Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc.
12 mars 2014

Améliorer la protection et la sécurité des utilisateurs dans le cyberespace

Rapport[1]
Commission de la culture, de la science, de l'éducation et des médias
Rapporteur: M. Axel E. FISCHER, Allemagne, Groupe du parti populaire européen

A. Projet de résolution[2]

1. L'Assemblée parlementaire craint que le développement et l'exploitation du cyberspace ne 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 notamment citer, parmi les affaires très médiatisées : l'interception de communications et l'exploration de données d'utilisateurs par l'intermédiaire de services de sécurité nationale en Europe et aux Etats-Unis, l'extraction professionnel 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 sur la sécurité et l'intégrité des services de communication en ligne et mobiles aient profondément ébranlé la confiance des utilisateurs dans les services informatiques. Par conséquent, l'Assemblée invite tous les Etats membres et observateurs de 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 cyberespace. L'Internet n'a pas de frontières nationales, nous devons donc agir ensemble.

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 reconnaît que les mêmes droits que toute personne a à l'extérieur cyberespace doivent également être protégés en ligne, en particulier le droit à la vie privée, étant reconnu 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 concernant l'Internet, l'Assemblée reconnaît que la mondialisation de l'*Internet Corporation for Assigned Names et 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 dans une position égale.

6. L'Assemblée recommande que tous les Etats membres et observateurs veilleront 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 pouvoirs publics, les sociétés commerciales ou les particuliers ne peuvent procéder à l'interception, à l'exploration, au profilage et à l'archivage de données d'utilisateurs que si la loi les y

[1] Renvoi en commission: Doc 12585, Renvoi 3772 du 27.05.2011.
[2] Projet de résolution adopté par la commission le 11 mars 2014.

autorise conformément à l'article 8 de la Convention européenne des droits de l'homme (STE n° 5) ; les États membres ont l'obligation positive d'assurer une protection juridique adéquate contre l'interception, l'exploration, le profilage et l'archivage de données d'utilisateurs ; les archives des données à caractère personnel doivent avoir recours à des mesures de précaution pour protéger leur base de données contre le vol et l'utilisation frauduleuse de données ;

6.2. 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* ») ; 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 ;

6.3. 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 ;

6.4. 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 cyber-harcèlement et les abus des enfants en ligne ;

6.5. la protection de la propriété doit être respectée en ligne ; les fournisseurs de services en ligne doivent 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 ;

6.6. 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 ;

6.7. les États 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 ; services de jeu en ligne ayant leur siège dans un pays, qui sont accessibles pour et destiné aux utilisateurs en un autre pays, doivent être sous la juridiction de ces derniers ;

6.8. 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 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 ;

6.9. 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 une entité privée ; la renonciation à des droits par les utilisateurs en faveur des prestataires de services nécessite le consentement préalable, éclairé et exprès par les utilisateurs ;

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

6.11. 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 de médiateurs internes ;

6.12. 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 atteinte 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. L'Assemblée invite l'Association des fournisseurs d'accès Internet européen (EuroISPA) et leurs membres nationaux à établir un code de conduite commun en tenant compte des principes fondamentaux susmentionnés sur la protection et la sécurité des utilisateurs dans le cyberespace. Les fournisseurs de services Internet et les autorités de police devraient avoir 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.

8. L'Assemblée invite le Haut-commissaire des Nations Unies pour les droits de l'homme à coopérer avec le Conseil de l'Europe et se référer à la présente résolution ainsi que 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 et la soixante-neuvième session de l'Assemblée générale des Nations Unies en 2014-2015.

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

10. L'Assemblée invite l'Union internationale des télécommunications d'élaborer des normes techniques mondiales sur l'intégrité, la sécurité et la confidentialité des communications en ligne et mobiles, qui sont fondés sur l'article 17 du Pacte international des Nations Unies relatif aux droits civils et politiques ainsi que la Convention du Conseil de l'Europe sur la cybercriminalité et la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

B. Projet de recommandation[3]

1. Se référant à sa Résolution .... (2014) sur l'amélioration de la protection et de la sécurité des utilisateurs dans le cyberespace, l'Assemblée parlementaire souligne l'importance de renforcer l'action intergouvernementale du Conseil de l'Europe dans ce domaine.

2. L'Assemblée, se félicitant de la Stratégie 2012-2015 du Comité des Ministres sur la gouvernance de l'internet et des nombreuses initiatives qu'il a déjà prises dans ce domaine, recommande au Comité des Ministres :

2.1. d'examiner la possibilité d'élaborer un protocole additionnel à la Convention sur la cybercriminalité (STE n° 185) concernant les violations graves des droits fondamentaux des utilisateurs de services en ligne ;

2.2. de déterminer dans quelle mesure la Convention européenne sur l'entraide judiciaire en matière pénale (STE n° 30) doit être actualisée afin de couvrir les affaires de cybercriminalité transnationale ainsi que les cyber preuves ;

2.3. de déterminer dans quelle mesure la Convention sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel (STE n° 178) peut être utilisée pour améliorer la sécurité des systèmes d'accès conditionnel pour les services en ligne, notamment en ce qui concerne les services d'informatique dématérialisée (« *cloud computing* ») ;

2.4. d'assister les Etats membres dans la mise en œuvre de la Convention sur la cybercriminalité et de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) ;

2.5. d'achever d'urgence la révision actuelle de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, en tenant compte de la Recommandation 1984 (2011) de l'Assemblée ;

2.6. de soutenir et coordonner une approche pan-européenne à la mondialisation de la Société pour les noms et numéros assignés de l'internet (ICANN) et son Autorité de numéros assignés (IANA), comme indiqué dans la Déclaration de Montevideo sur l'avenir de la coopération d'internet du 7 octobre 2013 ;

2.7. d'inviter ses Etats observateurs à travailler activement avec le Conseil de l'Europe en vue d'améliorer la protection et la sécurité des utilisateurs dans le cyberespace, et de leur demander de mettre en place des initiatives conjointes avec le Conseil de l'Europe à cet égard ;

2.8. d'inviter l'Union européenne à adhérer à la Convention sur la cybercriminalité ainsi que la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de demander aux parties à ces conventions de préparer activement ce processus.

[3] Projet de recommandation adopté par la commission le 11 mars 2014.

C. Exposé des motifs, par M. Axel FISCHER (Allemagne, PPE/DC), rapporteur

1. Mandat du rapport

1. Ayant déposé en avril 2011 la proposition de Résolution intitulée « Améliorer la protection et la sécurité des utilisateurs dans le cyberespace » (doc. 12585), j'ai été désigné rapporteur de la commission de la culture, de la science, de l'éducation et des médias le 23 juin 2011.

2. A la suite du débat d'actualité sur « l'ingérence de l'Etat dans la vie privée sur internet » tenu par l'Assemblée parlementaire le 27 juin 2013, le Bureau de l'Assemblée a décidé d'inclure le suivi de cette question dans le présent rapport. Le débat de l'Assemblée du 27 juin a été déclenché par l'affaire PRISM/Snowden.

2. Travaux préparatoires

3. La sous-commission des médias et de la société de l'information de l'Assemblée a organisé une audition à Strasbourg le 25 janvier 2012 avec M. John Carr OBE (secrétaire de la Children's Charities' Coalition on Internet Safety, Londres), Mme Catarina Katzer (présidente de l'Association contre le cyberharcèlement, Cologne) et M. Stefan Herwig (associé, Mindbase Strategic Consulting, Gelsenkirchen).

4. Conformément à mes instructions thématiques, la rédaction d'un rapport de fond technique a ensuite été confiée à M. Kei Ishii (Université technique de Berlin) et celle d'un rapport de fond juridique au Professeur Hans Schulte-Nölke (Université d'Osnabrück). Ces deux rapports, qui ont été présentés par leurs auteurs à la sous-commission des médias et de la société de l'information le 2 octobre 2012, ont servi de base à l'élaboration, en partie, du présent exposé. Je tiens à remercier tout particulièrement ces deux experts ainsi que les membres de la sous-commission pour leurs contributions.

5. La Commission de la culture, de la science, de l'éducation et des médias a examiné mon avant-projet de rapport à Paris le 11 mars 2013 et a tenu un échange de vues avec le Professeur Wolfgang Schulz, Directeur de l'Institut Hans Bredow pour la recherche sur les médias (Hambourg) et M. Thomas Spiller, vice-président de la Global Public Policy EMEA pour Walt Disney Company (Bruxelles), qui est intervenu en qualité d'expert de la Chambre de commerce internationale (Paris).

6. Le 1er octobre 2013, la commission a organisé une audition à Strasbourg sur l'ingérence de l'Etat dans la vie privée sur internet, avec la participation de Mme Dorothée Belz, vice-présidente de Microsoft Europe, M. Duncan Campbell, journaliste d'investigation et expert juridique, ainsi que M. Lawrence Early, jurisconsulte de la Cour européenne des droits de l'homme.

7. Je me suis aussi appuyé sur mon travail parlementaire en qualité de président de la commission d'enquête sur l'internet et la société numérique du Parlement allemand, qui a achevé ses travaux le 28 janvier 2013 et a adopté, entre autres, un rapport sur la protection des utilisateurs[4].

3. Normes du Conseil de l'Europe et autres normes internationales

8. La Convention européenne des droits de l'homme et son premier protocole (STE n° 5 et 9) garantissent aussi aux utilisateurs de services en ligne le droit à la liberté d'expression et d'information, le droit au respect de la vie privée et à la protection des données à caractère personnel ainsi que le droit à la protection de la propriété.

9. La Convention sur la cybercriminalité (STE n° 185) offre une protection supplémentaire, en érigeant en infraction pénale l'accès et l'atteinte, sans droit, aux systèmes ou données informatiques, ainsi que leur interception illégale. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son protocole additionnel (STE n°108 et 181) offrent aussi des garanties supplémentaires. Les deux conventions définissent des normes juridiques sur l'entraide judiciaire entre les parties.

10. La Convention européenne d'entraide judiciaire en matière pénale (STE n° 30) de 1959 établit le cadre d'assistance juridique dans des affaires pénales transnationales, y compris en matière de cybercriminalité. Dans ce contexte, d'importants travaux connexes sont actuellement menés dans le cadre de la Convention sur la cybercriminalité dans le but d'élaborer un protocole additionnel sur la compétence et

[4] Voir http://www.bundestag.de/internetenquete/dokumentation/Sitzungen/20130128/20_Sitzung_2013-01-28_PGVS_Zwischenbericht.pdf

l'accès transfrontalier aux données et flux de données. Ce protocole permettra de clarifier et d'étendre l'article 32 de la Convention sur la cybercriminalité, qui porte sur l'accès transfrontière à des données informatiques stockées, avec consentement ou lorsqu'elles sont accessibles au public.

11. Les données à caractère personnel, la correspondance et les biens des utilisateurs sont souvent protégés par des systèmes d'accès conditionnel aux services en ligne, tels que des mots de passe ou des outils d'authentification électronique. La reproduction ou l'utilisation illicites de ces dispositifs d'accès conditionnel sont passibles de sanctions, comme le prévoit la Convention sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel (STE n° 178).

12. Etant donné que des produits médicaux contrefaits sont souvent vendus par le biais d'internet, la protection de l'utilisateur à cet égard est garantie par la Convention sur la contrefaçon des produits médicaux et les infractions similaires menaçant la santé publique (STCE n° 211).

13. La protection de l'intégrité physique et morale des enfants est garantie par la Convention sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201) et l'article 9 de la Convention sur la cybercriminalité.

14. Le Comité des Ministres du Conseil de l'Europe a adopté des recommandations sur :

- la protection de la liberté d'expression et de la liberté de réunion et d'association en ce qui concerne les plates-formes internet gérées par des exploitants privés et les prestataires de services en ligne (2011)
- la protection et la promotion de l'universalité, de l'intégrité et de l'ouverture de l'internet (2011)
- la protection des droits de l'homme dans le cadre des services de réseaux sociaux (2012)
- la protection des droits de l'homme dans le contexte des moteurs de recherche (2012)

ainsi que des lignes directrices sur :

- les fournisseurs de services internet (2008), élaborées en coopération avec l'Association européenne des fournisseurs de services internet,
- les fournisseurs de jeux en ligne (2008), élaborées en coopération avec la Fédération européenne des éditeurs de logiciels interactifs.

15. L'Organisation pour la coopération et le développement économique (OCDE) a élaboré des normes non contraignantes mais qui présentent un intérêt direct : les Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique (1999), les Lignes directrices régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses (2003) et la Recommandation sur le règlement des litiges de consommation et leur réparation (2007).

16. Dans l'Union européenne, la législation pertinente comprend la directive sur les ventes aux consommateurs (1999/44/CE), la directive sur les signatures électroniques (1999/93/CE), la directive sur le commerce électronique (2000/31/CE), la directive vie privée et communications électroniques 2002/58/CE (modifiée par la directive 2009/136/CE), la directive relative aux pratiques commerciales déloyales (2005/29/CE), la directive relative aux droits des consommateurs (2011/83/UE) et la directive relative aux attaques contre les systèmes d'information (2013/40/UE).

4. Ingérence de l'Etat dans la vie privée sur internet

17. Le débat public d'actualité concernant le programme PRISM de l'Agence de sécurité nationale des Etats-Unis et, dans ce cadre, la coopération avec les services de sécurité en Europe, reflète des approches internationales différentes de la protection des données à caractère personnel vis-à-vis de la protection de la sécurité nationale et du maintien de l'ordre. Sur la base de documents qui auraient été divulgués par Edward Snowden à l'hebdomadaire The Observer, le Guardian a indiqué que « outre le Royaume-Uni – le Danemark, les Pays-Bas, la France, l'Allemagne, l'Espagne et l'Italie ont tous passé des accords officiels pour fournir aux Etats-Unis des données relatives aux communications. Il est précisé dans ces documents que ces Etats membres de l'UE, jugés plus ou moins dignes de confiance par les Etats-Unis, ont conclu, il y a plusieurs décennies, des accords d'échange de renseignements d'origine électromagnétique (Sigint) en vertu desquels ils sont tenus de fournir des données qui, des années plus tard, selon les experts, ont fini par inclure des données relatives aux téléphones portables et à l'internet »[5].

[5] Voir The Guardian (30 juin 2013), à l'adresse http://www.theguardian.com/world/2013/jun/30/nsa-spying-europe-claims-us-eu-trade

18. Dans ce contexte, il convient de mentionner les travaux de l'Assemblée qui ont donné lieu à la Résolution 1843 et à la Recommandation 1984 (2011) sur la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne, qui s'appuient sur un rapport de M^me^ Andreja Rihter (Slovénie, SOC), ainsi qu'à la Résolution 1877 et à la Recommandation 1998 (2012) sur la protection de la liberté d'expression et d'information sur l'internet et les médias en ligne, qui s'appuient sur un rapport de M^me^ Zaruhi Postanjyan (Arménie, PPE/DC).

19. Il y a plus de dix ans, un débat public similaire avait été tenu sur l'interception alléguée de communications radio et satellite par les Etats-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande. Le Parlement européen a analysé cette situation dans son rapport et sa résolution de 2001 sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)[6]. Même si les possibilités d'exploration à grande échelle de données relatives aux communications en ligne, au trafic et autres métadonnées étaient alors moins développées, les résultats du débat ECHELON présentent toujours un grand intérêt dans le débat d'actualité concernant le programme PRISM.

20. Le développement rapide des communications électroniques à l'échelle mondiale a permis aux services de sécurité nationale et aux services de police d'axer leurs efforts sur les services informatiques afin d'identifier et de localiser les terroristes ou autres criminels dangereux qui utilisent ces services. Benjamin Franklin, ancien président des Etats-Unis, a déclaré : « Celui qui sacrifie sa liberté au profit de sa sécurité ne mérite ni l'une ni l'autre ». Dans un débat sur les droits de l'homme aujourd'hui, nul ne sacrifierait un droit humain au profit d'un autre, mais définirait les deux en les mettant en corrélation.

21. Bien que l'article 8 de la Convention européenne des droits de l'homme protège aussi les données à caractère personnel en ligne, la sécurité nationale peut limiter ce droit. Les Etats-Unis ne sont pas partie à la Convention européenne des droits de l'homme, mais ils sont liés par l'article 17 correspondant du Pacte international des Nations Unies relatif aux droits civils et politiques. Les Etats membres du Conseil de l'Europe qui collaborent au programme PRISM sont eux liés par la Convention européenne. Toute ingérence pour des motifs de sécurité nationale doit être prescrite par la loi et proportionnée à la protection de la sécurité nationale.

22. La Cour européenne des droits de l'homme a énoncé les garanties à cet égard : « Dans sa jurisprudence relative aux mesures de surveillance secrète, la Cour énonce les garanties minimales suivantes contre les abus de pouvoir que la loi doit renfermer : la nature des infractions susceptibles de donner lieu à un mandat d'interception ; une définition des catégories de personnes susceptibles d'être mises sur écoute ; la fixation d'une limite à la durée de l'exécution de la mesure ; la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; les précautions à prendre pour la communication des données à d'autres parties ; et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements »[7].

23. Bien que nous ne disposions pas de toutes les informations concernant le programme PRISM, il semble qu'un grande nombre de données relatives aux communications électroniques aient été interceptées, conservées et analysées en collaboration avec les services de sécurité nationale de certains Etats en Europe. Des données à caractère personnel auraient été traitées et explorées dès l'instant où des mots clés ont été utilisés dans les communications électroniques ; ces mots faisaient partie d'une vaste liste de mots généralement utilisés par les terroristes ou les criminels. Au final, de nombreux utilisateurs ont dû être surveillés et leur profil établi. Dans ce contexte, il existe également des soupçons d'espionnage commercial.

24. Si la surveillance et le profilage ont été réalisés sans motifs suffisants de risques pour la sécurité nationale, on pourrait considérer qu'il y a eu violation de l'article 8 de la Convention européenne des droits de l'homme. La récente proposition de résolution sur les opérations massives de surveillance en Europe (doc. 13288 de l'Assemblée) pourrait déboucher sur une analyse et une discussion plus approfondies de ce cas particulier et de ses implications plus larges concernant la corrélation entre sécurité nationale et protection de la vie privée.

25. Edward Snowden a travaillé pour les sociétés de sécurité privées Booz Allen Hamilton et Dell, que l'Agence de sécurité nationale des Etats-Unis avait engagées. Cette externalisation de la surveillance de

[6] Voir http://www.europarl.europa.eu/comparl/tempcom/echelon/pdf/rapport_echelon_fr.pdf
[7] Voir, arrêt de la CEDH dans l'affaire Liberty et autres c. Royaume-Uni (requête n° 58243/00) citant la décision rendue dans l'affaire Weber et Saravia c. Allemagne (requête n° 54934/00), reproduit à l'adresse http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87207

l'internet à des fins de sécurité nationale peut sérieusement affaiblir la protection de la vie privée et des données à caractère personnel. Les propos d'Edward Snowden sont cités dans le Guardian : « Le gouvernement s'est octroyé des pouvoirs auxquels il n'a pas droit. Il n'y a pas de surveillance de la part du public. En conséquence, des gens comme moi peuvent aller plus loin qu'ils en ont le droit »[8]. Bien que l'enjeu soit différent, on pourrait également mentionner dans ce contexte la Recommandation 1858 (2009) sur les sociétés privées à vocation militaire ou sécuritaire et l'érosion du monopole étatique du recours à la force.

26. Edward Snowden a révélé au Guardian un nombre considérable d'informations secrètes concernant les activités des services de sécurité nationale aux Etats-Unis, au Royaume-Uni et dans d'autres pays de l'OTAN. Glenn Greenwald, journaliste au Guardian, a déclaré sous serment devant une commission des relations étrangères du Sénat brésilien qu'il avait reçu d'Edward Snowden jusqu'à 20 000 dossiers secrets de gouvernements[9]. La divulgation de ces dossiers a été décrite comme un « lancement d'alerte ». A la suite de ces événements, la présidente brésilienne a décidé de reporter sa visite officielle aux Etats-Unis tant que toute la lumière ne serait pas faite sur cette situation. Après un mois à Hong Kong, Chine, M. Snowden est maintenant en Russie depuis juin 2013.

27. Après les révélations de M. Snowden concernant la surveillance généralisée de la correspondance électronique en France ainsi que l'interception de la communication par téléphone mobile et SMS de la Chancelière fédérale d'Allemagne par le service de la sécurité nationale des Etats-Unis depuis de nombreuses années, les gouvernements de la France et de l'Allemagne sont en tête d'une initiative au sein du Conseil de l'Union européenne afin de clarifier la violation de la vie privée commises par les Etats-Unis et de développer des normes communes sur la surveillance et la coopération dans le domaine de la sécurité nationale. En outre, la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen a mis en place une enquête sur la surveillance électronique de masse de citoyens de l'UE, en tenant des audiences depuis le 5 septembre 2013, et a produit son rapport final le 21 février 2014.[10] L'Assemblée parlementaire du Conseil de l'Europe a donné, le 30 septembre 2013, la proposition sur les opérations massives de surveillance en Europe (Doc. 13288) à sa Commission des questions juridiques et des droits de l'homme pour rapport. Au niveau des Nations Unies, le Brésil et l'Allemagne ont, le 8 Novembre 2013, présenté à la Troisième Commission de l'Assemblée générale des Nations Unies un projet de résolution appelant à la protection de la vie privée conformément au droit international des droits de l'homme et à la cessation de la surveillance électronique excessive. Cette résolution sur le droit à la vie privée à l'ère numérique a été adoptée le 18 décembre 2013 par l'Assemblée générale des Nations Unies.

28. La résolution 1729 (2010) de l'Assemblée sur la protection des « donneurs d'alerte » précise au paragraphe 6.1.1 : « la définition des révélations protégées doit inclure tous les avertissements de bonne foi à l'encontre de divers types d'actes illicites, y compris toutes les violations graves des droits de l'homme, qui affectent ou menacent la vie, la santé, la liberté et tout autre intérêt légitime des individus en tant que sujets de l'administration publique ou contribuables, ou en tant qu'actionnaires, employés ou clients de sociétés privées ». Il est possible, en dernier recours, d'utiliser les médias pour donner l'alerte, comme indiqué au paragraphe 6.2.3 de la Résolution 1729 : « Lorsqu'il n'existe pas de voies internes pour donner l'alerte, ou qu'elles ne fonctionnent pas correctement, voire qu'il ne serait pas raisonnable de s'attendre à ce qu'elles fonctionnent correctement étant donné la nature du problème dénoncé par le donneur d'alerte, il conviendrait de la même manière de protéger celui qui utilise des voies externes, y compris les médias ».

29. En tout état de cause, les pouvoirs publics ne seraient pas autorisés, en vertu de l'article 8, à procéder à la surveillance et au profilage des utilisateurs pour des motifs strictement politiques, par exemple pour cibler des opposants politiques. Bien que la plupart des Etats dans le monde possèdent probablement les ressources technologiques et humaines pour le faire, et bien que l'on puisse supposer que tel serait le souhait des gouvernements non démocratiques et oppresseurs, aucun indice concret ne corrobore cette hypothèse en ce qui concerne l'affaire PRISM.

30. Dans l'affaire Klass et autres c. l'Allemagne (requête n° 5029/71), la Cour européenne des droits de l'homme a précisé, en évaluant l'article 8, « que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications est, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales. (…) Consciente du danger, inhérent à

[8] Voir, The Guardian (11 juin 2013), à l'adresse http://www.theguardian.com/world/2013/jun/10/obama-pressured-explain-nsa-surveillance
[9] Voir http://rt.com/news/journalist-thousands-snowden-documents-143/
[10] Voir http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bREPORT%2bA7-2014-0139%2b0%2bDOC%2bPDF%2bV0%2f%2fFR

pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée. Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif : elle dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne. »[11]

31. Pour conclure, il est nécessaire d'exercer une surveillance interne suffisante et efficace et un contrôle juridictionnel des services de sécurité nationale et des services de police, afin d'empêcher tout abus et ainsi toute violation de l'article 8 de la Convention européenne des droits de l'homme. Les éventuels dommages qui découleraient d'un accès et d'une utilisation irresponsables de ces données sont évidents.

32. Bien qu'à une échelle plus petite, les possibilités technologiques de surveillance et de profilage des utilisateurs sont, en principe, également mises à la disposition des sociétés commerciales et des particuliers, qui peuvent vouloir exploiter des données dans leur intérêt personnel. Les Etats doivent donc garantir aux utilisateurs une protection suffisante dans ce domaine également. La surveillance des employés par leurs employeurs est restreinte par la Recommandation n° R (89) 2 du Comité des Ministres sur la protection des données à caractère personnel utilisées à des fins d'emploi.

5. Les développements concernant les technologies de l'information

33. La sécurité est aujourd'hui un champ important de la recherche informatique. Son objectif est de mettre au point des méthodes sophistiquées visant à éviter les intrusions, les manipulations ou les destructions de bases de données, mais aussi à empêcher les pirates de prendre le contrôle des systèmes informatiques privés ou professionnels ou de menacer ceux des organismes publics (police, justice, défense, etc.) ou encore les infrastructures informatiques essentielles qui sont absolument nécessaires à la vie de tous les jours dans nos sociétés (systèmes bancaires et financiers, transports, énergie, etc.).

34. Ce dernier point a fait l'objet d'une coopération internationale, notamment via l'International Cyber Security Protection Alliance[12] et par la mise en place récente par l'Union européenne du Centre européen de lutte contre la cybercriminalité installé au siège d'Europol à La Haye[13].

35. Pourtant, en dépit des efforts déployés depuis des dizaines d'années, les organisations peinent toujours à protéger leurs systèmes informatiques contre les actes de malveillance, comme le montrent les nombreuses effractions que ceux-ci subissent et dont les médias se font l'écho. De plus, les appareils connectés et les services électroniques proposés aux utilisateurs individuels montent en puissance et sont aujourd'hui aussi la cible des pirates, qui en tirent un bénéfice important. La sécurité informatique semble ici encore moins assurée, comme en témoignent régulièrement dans les médias les récits d'attaques par virus.

36. Les ordinateurs sont accessibles à distance et les données et logiciels peuvent être rapidement échangés. Ces possibilités ont conduit à développer des moyens technologiques pour faire face aux nouveaux défis que pose la sécurité informatique : pare-feux, logiciels antivirus, outils de cryptage, etc. Cela étant, la complexité croissante des systèmes, conjuguée aux actions (ou inactions) quotidiennes des utilisateurs, révèle des vulnérabilités que des esprits malintentionnés peuvent exploiter.

37. Comme les moyens exclusivement technologiques ne sauraient suffire, on s'intéresse désormais davantage aux facteurs organisationnels qu'aux solutions technologiques. Même sécurisés d'un point de vue technologique, les appareils et les logiciels restent vulnérables si des politiques et des procédures de sécurité efficaces n'ont pas été définies ou si elles sont insuffisamment appliquées et encouragées. Des cadres d'orientation et des certifications ont été conçus pour permettre aux organisations de procéder à l'évaluation systématique de leurs besoins en matière de sécurité informatique et de mettre en œuvre les produits, politiques et procédures nécessaires. La *sécurité organisationnelle* a ainsi été reconnue comme un élément important de la sécurité informatique.

38. Les problèmes de sécurité informatique ont persisté malgré la mise en place de mesures de sécurité technologiques et organisationnelles. Les utilisateurs sont souvent dépassés par les procédures de sécurité ou non conscients des conséquences de leurs actions en matière de sécurité. En outre, le besoin croissant

[11] Voir http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510
[12] Voir https://www.icspa.org/
[13] Voir https://www.europol.europa.eu/ec3

des utilisateurs de protéger leur environnement informatique privé a conduit à examiner en détail le rôle que joue l'utilisateur final en matière de sécurité informatique.

39. Par conséquent, la recherche s'est récemment recentrée sur la *sécurité informatique personnelle* en tant qu'autre élément fondamental de la sécurité informatique. Le concept de « sécurité et [protection de la vie privée] utilisable[s] » suscite aujourd'hui un débat passionné dans le milieu de la recherche sur la sécurité des technologies de l'information. Ce phénomène pourrait s'expliquer par l'inadaptation du *modèle mental* élaboré pour évaluer les risques courus par l'utilisateur et les actions qu'il entreprend. Aussi, une meilleure compréhension du rôle des modèles mentaux et l'élaboration de modèles plus adaptés pourraient renforcer la sécurité informatique des utilisateurs. La technologie doit donc prendre une forme « utilisable », qui aide l'utilisateur tout en contribuant à la sécurité informatique. Il reste à voir de quelle manière les résultats de la recherche peuvent être transposés dans les outils, logiciels et services de demain, et à définir les actions de formation et d'aide en direction des utilisateurs privés.

6. Situation actuelle de la sécurité des technologies de l'information

40. Avec la croissance rapide des services internet dans tous les domaines de la vie, le taux de criminalité a également augmenté de façon exponentielle. Le rapport de 2012 de Norton Symantec sur la cybercriminalité estime qu'il y a 1,5 millions de victimes de la cybercriminalité par jour avec des montants annuels estimés à 110 milliards de dollars américains dans le monde et 16 milliards de dollars américains en Europe[14]. Parallèlement à la croissance de l'accès mobile à internet, le nombre d'attaques de cybercriminalité a doublé de 2010 à 2011.

41. Plusieurs affaires ont défrayé la chronique : on peut notamment citer le piratage massif de données d'utilisateurs, par exemple par un groupe dénommé Lulz Security, dans les serveurs de Sony et de Nintendo en 2011, la cyberattaque du répertoire téléphonique Truecaller par un groupe dénommé Syrian Electronic Army en juillet 2013 ainsi que le vol de 2 millions de données d'utilisateurs archivées sur un serveur Vodafone en Allemagne en septembre 2013. En mars 2011, la société de sécurité internet McAfee a fait savoir que des pirates informatiques en Chine se livraient depuis 2009 à un vaste espionnage commercial de plusieurs multinationales pétrolières, appelé « opération dragon de nuit ».

42. Une autre affaire spectaculaire a été l'utilisation de données de cartes de crédit volées pour retirer 45 millions de dollars à des distributeurs automatiques dans la ville de New York et dans d'autres villes du monde en décembre 2012 et février 2013. En mai 2013, le service de transfert de fonds en ligne Liberty Reserve a été fermé par les services de police aux Etats-Unis et dans 16 autres pays car il était soupçonné d'avoir mis au point un vaste système de blanchiment d'argent via internet, pour un montant de 6 milliards de dollars. Alors que ces affaires retentissantes laissent présager qu'il existe des risques de sécurité sur internet, les attaques moins importantes mais plus fréquentes dirigées contre les internautes individuels sont plus préjudiciables en valeur absolue et nous devrions en tenir compte dans notre analyse.

43. Nous nous appuyons ici sur le site « *Verbraucher sicher online* »[15], portail allemand d'information en ligne axé sur l'utilisateur et dédié à la sécurité informatique et à la protection des données personnelles – portail dont nous avons une connaissance pratique –, pour esquisser les grandes lignes de la sécurité vis-à-vis des technologies de l'information des points de vue du pirate et de l'utilisateur. Le pirate est à la recherche des vulnérabilités d'un système, qu'il ou elle va exploiter pour tenter d'y accéder. L'utilisateur doit prendre des mesures appropriées pour combler ces failles et réduire au minimum les risques de piratage.

44. L'environnement informatique d'un utilisateur peut être décrit en quatre composantes, avec chacune ses vulnérabilités et les parades pour y remédier : une attaque peut être dirigée contre n'importe quel *appareil* de l'utilisateur (ordinateur, téléphone intelligent, etc.) ou contre les *réseaux informatiques* auxquels se connectent les appareils (internet et réseaux mobiles), dans le but d'interagir avec les *services électroniques* dont se sert l'utilisateur. Enfin, *l'utilisateur* lui-même peut être la cible d'une attaque.

6.1. Attaques contre les appareils de communication

45. Parmi les appareils de communication, citons les ordinateurs de bureau, les ordinateurs portables et les téléphones intelligents, dont l'utilisateur se sert sans intermédiaire. Ils se composent du matériel, du

[14] Voir http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[15] Voir http://www.verbraucher-sicher-online.de/

système d'exploitation et des logiciels applicatifs, et sont généralement connectés à des réseaux locaux ou mobiles et, via ces réseaux, à l'internet.

46. Les attaques dirigées contre un appareil exploitent une ou plusieurs *vulnérabilités* techniques, par exemple des failles du système d'exploitation ou des applications, que l'on désigne sous le nom d'*exploits*, pour installer un programme malveillant ou « infecter » l'appareil avec ce type de programme. Après l'infection, le logiciel malveillant prend régulièrement le contrôle total de l'appareil. Toutes les données deviennent accessibles, toutes les actions de l'utilisateur sont interceptées (par exemple, la saisie des mots de passe), et l'appareil est utilisé pour infecter ou attaquer d'autres appareils et services électroniques.

47. Les *parades technologiques* contre ce type d'attaques sont les suivantes : (1) sauvegardes périodiques des données de l'appareil, (2) logiciel efficace et actualisé de protection contre les logiciels malveillants, et (3) mise à jour permanente des applications et du système d'exploitation afin de corriger les failles connues du logiciel.

48. En l'absence d'une organisation centrale pour la protection des appareils, les politiques ou procédures de sécurité reposent nécessairement sur des *parades individuelles*, autrement dit sur les connaissances de l'utilisateur et sa prise de conscience des dangers qu'il court. A cet égard, la *facilité d'utilisation* des fonctions de sécurité s'est améliorée ces dernières années. Avec la médiatisation des questions de sécurité informatique, les fabricants d'appareils et les concepteurs de logiciels ont redoublé d'efforts pour intégrer la sécurité dans leurs produits et proposent désormais des mises à jour de sécurité en temps utile. En outre, de plus en plus de logiciels peuvent être configurés pour que les mises à jour de sécurité s'effectuent de façon automatique, déchargeant ainsi l'utilisateur de cette tâche. L'utilisateur doit toutefois se tenir informé des nouveautés en matière de sécurité, faire des sauvegardes et installer un logiciel antivirus. De plus, il ne doit jamais relâcher sa vigilance et être en mesure de repérer et de prévenir les attaques par messagerie électronique, sites web, etc., qui risquent d'infecter son appareil.

6.2. Attaques contre les réseaux

49. Les appareils se connectent à divers réseaux pour accéder aux services électroniques proposés sur l'internet. Ces connexions se font de plus en plus fréquemment par voie hertzienne. En règle générale, les points d'entrée des réseaux sont soit des routeurs domestiques, soit des points d'accès (*hotspots*) publics ou privés.

50. Les attaques les plus courantes contre les routeurs domestiques consistent à s'y introduire et à intercepter les connexions qu'ils acheminent, ou encore à utiliser la connexion pour lancer de nouvelles attaques contre des appareils locaux ou distants. Les principales *solutions technologiques* applicables aux routeurs consistent à mettre en place un cryptage renforcé des connexions sans fil (actuellement, WPA2) grâce à un mot de passe efficace, à protéger l'interface administrative à l'aide d'un (autre) mot de passe efficace et à effectuer des mises à jour régulières du micrologiciel du routeur. L'une des récentes *solutions en matière de facilité d'utilisation* apportées par les fabricants de routeurs est l'activation par défaut du cryptage de la connexion sans fil, qui a conduit à une réduction sensible du nombre de réseaux domestiques sans fil non sécurisés.

51. Les attaques via des points d'accès publics ou privés prennent généralement l'une des deux formes suivantes : soit le pirate prend le contrôle du routeur du point d'accès, soit il installe un autre point d'accès qui simule le point d'accès officiel. Dans les deux cas, les connexions acheminées par le routeur peuvent être interceptées. Les points d'accès sont des cibles privilégiées des pirates, car de nombreux utilisateurs, attirés par les points d'accès gratuits, en sous-estiment les dangers. S'il existe des *solutions techniques* susceptibles d'atténuer les risques liés à ce type d'accès (recours à des réseaux privés virtuels [VPN, *virtual private networks*] par exemple), elles sont peu pratiques et les points d'accès en bloquent parfois l'utilisation.

52. La *parade personnelle* logique consisterait donc à trouver un autre moyen, plus sûr, de se connecter à l'internet. A moyen terme, la généralisation de l'accès mobile à l'internet à haut débit pourrait réduire les problèmes liés aux points d'accès.

6.3. Attaques contre les services électroniques

53. Accéder sans autorisation aux services électroniques des utilisateurs est sans nul doute l'un des objectifs premiers des pirates. L'accès à la plupart de ces services repose encore uniquement sur de simples identifiants (nom d'utilisateur, mot de passe, etc.), même si certaines organisations, notamment les banques, ont mis au point des systèmes plus complexes reposant sur des mots de passe à usage unique (numéros d'authentification des transactions – *transaction authentication numbers*, TAN) et une

authentification multi-facteurs (identifiants supplémentaires par divers moyens techniques, notamment le téléphone portable ou les générateurs de TAN).

54. Un autre risque fréquemment négligé concerne la disponibilité des données d'utilisateur mises en mémoire par les fournisseurs de services électroniques. Il arrive par exemple que les fournisseurs n'assurent pas la confidentialité ou l'intégrité des données ou qu'ils n'en protègent pas suffisamment l'accès, ce qui ouvre la porte aux attaques directes contre le service électronique, susceptibles d'entraîner la perte des données des utilisateurs. La *parade technique* appropriée consiste à sauvegarder (archiver) les données dans plusieurs endroits.

6.4. Attaques contre les utilisateurs

55. Du point de vue d'un pirate, l'utilisateur peut être la cible d'une attaque, au même titre qu'un appareil, un réseau ou un service électronique. Les attaques de ce type, souvent regroupées sous l'expression « ingénierie sociale », peuvent être définies comme toute « attaque ayant recours à des méthodes à caractère social, telles la tromperie et la manipulation, pour accéder aux technologies de l'information. » L'hameçonnage, qui consiste à envoyer des messages électroniques pour inciter le destinataire à ouvrir une pièce jointe contenant un logiciel malveillant, à répondre à une escroquerie ou à saisir ses identifiants sur un faux site web de services électroniques, relève de cette catégorie. Par exemple, un faux courriel invite à transmettre l'identifiant et le mot de passe « pour des raisons de sécurité ».

56. Les mesures de sécurité les plus efficaces sont de nature *non technique* : vigilance et prudence. A contrario, les parades techniques (détection automatique des courriels d'hameçonnage par exemple) se sont montrées largement inefficaces contre les innombrables variantes de ces attaques.

57. Les risques peuvent aussi venir de contenus produits volontairement par les internautes et accessibles à tous en ligne. Ces contenus peuvent être explorés et rassemblés au moyen de logiciels spéciaux d'extraction de données. Un exemple récent est fourni par la technologie RIOT (*Rapid Information Overlay Technology*) de la société américaine Raytheon, à laquelle les pouvoirs publics eux-mêmes ont recours pour explorer les réseaux sociaux et dresser des profils d'utilisateurs[16].

7. Risques à venir : communications mobiles, informatique dématérialisée et internet des objets

58. Les téléphones portables, et particulièrement les téléphones intelligents, sont des ordinateurs au même titre que les ordinateurs portables ou de bureau. Partageant les mêmes vulnérabilités, ils sont exposés aux mêmes risques et menaces (attaques de logiciels malveillants par exemple). Cela étant, certaines caractéristiques des téléphones intelligents aggravent les difficultés qui sont inhérentes à la sécurité informatique en mode mobile.

59. Parmi ces caractéristiques, citons notamment :

- leur taille, qu'il s'agisse de leur taille physique (il est facile de les perdre ou de les voler) ou de leurs capacités de calcul limitées (par rapport aux ordinateurs portables ou de bureau) ;
- la multitude des technologies de réseau (mobile, WiFi, Bluetooth) et d'autres paramètres techniques internes (GPS, paiement électronique par communication en champ proche) ;
- d'où la complexité du système d'exploitation mobile, avec un risque accru de vulnérabilité ; et le grand nombre d'applications (ou « apps ») et d'usages.

60. L'informatique dématérialisée (*« cloud computing »*) s'adresse en règle générale aux entreprises, qui sont susceptibles de retirer des profits économiques de l'externalisation de diverses ressources informatiques – logiciels, archivage, temps d'exécution, etc. – vers des fournisseurs de ce type de services. Parallèlement, les offres de Google ou l'iCloud d'Apple par exemple peuvent être vus comme le « versant consommateur » de l'informatique dématérialisée.

61. Ces offres intègrent dans une écosphère « dématérialisée » et centralisée unique plusieurs services qui existent par ailleurs indépendamment (messagerie électronique, partage de photos et de vidéos, réseautage social, archivage à distance, etc.). Une autre caractéristique est l'intégration étroite de logiciels (navigateurs web, systèmes d'exploitation) ou d'appareils (téléphones intelligents) dans cette écosphère.

[16] Voir la critique formulée par l'Union américaine pour les libertés civiles (ACLU), disponible à l'adresse : http://www.aclu.org/blog/technology-and-liberty-national-security/raytheons-riot-social-network-data-mining-software

62. Les incidences sur la sécurité informatique ne sont pas aussi manifestes. D'un côté, certains affirment que les données personnelles sont mieux protégées dans le *cloud* parce qu'elles sont stockées indépendamment des appareils. Des fonctions de sécurité spécifiques comme la suppression à distance des données en cas de perte d'un appareil ou l'authentification centralisée, qui épargne à l'utilisateur la mémorisation de tous ses mots de passe (en supposant que cette authentification soit sûre), peuvent ainsi être vues comme des avantages de l'informatique dématérialisée en matière de sécurité.

63. D'un autre côté, certaines données empiriques laissent entrevoir d'éventuels problèmes. Par exemple, une attaque réussie contre le système d'authentification centralisée donne accès à l'ensemble des données et services des utilisateurs. Lors de l'attaque menée en été 2012 contre le service iCloud d'Apple, les pirates ont réussi à accéder à l'iCloud d'un journaliste et à effacer l'ensemble des données stockées sur tous ses appareils connectés, y compris son téléphone et son ordinateur portable. Cette fonctionnalité, présentée au départ comme un service de sécurité contre le vol, est finalement apparue comme une grave menace pour la sécurité.

64. L'intégration progressive de nouveaux mécanismes de sécurité dans les services dématérialisés pourrait atténuer les risques informatiques inhérents à ce type de services centralisés. Quoi qu'il en soit, l'utilisateur doit évaluer avec le plus grand soin les risques que présentent ces services.

65. Au vu des difficultés que pose actuellement la sécurité informatique et des problèmes que poseront probablement certaines technologies déjà disponibles (accès mobile à l'internet et informatique dématérialisée notamment), il semble impossible de prévoir quelle forme prendront les menaces dues à des technologies aussi potentiellement perturbatrices que « l'internet des objets ». Les objets physiques du quotidien, des appareils électroménagers aux voitures dotés de capacités réseau, sont des points d'attaques additionnels. Comme ces objets avec internet sont généralement des biens commerciaux qui requièrent des services commerciaux et permettent le profilage d'un utilisateur (p.ex. des impulsions automatisées pour l'entretien de la voiture, la réparation du chauffage ou le remplacement de la cartouche dans l'imprimante), l'intérêt économique d'une attaque est évidemment augmenté.

66. L'« informatique ambiante » ou « omniprésente » peut aller plus loin dans la vie des utilisateurs, où informatique et réseaux s'intègrent étroitement aux objets et aux activités, voire au corps humain, et « disparaissent » en tant que technologies distinctes.

8. Des mesures pour renforcer la protection et la sécurité des utilisateurs

67. Depuis près d'un siècle, les principes de protection des consommateurs ont été mis en place pour le commerce traditionnel de biens et services. Cependant, ils sont plus ou moins absents dans le cyberespace moderne. Des principes de protection des utilisateurs ont été développés dans certains domaines par l'OCDE et la CNUDCI. Quelques principes juridiques ont été mis en place par les Nations Unies, le Conseil de l'Europe et, en particulier, l'Union européenne.

68. La coopération entre les services de police doit être renforcée, notamment en étendant l'application de la Convention de Budapest sur la cybercriminalité (STE n° 185) ainsi que des traités internationaux sur l'assistance juridique comme la Convention européenne sur l'entraide judiciaire en matière pénale (STE n° 30).

69. Tant les fournisseurs de services internet que les utilisateurs ont une connaissance relativement faible de ces normes et principes. En outre, leur force juridique est plutôt limitée, à l'exception de la législation de l'UE en vigueur dans tous ses Etats membres. Par conséquent, il semble nécessaire de mieux faire connaître les normes juridiques déjà établies et d'en développer d'autres si besoin est.

70. Les utilisateurs achètent des ordinateurs ou d'autres appareils et souscrivent à des services internet. Il s'agit typiquement de transactions commerciales entre un utilisateur et une société commerciale. Sur cette base, les utilisateurs peuvent légitimement s'attendre à ce que les biens et services qu'ils reçoivent soient sans défaut et sans danger potentiel. Une telle attente légitime peut entraîner l'obligation pour les sociétés de vendre leurs biens et services avec des précautions visant la sécurité de leurs utilisateurs.

71. Par exemple, les fournisseurs de services peuvent être tenus de fournir des outils de cryptage automatiquement (c'est-à-dire comme une option par défaut) et gratuitement. Cela permettra d'accroître la sécurité des usagers en ce qui concerne les mots de passe ou d'autres données sensibles. Les ordinateurs modernes ou d'autres dispositifs devraient avoir des programmes anti-virus avancés mis en place automatiquement. En outre, les sites Web devraient indiquer de manière transparente s'ils appliquent des signes automatiques ou des cookies aux dispositifs d'accès des utilisateurs.

72. Les entreprises peuvent satisfaire à ces normes volontairement, mais les Etats peuvent utilement les encourager ou même les prescrire si nécessaire. Dans un monde globalisé, il est important de coordonner les approches entre les Etats, en particulier en Europe.

73. Le Conseil de l'Europe est la première et jusqu'à présent l'unique organisation internationale à lutter contre la cybercriminalité par le biais d'une convention internationale. La Convention de Budapest sur la cybercriminalité a également été signée par de nombreux Etats en dehors de l'Europe et elle est un modèle pour plus de 100 pays à travers le monde. Lors de la récente Conférence du Conseil de l'Europe sur les stratégies prioritaires en matière de coopération contre la cybercriminalité (Dubrovnik, 15 février 2013), les ministres participants ont adopté les objectifs suivants:

- poursuivre des stratégies contre la cybercriminalité pour assurer une réponse efficace de la justice pénale aux infractions contre et au moyen d'ordinateurs ainsi qu'à toute infraction impliquant une preuve électronique ;
- adopter une législation complète et efficace sur la cybercriminalité conforme aux droits de l'homme et à la primauté du droit ;
- renforcer les unités de police spécialisées et la spécialisation des services du parquet concernant la cybercriminalité et la preuve électronique ;
- mettre en œuvre des stratégies durables de formation sur l'application des lois ;
- soutenir la formation des juges et des procureurs en matière de cybercriminalité et de preuve électronique ;
- poursuivre des stratégies globales visant à protéger les enfants contre l'exploitation sexuelle et les abus sexuels en ligne en accord avec la Convention de Lanzarote ;
- promouvoir les enquêtes financières et la prévention et la lutte contre la fraude et le blanchiment d'argent sur internet ;
- renforcer la coopération avec le secteur privé, en particulier entre les services de police et les fournisseurs de services internet ;
- s'engager dans une coopération régionale et internationale efficace ;
- partager leur expérience avec d'autres régions du monde pour soutenir le renforcement des capacités de lutte contre la cybercriminalité ;
- promouvoir l'adhésion à la Convention de Budapest sur la cybercriminalité au niveau mondial.

9. Exemples d'autorégulation par les acteurs du marché

74. En 2011, l'Alliance européenne pour l'éthique en publicité (EASA) a publié son Code de bonnes pratiques en matière de publicité comportementale en ligne, qui vise à garantir la protection de la vie privée dans toute l'Europe[17]. L'idée fondamentale est de permettre aux utilisateurs d'identifier la publicité comportementale en ligne au moyen d'une même icône de référence européenne. L'icône sera insérée dans ou à côté de toutes les bannières de publicité comportementale en ligne afin d'avertir l'internaute de l'usage de ce procédé. Cette icône sera interactive et permettra aux utilisateurs de découvrir les sociétés impliquées et de cliquer pour être redirigés vers un portail paneuropéen. Ce dernier fournira des informations générales sur la publicité comportementale en ligne et sur les moyens dont disposent les utilisateurs (déclinés dans leur langue nationale) d'exercer leur choix, en l'occurrence d'indiquer s'ils souhaitent ou non recevoir de la publicité comportementale en ligne.

75. Cela étant, ce système n'est pas très efficace, notamment pour les usagers inexpérimentés. Plusieurs dizaines de sociétés se sont à ce jour engagées par écrit, mais tous les prestataires de ce type de publicité ne l'ont pas fait, tant s'en faut. L'utilisateur est obligé de visiter les nombreux sites des sociétés concernées et de refuser les témoins de connexion employés par ces prestataires. Il doit répéter cette procédure sur tous ses ordinateurs y compris sur les téléphones portables. Par ailleurs, il n'existe pas de réglementation relative aux « cookies Flash », témoins de connexion les plus tenaces qui ne sont pas intégrés dans le navigateur, mais installés au plus profond du système informatique, et qui sont de ce fait très difficiles à supprimer.

76. Les Principes de l'Union européenne pour des réseaux sociaux plus sûrs (2009) ont été élaborés par plusieurs prestataires de services de socialisation en concertation avec la Commission européenne, dans le cadre de son programme « Safer Internet Plus » (« Pour un internet plus sûr »), et plusieurs ONG. Ils visent à fournir des recommandations de bonnes pratiques à l'intention des fournisseurs de réseaux sociaux et d'autres sites interactifs, afin de renforcer la sécurité des enfants et des jeunes utilisateurs de leurs services. Les sept principes fondamentaux sont les suivants :

[17] Disponible à l'adresse : http://www.easa-alliance.org/page.aspx/386.

- Principe 1 : Attirer l'attention des utilisateurs, parents, enseignants et éducateurs sur les messages d'éducation à la sécurité et les politiques en matière d'usage acceptable, de façon bien visible et dans un langage clair et adapté à l'âge
- Principe 2 : Veiller à ce que les services soient adaptés à l'âge du public visé
- Principe 3 : Donner à l'utilisateur des moyens d'agir, sous la forme d'outils et de technologies
- Principe 4 : Fournir des mécanismes simples d'utilisation pour signaler des comportements ou des contenus qui enfreignent les conditions d'utilisation
- Principe 5 : Répondre aux notifications concernant des contenus ou des comportements illicites
- Principe 6 : Permettre aux utilisateurs d'appliquer une gestion sans risque des données à caractère personnel et de leur vie privée et les y encourager
- Principe 7 : Evaluer les moyens pour passer en revue les contenus ou comportements illicites ou interdits.

77. Le document contient des recommandations spécifiques plus concrètes relatives à chaque principe. Il précise toutefois que si les fournisseurs soutiennent l'ensemble des sept principes, il appartient à chacun de juger où et dans quelle mesure appliquer les recommandations spécifiques.

78. Le Cadre européen pour une utilisation plus sûre des téléphones mobiles par les adolescents et les enfants (2007) a été signé par de nombreux opérateurs européens de téléphonie mobile et fournisseurs de contenu afin de garantir une utilisation plus sûre des téléphones mobiles par les adolescents et les enfants. Il énonce diverses recommandations à cet effet, en particulier sur l'accès aux mécanismes de contrôle, la sensibilisation et l'éducation, la classification des contenus commerciaux ainsi que sur les contenus illicites diffusés par téléphonie mobile ou sur internet. Les rapports réguliers de mise en œuvre publiés par l'industrie témoignent des progrès réalisés par les opérateurs de téléphonie mobile pour préserver la sécurité des enfants lorsqu'ils utilisent leurs téléphones portables.

79. Les fournisseurs de services internet et les fabricants de dispositifs d'accès à internet devraient être encouragés et soutenus dans la mise en place de mesures de précaution pour la protection et la sécurité des utilisateurs et des clients ; ils pourraient éventuellement y être contraints. Le secteur pourrait notamment librement adopter et appliquer ses propres dispositions ou une co-réglementation reposant sur un cadre juridique. La certification de qualité peut jouer un rôle important à cet égard, notamment pour les outils offrant une protection contre des attaques dirigées contre des appareils, des réseaux et des services. L'ISO (Organisation internationale de normalisation) à Genève a établi un certain nombre de normes techniques internationales, tels que des critères communs ISO/CEI 15408:1999 pour l'évaluation de la sécurité des TI. Pour assurer une protection efficace et transparente des utilisateurs dans un cyber environnement qui change rapidement, des normes techniques spécifiques supplémentaires doivent être développés, par exemple sur la sécurité des logiciels et du matériel. Le respect de ces derniers normes ISO pourrait servir comme étiquette de qualité, qui peut être reconnu et digne de confiance par les utilisateurs.

10. Conclusions

80. Pour améliorer la sécurité dans le cyberespace, il faut davantage d'information, de transparence et de responsabilisation. Toutes les parties prenantes doivent relever ce défi, que ce soit le secteur de l'internet, les utilisateurs ou l'Etat.

81. Des solutions technologiques satisfaisantes existent pour lutter contre certains problèmes de sécurité informatique ; certaines ont déjà évolué vers une plus grande facilité d'utilisation. Mais la capacité des utilisateurs à traduire leurs connaissances en actions efficaces dépend de la pertinence des modèles mentaux applicables à la sécurité informatique, qu'il reste à développer. A cet égard, l'apprentissage en ligne pourrait être un outil systémique utile. Il faut créer des structures institutionnelles fiables (par les gouvernements ou le secteur privé) qui aident les utilisateurs à bien évaluer les risques et leur offrent une assistance concrète, à l'image des politiques et procédures de sécurité et du personnel de soutien mis en place dans les organisations.

82. L'anonymat complique la mise en œuvre de la responsabilité directe des utilisateurs. En outre, l'analyse ou le contrôle à grande échelle du comportement des internautes n'est pas acceptable du point de vue des droits de l'homme. Or tout fournisseur d'accès à l'internet connaît généralement l'identité de ses abonnés grâce à leur adresse IP ou à leurs identifiants. Les usagers qui respectent la législation devraient rester anonymes, alors que ceux qui l'enfreignent devraient être identifiables. Les opérateurs des sites commerciaux qui offrent une plate-forme aux internautes désireux d'enfreindre la législation devraient être tenus responsables, à moins qu'ils ne divulguent l'identité des contrevenants.

83. Les services de sécurité nationale et les services de police peuvent rechercher et saisir des données privées en ligne dans les limites de leurs compétences conformément au droit national et à l'article 8 de la Convention européenne des droits de l'homme. Cette ingérence doit être proportionnée aux buts légitimes poursuivis, qui sont énoncés à l'article 8, paragraphe 2, parmi lesquels figure la sécurité nationale. Ainsi qu'il ressort de la jurisprudence constante de la Cour européenne des droits de l'homme, cependant, il ne suffit pas que ces ingérences soient seulement opportunes ou souhaitables. Des interceptions permanentes et aléatoires des communications privées seraient contraires au principe de proportionnalité et donc incompatibles avec la Convention européenne des droits de l'homme.

84. Pour responsabiliser les utilisateurs, il faut davantage de transparence de la part des fournisseurs de services en ligne et des intermédiaires. Le manque de transparence nuit à la protection et à la sécurité des utilisateurs. S'il est possible d'imposer aux fournisseurs de services commerciaux et aux intermédiaires une obligation de transparence, cela peut être plus difficile en ce qui concerne les réseaux sociaux privés, les services de type « *peer-to-peer* » (entre homologues) et les contenus générés par l'utilisateur. Toujours est-il que des principes généraux de transparence doivent être définis.

85. La Convention sur la cybercriminalité protège l'intégrité des réseaux informatiques. Il pourrait être nécessaire d'analyser la portée de cette protection, et éventuellement de l'élargir aux attaques menées contre l'intégrité des systèmes au moyen de logiciels malveillants (moyens techniques), mais aussi au refus délibéré de mettre à disposition les composants essentiels nécessaires au bon fonctionnement des réseaux d'ordinateurs du domaine public. Par exemple, certaines attaques techniques peuvent provenir de messages non sollicités, de pourriels, de cookies, de logiciels malveillants tels que l'établissement de liens externes entre ordinateurs au moyen des « *botnets* », ainsi que de « *flash cookies* » qui sont enfouis plus profondément dans les systèmes informatiques et sont très difficiles à supprimer.

86. Les points d'accès publics et les zones d'accès sans fil à l'internet constituent en général des failles de sécurité, car ils peuvent servir de points d'entrée aux logiciels malveillants, au piratage, à la manipulation de données et autres types d'attaques contre la sécurité des usagers. L'accès mobile à l'internet est éventuellement plus sûr du fait que l'utilisateur n'a qu'un seul intermédiaire contractuel (opérateur ou fournisseur de services).

87. Le cryptage peut renforcer la confidentialité des communications dans le cyberespace, en particulier sur les liaisons sans fil. Les intrusions de type technique dans les systèmes de communication évoluent sans cesse à un rythme soutenu et il est donc nécessaire d'actualiser et de renforcer régulièrement les logiciels de cryptage. Pour aider les utilisateurs moins expérimentés, le cryptage sera activé par défaut.

88. Les contenus payants doivent être rendus transparents et donc faire l'objet d'un tri. Il conviendrait d'interdire aux prestataires de services payants et aux intermédiaires de recourir à des pratiques commerciales frauduleuses et trompeuses. A cet égard, il pourrait être intéressant de s'entendre sur une liste de pratiques commerciales interdites et sur un cadre de référence paneuropéen de normes de qualité. Cette idée pourrait aussi s'appliquer aux pratiques loyales en matière de marketing et de publicité des entreprises. Une législation sectorielle permet de traiter les questions pointues de protection et de sécurité des utilisateurs de façon plus ciblée, par exemple en visant spécifiquement les télécommunications, le système bancaire, le secteur de l'assurance, les instruments financiers, les paiements électroniques et les contrats de transport. L'utilisation et la fiabilité technique des signatures électroniques pourraient présenter un intérêt à cet égard.

89. Du fait de la portée internationale des services en ligne, les droits des utilisateurs peuvent être mis en danger par les incertitudes liées à la compétence des tribunaux nationaux et à l'applicabilité des législations nationales. Les Etats devraient donc œuvrer à des mécanismes de résolution et de réparation des litiges en ligne, et mettre en place une coopération et une assistance juridiques reposant sur le droit public international.

90. Les enfants constituent un groupe à haut risque. Le danger peut provenir de contenus en ligne illégaux ou à caractère violent et de contacts avec d'autres internautes. En outre, les enfants peuvent se faire du tort à eux-mêmes ou mutuellement en mettant en ligne des images ou des données à caractère privé ou en se rendant coupables de harcèlement. Etant donné qu'il est difficile de supprimer les données et les images à caractère privé stockées sur l'internet, il se peut que la victimisation ne prenne jamais fin. Par ailleurs, l'internet est une porte d'entrée à divers dangers venus de l'extérieur, qui guettent les enfants jusque dans leur chambre. La menace peut aussi venir des adultes : abus sexuels notamment. Il importe donc de mettre en place des mécanismes d'aide en ligne pour les parents et les enfants, et de soutenir l'éducation aux médias, la formation des enseignants et l'éducation par les pairs.