoyens devraient être représentées dans cette nouvelle structure. La gouvernance mondiale de l'internet sera améliorée. Une charte internationale sur les principes et objectifs globaux de l'internet sera élaborée. Elle garantira notamment le respect des données personnelles, y

1. *Discussion par l'Assemblée* le 9 avril 2014 (14e séance) (voir [Doc. 13451](#), rapport de la commission de la culture, de la science, de l'éducation et des médias, rapporteur: M. Axel E. Fischer; et [Doc. 13481](#), avis de la commission des questions juridiques et des droits de l'homme, rapporteur: M. Arcadio Díaz Tejera). *Texte adopté par l'Assemblée* le 9 avril 2014 (14e séance).

Voir également la [Recommandation 2041 \(2014\)](#).



compris biologiques, et le respect de droits de l'homme. Ce processus devrait être soutenu par le Conseil de l'Europe au niveau de l'Union européenne et des Nations Unies pour garantir l'indépendance de l'infrastructure essentielle d'internet à l'égard des gouvernements.

6. L'Assemblée recommande que tous les Etats membres et observateurs veillent à la mise en œuvre effective des principes suivants:

6.1. la vie privée, la correspondance et les données à caractère personnel de chacun doivent être protégées en ligne; les utilisateurs ont la possibilité permanente de retirer des données, des contenus et des informations; les pouvoirs publics, les sociétés commerciales ou les particuliers ne peuvent procéder à l'interception, à la surveillance, au profilage ou à l'archivage de données d'utilisateurs que si la loi les y autorise, conformément à l'article 8 de la Convention européenne des droits de l'homme (STE n° 5); les Etats membres ont l'obligation positive d'assurer une protection juridique adéquate contre l'interception, la surveillance, le profilage et l'archivage de données d'utilisateurs; les archives des données à caractère personnel doivent faire l'objet de mesures de précaution pour être protégées contre le vol et l'utilisation frauduleuse de données;

6.2. la collecte, la conservation et le traitement des métadonnées (données qui décrivent d'autres données, par exemple les informations relatives à l'expéditeur, au destinataire, à l'horaire, aux mots-clés, aux déplacements et aux contacts) doivent faire l'objet, en principe, des mêmes règles que la collecte, la conservation et le traitement de n'importe quelle autre donnée à caractère personnel;

6.3. les fabricants de dispositifs d'accès et les fournisseurs de services en ligne devraient automatiquement appliquer des technologies de cryptage et d'accès conditionnel ainsi que des outils pour combattre les virus en ligne et les témoins de connexion (*cookies*); la durée de vie de ces derniers devrait être limitée dans le temps; une protection spéciale devrait être garantie par les fournisseurs de points d'accès sans fil (*hotspots*), également en ce qui concerne les données à caractère personnel produites par le biais de «l'internet des objets»; des normes ISO (Organisation internationale de normalisation) devraient être développées à cet égard; il est nécessaire de fournir aux utilisateurs d'internet des informations transparentes et accessibles sur les mesures de sécurité et les mécanismes appliqués;

6.4. les autorités nationales compétentes doivent lutter efficacement contre les activités criminelles perpétrées sur des services en ligne ou par le biais de ces derniers, dans le respect de l'article 8 de la Convention européenne des droits de l'homme; les usagers qui respectent la législation ont le droit de rester anonymes, alors que ceux qui l'enfreignent doivent être identifiables et les auteurs d'infractions doivent pouvoir être identifiés par les services répressifs, dans le respect des garanties légales exigées par la Convention européenne des droits de l'homme; pour lutter contre le vol d'identité en ligne, le recours à l'identification réelle doit être prévu soit par signature électronique, soit en utilisant des outils d'authentification, soit par un tiers de confiance;

6.5. des *hotlines* ou autres systèmes d'assistance en ligne destinés aux enfants et aux personnes ayant des besoins spéciaux devraient être mis en place par les pouvoirs publics et les fournisseurs de services en ligne, notamment en ce qui concerne le cyberharcèlement et les abus des enfants en ligne;

6.6. la protection de la propriété doit être respectée en ligne; les fournisseurs de services en ligne devraient offrir la possibilité de joindre des signatures électroniques ou d'appliquer des outils d'authentification électronique à du contenu et des services en ligne; les fournisseurs de services d'informatique dématérialisée (*cloud computing*) devraient automatiquement appliquer des mesures de protection spéciale pour les biens qu'ils conservent, y compris des outils d'accès conditionnel et l'archivage régulier des sauvegardes;

6.7. les fournisseurs de services d'informatique dématérialisée ne doivent pas réduire les droits et la protection de leurs utilisateurs par la délocalisation de leur «nuage de données» en dehors de la juridiction applicable à leur entreprise; le système juridique et fiscal applicable à des services en ligne doit être celui du consommateur final et les droits du consommateur qui s'appliquent doivent être ceux les plus favorables entre le pays d'origine et le pays de service;

6.8. les Etats membres devraient mettre en place un cadre réglementaire adéquat pour les services de jeu en ligne, indépendamment du fait que ces services de jeux sont offerts par des entreprises publiques ou privées; les services de jeu en ligne ayant leur siège dans un pays, qui sont accessibles et destinés aux utilisateurs dans un autre pays, devraient être soumis à la juridiction de ce dernier;

6.9. les fournisseurs de services commerciaux ou institutionnels doivent avoir l'obligation légale d'indiquer à leurs utilisateurs leur dénomination, leur siège social et leur représentant légal ou directeur, et de les informer de leur politique en matière de protection et de sécurité des utilisateurs, notamment en ce qui concerne la protection de la vie privée, de la correspondance, des données à caractère personnel et de la propriété de l'utilisateur;

6.10. les utilisateurs de services en ligne doivent être suffisamment informés sur leurs droits par leur fournisseur de services, que ces services soient fournis par une autorité publique ou par une entité privée; la renonciation à des droits par les utilisateurs en faveur des prestataires de services devrait nécessiter le consentement préalable, éclairé et exprès des utilisateurs;

6.11. les utilisateurs de services en ligne doivent disposer de recours effectifs devant une instance nationale contre des violations de leurs droits, compte tenu des articles 6 et 13 de la Convention européenne des droits de l'homme, ainsi que de l'article 2 du Pacte international des Nations Unies relatif aux droits civils et politiques;

6.12. les fournisseurs de services commerciaux ou institutionnels devraient offrir à leurs utilisateurs la possibilité de déposer des réclamations et de régler des différends à l'amiable, notamment par le biais de centres nationaux ou européens de protection des consommateurs, d'organismes pour la résolution de litiges en ligne; et un médiateur du citoyen («ombudsman») facilement joignable, ayant obligation de réponse, devrait être nommé par chaque fournisseur d'accès à internet ou par leur association nationale;

6.13. le secret de la correspondance privée des employés transmise par le biais des moyens de communication de leur employeur est protégé par l'article 8 de la Convention européenne des droits de l'homme; les contrats de travail devraient interdire toute interférence, conformément à la Recommandation n° R (89) 2 du Comité des Ministres sur la protection de données à caractère personnel utilisées à des fins d'emploi.

7. Les gouvernements et les fournisseurs d'accès devraient engager un plan ambitieux d'éducation des utilisateurs aux opérations de sécurisation.

8. L'Assemblée invite l'EuroISPA (association européenne des fournisseurs d'accès à internet) et ses membres nationaux à établir un code de conduite commun en tenant compte des principes fondamentaux susmentionnés sur la protection et la sécurité des utilisateurs d'internet dans le cyberspace. Les fournisseurs de services internet et les autorités de police devraient disposer d'un cadre juridique pour leur coopération pratique face aux attaques contre les droits et la sécurité des utilisateurs de l'internet et des médias en ligne.

9. L'Assemblée invite le Haut-Commissaire des Nations Unies pour les droits de l'homme à coopérer avec le Conseil de l'Europe et à se référer à la présente résolution, ainsi qu'à la [Résolution 1843 \(2011\)](#) sur la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne, lors de la préparation de son rapport sur la protection et la promotion du droit à la vie privée pour le Conseil des droits de l'homme des Nations Unies et la 69e session de l'Assemblée générale des Nations Unies en 2014-2015.

10. L'Assemblée invite le groupe consultatif multipartite pour la préparation du prochain Forum sur la gouvernance de l'internet (Istanbul, 2-5 septembre 2014) à accorder une attention particulière aux questions relatives à la protection et la sécurité des utilisateurs d'internet dans le cyberspace, en particulier le droit à la protection de la vie privée et des données à caractère personnel.

11. L'Assemblée invite l'Union internationale des télécommunications à élaborer des normes techniques mondiales sur l'intégrité, la sécurité et la confidentialité des communications en ligne et mobiles, fondées sur l'article 17 du Pacte international des Nations Unies relatif aux droits civils et politiques, et prenant en compte les dispositions des traités régionaux pertinents.