



MCM(2013)008

## **Liberté sur internet et droit à la vie privée, protection des données à caractère personnel et respect des formes légales**

**Rapport présenté par Access (AccessNow.org) :  
Raegan MacDonald, Jochai Ben-Avie et Fabiola Carrion**

Site internet : <https://www.accessnow.org/>

E-mail: [raegan@accessnow.org](mailto:raegan@accessnow.org)

Les avis exprimés dans ce texte relèvent de la responsabilité de l'auteur  
et ne reflètent pas nécessairement la politique officielle du Conseil de l'Europe



# Table des matières

|                                                                                                                                                                                                  |           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Résumé .....</b>                                                                                                                                                                              | <b>5</b>  |
| <b>Introduction .....</b>                                                                                                                                                                        | <b>8</b>  |
| <b>Première partie : Défis.....</b>                                                                                                                                                              | <b>10</b> |
| 1.1 Les progrès technologiques rendent possible une surveillance à une échelle inimaginable jusqu'à-là.....                                                                                      | 10        |
| 1.2 La surveillance basée sur le contournement des formes légales .....                                                                                                                          | 11        |
| 1.3 L'absence d'éclaircissements sur le droit à la protection de la vie privée entrave sa protection .....                                                                                       | 12        |
| 1.4 Opacité autour de la collecte de données.....                                                                                                                                                | 14        |
| 1.5 Atteintes des entreprises aux droits de l'homme .....                                                                                                                                        | 16        |
| 1.6 Non-cryptage du trafic internet et pressions croissantes sur les entreprises privées afin qu'elles introduisent des vulnérabilités en matière de sécurité dans les produits et services..... | 18        |
| 1.7 La justification de la législation sur la surveillance s'est renforcée au détriment de la nécessité, proportionnalité et finalité légitime .....                                             | 20        |
| 1.8 Nécessité d'une protection renforcée des sources et des donneurs d'alerte .....                                                                                                              | 22        |
| <b>Deuxième partie : Recommandations.....</b>                                                                                                                                                    | <b>23</b> |
| 2.1 Saisir l'occasion de faire de la Convention n° 108 une norme internationale relative à la protection de la vie privée .....                                                                  | 23        |
| 2.1.1 Renforcer le contrôle et la mise en œuvre de la Convention actualisée .....                                                                                                                | 23        |
| 2.1.2 Comblent autant que possible les lacunes subsistant dans la Convention.....                                                                                                                | 24        |
| 2.2 Renforcement du rôle des autorités de protection des données.....                                                                                                                            | 24        |
| 2.3 Adoption et mise en œuvre des principes internationaux sur l'application des droits de l'homme à la surveillance des communications.....                                                     | 24        |
| 2.4 Instauration d'une plus grande transparence .....                                                                                                                                            | 25        |
| 2.5 Rétablir la confiance dans le secteur des entreprises.....                                                                                                                                   | 26        |
| 2.6 Promouvoir la culture numérique.....                                                                                                                                                         | 26        |
| 2.7 Renforcer les mesures de protection pour les donneurs d'alerte.....                                                                                                                          | 27        |
| <b>Conclusion.....</b>                                                                                                                                                                           | <b>28</b> |



## Résumé

La liberté sur internet peut et doit aujourd'hui englober un éventail plus large de droits de l'homme au-delà de la liberté d'expression. Ceux-ci comprennent, sans toutefois s'y limiter, le droit à la vie privée (article 8), la liberté d'expression, qui inclut la liberté des médias (article 10), la liberté de réunion et d'association (article 11), la liberté de pensée (article 9) et le droit à un recours (article 13). Ces droits sont depuis longtemps consacrés dans plusieurs instruments internationaux, y compris le Pacte international relatif aux droits civils et politiques (PIDCP) et la Convention européenne des droits de l'homme, et il importe maintenant de les protéger et faire appliquer de manière plus effective dans l'environnement numérique.

Les progrès des technologies de communication et leur utilisation croissante ont rendu possible une surveillance à une échelle sans précédent. La dépendance croissante vis-à-vis des technologies – pour nous connecter, faire des affaires et même gérer une infrastructure domestique cruciale – amplifie la menace sur les droits de l'homme lorsque les usagers, entreprises et administrations n'ont plus confiance dans ces systèmes. Si la confiance n'est plus de mise, nous risquons de voir la liberté sur internet compromise et les avantages de l'environnement numérique pour tous annihilés.

Le présent rapport met en exergue les défis associés à la liberté sur internet, en s'intéressant en particulier au droit à la vie privée, à la protection des données et au respect des formes légales, dans le contexte des révélations de cet été sur la surveillance de masse. Le rapport identifie des éléments pour la formulation de politiques publiques et propose des lignes d'action à envisager dans le cadre du mandat du Conseil de l'Europe. Un rapport parallèle traite de la liberté sur internet, sous l'angle des droits associés à la liberté d'expression, à la liberté d'association et à la liberté des médias en Europe.

Le Conseil de l'Europe joue de longue date un rôle normatif dans le domaine des droits de l'homme en Europe et dans le monde. Le Comité des Ministres et l'Assemblée parlementaire du Conseil de l'Europe ont adopté des déclarations, résolutions et recommandations importantes qui promeuvent la liberté sur internet. Pour répondre aux nouveaux défis, atténuer les conséquences futures sur les droits de l'homme et réaliser son agenda relatif à la liberté sur internet, le Conseil de l'Europe devrait prendre en considération les recommandations ci-après, qui sont approfondies dans la deuxième partie de ce rapport :

### ***Saisir l'occasion de faire de la Convention n° 108 une norme internationale relative à la protection de la vie privée***

La protection de la vie privée représente un élément clef pour les libertés démocratiques. Le Conseil de l'Europe peut jouer un rôle déterminant dans la réaffirmation et le renforcement des normes internationales en actualisant la Convention de manière efficiente et en œuvrant pour sa large ratification de manière proactive.

### ***Renforcer le contrôle et la mise en œuvre de la Convention actualisée***

Afin de renforcer la mise en œuvre et le contrôle de la conformité, l'autorité compétente dans chaque pays signataire devrait désigner un point de contact unique dédié à la Convention au niveau national. Ce groupe de points de contact désignés pourrait se concerter à travers des réunions périodiques et jouer un rôle important dans les réponses aux nouveaux défis liés aux technologies en produisant des orientations communes sur des aspects spécifiques.

### ***Comblar autant que possible les lacunes subsistant dans la Convention***

Afin que la Convention serve véritablement de référence en matière de protection des données à caractère personnel, il importe qu'elle comporte le moins de failles possible, sachant que l'efficacité de la Convention dépend de son maillon le plus faible. Le Comité consultatif (T-PD) de la Convention n° 108 du Conseil de l'Europe, qui a déjà œuvré, avec diligence, à la modernisation du texte, devrait veiller à ce que la Convention ne soit pas affaiblie sur des points essentiels au nom de ce que certains Etats ont appelé une plus grande « interopérabilité » des systèmes de protection des données.

### ***Renforcement du rôle des autorités de protection des données***

Afin que les autorités de protection des données puissent remplir leur mandat, il est absolument essentiel qu'elles jouissent d'une indépendance à l'égard du pouvoir exécutif dans les Etats membres. Si le Conseil de l'Europe a déjà reconnu l'importance de l'indépendance et d'une dotation en ressources suffisantes des autorités de protection des données, les membres du Conseil de l'Europe devraient veiller à la mise en œuvre des propositions visant à intégrer le protocole additionnel de la Convention dans la version actualisée de la Convention n° 108. Au niveau des Etats membres, il importe de mettre en œuvre – ou appuyer – la réglementation de sorte à renforcer la position des autorités compétentes.

### ***Adoption et mise en œuvre des principes sur l'application des droits de l'homme à la surveillance des communications***

Pour faire face aux défis qui se posent en matière de protection des droits de l'utilisateur en ce qui concerne la surveillance des communications, les Principes sur l'application des droits de l'homme à la surveillance des communications (élaborés par la société civile) sont édifiants. Le Conseil de l'Europe, à un niveau tant régional que national, devrait jouer un rôle de premier plan dans la promotion de la liberté sur internet à travers l'adoption et la mise en œuvre de ces Principes.

D'autre part, le Programme européen de formation aux droits de l'homme pour les professionnels du droit (HELP) du Conseil de l'Europe, qui accomplit déjà un travail significatif dans ce domaine, devrait intégrer les Principes dans les futures manifestations, mesures de formation et activités diverses qui contribueront à élaborer des normes communes et à renforcer la coopération internationale en matière d'application du droit relatif aux droits de l'homme à la surveillance des communications.

### ***Instaurer une plus grande transparence***

La transparence étant essentielle pour s'assurer que les gouvernements et entreprises rendent des comptes, le Conseil de l'Europe devrait sérieusement envisager d'élargir son agenda relatif à la transparence pour inclure les rapports annuels accessibles au public sur les pratiques de surveillance par les Etats. Pour renforcer la responsabilité et le contrôle, les Etats membres du Conseil de l'Europe devraient instamment inviter les entreprises à publier les mêmes informations.

### ***Rétablir la confiance dans le secteur des entreprises***

Il est important de s'appuyer sur le travail déjà entrepris par le Conseil de l'Europe, notamment par le truchement du Groupe de rédaction sur les droits de l'homme et les entreprises (CDDH-CORP) du Conseil de l'Europe. Les récentes révélations sur la nature et l'étendue de la surveillance de masse nous édifient quant à la nécessité d'orientations supplémentaires, allant au-delà de ce qui est déjà énoncé dans les cadres de référence existants (par exemple, les Principes directeurs [des Nations Unies] relatifs aux entreprises et aux droits de l'homme). Le Conseil de l'Europe et ses Etats membres devraient adopter des mesures proactives en vue d'élaborer des lignes directrices opportunes et sectorielles et/ou sous-sectorielles spécifiques sur la façon dont les entreprises peuvent s'acquitter de leurs obligations de respecter les droits de l'homme, en particulier en rapport avec les défis liés à la liberté sur internet.

### ***Promouvoir la culture numérique***

Afin que les Etats honorent leurs obligations positives de protéger les droits de l'homme, les citoyens doivent avoir les moyens d'exercer un plus grand contrôle sur leurs données à caractère personnel, faire des choix éclairés concernant leurs habitudes en ligne et être davantage informés des risques potentiels et de la manière dont ils peuvent se protéger. Si le Conseil de l'Europe a déjà reconnu la nécessité d'une « sensibilisation en milieu scolaire aux droits d'autrui à exercer sa liberté d'expression », cette ligne d'action peut et devrait être élargie à tout l'éventail des droits qui se rapportent à la liberté sur internet, en particulier la protection de la vie privée et la protection des données.

De plus, les Etats membres du Conseil de l'Europe devraient promouvoir l'utilisation d'outils libres (« open source ») destinés à renforcer la protection de la vie privée, et prévoir des enveloppes financières spécifiques pour la conception, le développement et le déploiement de telles technologies.

### ***Renforcer les mesures de protection pour les donneurs d'alerte***

Pour s'assurer que les abus ayant trait aux atteintes aux droits de l'homme et à la corruption sont mis au jour, le Conseil de l'Europe et ses Etats membres devraient sans délai renforcer les mesures de protection des donneurs d'alerte. Le travail du Comité européen de coopération juridique (CDCJ) est exemplaire à cet égard, et le (projet de) recommandation sur la protection des donneurs d'alerte devrait être soutenu avec détermination par le Conseil de l'Europe et chacun de ses Etats membres.

## Introduction

Les récentes révélations sur les activités de surveillance de divers services de renseignement d'Etat ont suscité une réaction énergique de la part des instances internationales des droits de l'homme. M<sup>me</sup> Navi Pillay, Haut-Commissaire des Nations Unies aux droits de l'homme, a souligné que ces pratiques gouvernementales soulèvent un certain nombre de questions relatives au droit international des droits de l'homme qui doivent être traitées<sup>1</sup>. Dans son récent rapport A/HRC/23/40, Frank La Rue, Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression mentionne de même la nécessité d'un respect des formes légales et d'un contrôle judiciaire pour garantir ces droits fondamentaux dans le contexte de la surveillance exercée par les Etats<sup>2</sup>. En effet, les révélations de cet été concernant la surveillance de grande envergure exercée par certains Etats démontrent très clairement la nécessité d'une extension de l'agenda relatif à la liberté sur internet.

L'explosion des contenus de communication numérique, les « métadonnées des communications »<sup>3</sup>, la baisse du coût de stockage et d'exploration de grands ensembles de données par des prestataires externes, la possibilité d'associer et d'organiser des ensembles de données différents et le caractère plus sensible des informations accessibles rendent possible une surveillance à une échelle sans précédent, ce qui crée des menaces grandissantes pour les droits fondamentaux. Sachant qu'une part dominante et croissante des communications dans nos sociétés est réalisée via des supports électroniques, les détails les plus personnels et intimes des actions passées, présentes ou futures des individus peuvent être révélés.

Les rapports diffusés cet été, qui révèlent avec détails à l'appui l'ampleur des programmes de surveillance d'Etat, ont démontré qu'il ne s'agit pas d'un futur dystopique mais plutôt de la réalité contemporaine. Chaque courrier électronique, chaque conversation téléphonique, chaque publication sur Facebook, chaque opération bancaire, littéralement chaque communication et activité sur internet et les réseaux de télécommunication peuvent être et sont peut-être en train d'être surveillés par l'Agence nationale de sécurité des Etats-Unis d'Amérique (la NSA), son homologue britannique (le Quartier général des communications du gouvernement – GCHQ) ainsi que d'autres services de renseignement d'Etat. En effet, comme le Comité des Ministres l'a reconnu dans sa Déclaration [du 11 juin 2013] sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux, « [d]e telles possibilités et pratiques peuvent dissuader les citoyens de participer à la vie sociale,

---

1 Haut-Commissariat des Nations Unies aux droits de l'homme, "Mass surveillance: Pillay urges respect for right to privacy and protection of individuals revealing human rights violations," [non disponible en français]  
<http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13534&LangID=E>

2 La Rue, Frank, Report of the Special Rapporteur on the Promotion and Protection of the right to freedom of opinion and expression, A/HR/23/40 [rapport A/HR/23/40 du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, non disponible en français].

3 La Rue, Frank. Rapport A/HR/23/40 du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression (indiquant que les données de communication incluent des informations à caractère personnel sur l'identité, l'emplacement géographique et les activités des individus, ainsi que des journaux et informations connexes sur les courriels et autres communications envoyées ou reçues), paragraphe 6, [ci-après, Frank La Rue, rapport A/HR/23/40].



culturelle et politique et à plus long terme, avoir des effets dommageables sur la démocratie »<sup>4</sup>. D'un point de vue général, ces effets incluent la remise en cause de la liberté de recevoir et communiquer des informations, consacrée à l'article 10 et l'article 8 de la Convention européenne des droits de l'homme.

La Déclaration et le Programme d'action de Vienne énoncent que « [t]ous les droits de l'homme sont universels, indissociables, interdépendants et intimement liés. » Les libertés d'expression et d'association ne peuvent pas être pleinement exercées lorsque les droits à la protection de la vie privée et au respect des formes légales ne sont pas correctement protégés. Et cela, le Conseil de l'Europe l'a reconnu, dans sa stratégie relative à la gouvernance de l'internet, en soulignant que « [la] liberté, la dignité et le respect de la vie privée des usagers de l'internet doivent constituer une préoccupation centrale et une priorité des démocraties, et en particulier des gouvernements, qui s'appuient sur l'utilisation des nouvelles technologies et encouragent leur utilisation »<sup>5</sup>. Cet aspect ainsi que d'autres aspects de l'agenda du Conseil de l'Europe relatif à la liberté sur internet peuvent être développés afin de répondre aux défis que posent les nouvelles pratiques de surveillance du point de vue de la protection de la vie privée et du respect des formes légales. De même, il importe que cet agenda aborde la question du rôle du secteur privé, notamment en ce qui concerne les règles de protection des données ; après tout, la plupart des données analysées par la NSA, le GCHQ et d'autres services de renseignement sont à l'origine recueillies par des entreprises du secteur des technologies.

Ce rapport dresse le bilan des défis et menaces concernant la liberté sur internet dans les Etats membres du Conseil de l'Europe et analyse les rôles et responsabilités des acteurs étatiques et non étatiques dans la protection de cette liberté, en faisant particulièrement référence aux aspects suivants :

*le droit à la vie privée, notamment en rapport avec le contrôle et la surveillance des communications et activités des usagers d'internet, la conformité avec les normes du droit international, notamment la Convention européenne des droits de l'homme et la jurisprudence de la Cour européenne des droits de l'homme ;*

*le droit à la protection de la vie privée en ce qui concerne les données à caractère personnel, notamment en rapport avec la collecte et le traitement des données à caractère personnel par des acteurs étatiques et non étatiques, les sauvegardes et garanties procédurales (respect des formes légales), la conformité avec le droit international, notamment la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) et son Protocole additionnel (STE n° 181) ;*

---

4 Conseil de l'Europe, Déclaration du Comité des Ministres sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux, <https://wcd.coe.int/ViewDoc.jsp?id=2074329&Site=CM>

5 Stratégie du Conseil de l'Europe relative à la gouvernance de l'internet 2012-2015, [http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/CoE\\_IGS\\_adopted\\_F.pdf](http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/CoE_IGS_adopted_F.pdf), point n° 10

*le renforcement des capacités et la culture numérique, y compris la nécessité de s'assurer que les citoyens sont bien informés à propos des pratiques de collecte de données et de traitement mises en œuvre par des acteurs étatiques et non étatiques, et ont les moyens d'exercer un contrôle effectif sur leurs données à caractère personnel.*

Sur cette base, le rapport identifie des éléments pour l'élaboration de réponses et de lignes d'action souhaitables dans le cadre du mandat du Conseil de l'Europe relatif au traitement des menaces pour la liberté sur internet émanant des Etats, en particulier à la garantie de l'applicabilité des règles de protection de la vie privée, y compris à travers la coopération avec le monde des affaires en matière de respect des normes et de responsabilité dans le domaine des droits de l'homme sur l'internet.

## Première partie : Défis

### 1.1 *Les progrès technologiques rendent possible une surveillance à une échelle inimaginable jusque-là*

Les programmes de surveillance dont l'existence a été mis au jour par l'ancien consultant auprès de la NSA Edward Snowden, le journaliste Glenn Greenwald et la réalisatrice Laura Poitras ont ébranlé le monde. En juin 2013, il a été révélé que le gouvernement des Etats-Unis d'Amérique accédait en masse et de façon permanente et quotidienne<sup>6</sup> aux métadonnées des clients des entreprises de télécommunications dans le pays. Peu après cette révélation, il a été établi que neuf entreprises des secteurs d'internet et des technologies donnaient à l'Agence nationale de sécurité des Etats-Unis accès au contenu des comptes de leurs clients à travers un programme portant le nom de code de Prism<sup>7</sup>. Quelques programmes connexes, tels que XKeyScore qui permet au gouvernement américain d'accéder au contenu du courrier électronique, aux recherches en ligne, à l'activité sur les réseaux sociaux et aux métadonnées de tout usager et de les explorer, ont aussi été mis au jour<sup>8</sup>. Par ailleurs, l'opinion publique a appris qu'en plus des Etats-Unis, d'autres puissances dans le monde, telles que le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande, consultent et échangent les données de communication de leurs citoyens dans le cadre d'un accord de renseignement informel dénommé « Five Eyes »<sup>9</sup>.

---

<sup>6</sup> The Guardian, "NSA collecting phone records of millions of Verizon customers daily," <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

<sup>7</sup> The Guardian, "NSA Prism program taps into user data of Apple, Google and others," <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

<sup>8</sup> The Guardian, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'," <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>

<sup>9</sup> The Guardian, "NSA leaks: US and Britain team up on mass surveillance," <http://www.theguardian.com/world/2013/jun/22/nsa-leaks-britain-us-surveillance>

Par ailleurs, ainsi que l'a indiqué The Guardian, le GCHQ coopère étroitement avec la NSA pour recevoir « directement » des données en provenance des câbles sous-marins et terrestres à fibres optiques qui constituent la dorsale d'internet. A travers des programmes destinés à capter les flux de données « en amont », tels que Stellar Wind, Fairview, Blarney, Oakstar, Lithium, Stormbrew et Tempora<sup>10</sup>, la NSA, le GCHQ et d'autres services de renseignement ont les moyens d'accéder à la *totalité* du trafic téléphonique et internet transitant par les câbles à fibres optiques qui relient la plus grande partie du monde ainsi qu'environ 75 % du réseau national des Etats-Unis<sup>11</sup>.

Nos sociétés sont de plus en plus dépendantes à l'égard des technologies de communication : entrer en contact avec les amis, proches ou collègues, effectuer des transactions commerciales mais aussi, dans de nombreux pays, gérer des services de base cruciaux (tels que la fourniture d'électricité) représentent autant d'activités que l'on peut aujourd'hui faire en ligne – ainsi, pour une bonne partie, les échanges commerciaux s'effectuent aujourd'hui en ligne. Ces systèmes doivent être dignes de confiance. Cependant, les politiques visant à assurer l'ordre et, en particulier, la sécurité nationale, se sont enfermées dans la perspective de la surveillance. Cette approche a présenté aux citoyens un choix faustien entre la sécurité et protection de la vie privée, laissant entendre qu'il faut sacrifier l'un pour jouir pleinement de l'autre. Cela n'est pas vrai. Comme le montrent les rapports publiés par The Guardian, la NSA, le GCHQ et d'autres services de renseignement introduisent de plus en plus de nouvelles vulnérabilités dans l'architecture d'internet<sup>12</sup>, ce qui non seulement pose des défis de taille pour la protection de la vie privée des usagers dans le monde entier mais aussi menace l'intégrité et la sécurité de cette ressource mondialement partagée.

Etant donné que les canaux à travers lesquels nous communiquons sont pour l'essentiel détenus et exploités par entreprises, les entreprises du secteur des technologies sont forcément impliquées dans la réalisation de la liberté sur internet. Les Principes directeurs [des Nations Unies] relatifs aux entreprises et aux droits de l'homme énoncent clairement que les entreprises ont la responsabilité de *respecter* les droits de l'homme, et ce, d'autant plus que ce sont elles qui conçoivent, développent et mettent en œuvre des technologies qui facilitent la surveillance.

## 1.2 La surveillance basée sur le contournement des formes légales

Les services chargés de l'application de la loi et les organismes de sécurité d'Etat ont montré un intérêt accru à accéder à la myriade de données qui sont produites, collectées et stockées du fait de l'omniprésence des technologies de communication. La prévalence croissante de l'informatique dématérialisée (« cloud computing » – stockage de données sur internet, par le truchement d'un prestataire externe, plutôt que sur

---

10 The Guardian, "GCHQ taps fibre-optic cables for secret access to world's communications," <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

11 The Wall Street Journal, "New Details Show Broader NSA Surveillance Reach," <http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html>

12 The Guardian, "Revealed: how US and UK spy agencies defeat internet privacy and security," <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

l'ordinateur personnel)<sup>13</sup> rend plus complexe les efforts visant à faire respecter les réglementations nationales et régionales protégeant les droits de l'homme, dans la mesure où les données sont de plus en plus stockées dans des conditions impliquant des conflits de compétence. Cela pose un défi du point de vue de la protection effective de la vie privée de l'utilisateur, lorsque les normes en la matière dans la région ou le pays où l'utilisateur est établi sont en contradiction avec les normes du lieu où ces données sont stockées ou traitées ou par lequel elles transitent.

Par ailleurs, le Commissaire aux droits de l'homme du Conseil de l'Europe, M. Nils Muižnieks, a souligné que « [d]eux principes essentiels, la proportionnalité et le contrôle juridictionnel, doivent être appliqués systématiquement lors du recours à des mesures comme la restriction de l'accès à internet ou la mise sous surveillance des activités en ligne »<sup>14</sup>. Toutefois, dans son rapport A/HRC/23/40, le Rapporteur spécial M. Frank La Rue a averti que cette dynamique pose un défi du point de vue du respect des formes légales, sachant que l'accès aux données de communication peut être obtenu dans de nombreux Etats sans autorisation indépendante et moyennant un contrôle limité<sup>15</sup>.

Les lois réglementant la capacité des Etats à pratiquer une surveillance, notamment établissant les critères obligatoires de nécessité, proportionnalité et légitimité, soit sont inadaptées pour la mission concernée soit n'existent tout simplement pas. Cela crée un environnement propice aux abus et soumet l'Etat de droit rude à épreuve<sup>16</sup>.

### ***1.3 L'absence d'éclaircissements sur le droit à la protection de la vie privée entrave sa protection***

Si la quasi-totalité des cadres juridiques internationaux, régionaux et nationaux ont consacré le droit à la protection de la vie privée, dans la pratique ces documents ne comportent pas d'orientations à un niveau opérationnel quant aux modalités de protection de ce droit.

M. Frank La Rue indique que les Etats peuvent tirer profit d'une explication plus nuancée de la protection de la vie privée et de la façon dont les technologies actuelles peuvent porter atteinte à ce droit. Il définit la protection de la vie privée comme la présomption selon laquelle l'individu devrait avoir une sphère de développement autonome, d'interaction et de liberté, « sphère privée » dans laquelle il interagit avec d'autres individus le cas échéant, sans intervention de l'Etat ni intervention excessive non sollicitée d'autres personnes non invitées<sup>17</sup>.

---

13 Voir brochure rédigée par des membres et observateurs de European Digital Rights (EDRi) : EDRi, "An Introduction to Data Protection" (Spring 2013), [http://www.edri.org/files/paper06\\_datap.pdf](http://www.edri.org/files/paper06_datap.pdf)

14 Commentaires du Commissaire aux droits de l'homme du Conseil de l'Europe, « La liberté de la presse à l'ère numérique : nouvelles menaces, nouveaux défis », <http://fr.humanrightcomment.org/2013/05/03/liberte-de-la-presse/>

15 Frank La Rue, Rapport A/HR/23/40, paragraphe 17

16 Voir Frank La Rue, Rapport A/HR/23/40, paragraphes 3 et 17.

17 Frank La Rue, Rapport A/HR/23/40.

En outre, d'après l'article 8 de la Convention européenne des droits de l'homme, toute ingérence dans le droit à la protection de la vie privée doit être exercée en conformité avec la loi, obéir à un objectif légitime (tel que défini à l'article 8(2)) et être nécessaire dans une société démocratique. Etant donné les intrusions flagrantes dans la vie privée au niveau national<sup>18</sup>, régional<sup>19</sup> et international<sup>20</sup>, il est manifeste que les orientations devant permettre aux Etats de prendre des décisions sur ces points ou de protéger cet équilibre sont insuffisantes.

En réponse à ces défis, et aux fins de guider les Etats dans l'évaluation de la conformité des pratiques de surveillance des communications avec le droit international et les normes internationales relatives aux droits de l'homme, un groupe d'organisations de la société civile et de juristes a rédigé les « Principes internationaux sur l'application des droits de l'homme à la surveillance des communications »<sup>21</sup>. Les Principes sont édifiants dans le présent contexte et il est utile de les citer in extenso :

Le caractère intrusif de la surveillance des communications est traditionnellement évalué sur la base de catégories artificielles et formelles. Les cadres légaux existants font la distinction entre le "contenu" et les "données hors contenu", les "informations sur l'abonné" et les "métadonnées", les données stockées et celles en transit, les données conservées dans leur emplacement d'origine et celles transmises à un prestataire de services tiers<sup>22</sup>. Pourtant, ces distinctions ne sont plus appropriées pour mesurer le niveau d'intrusion entraîné par la surveillance des communications dans la vie privée et les relations sociales des individus. Il est admis de longue date que le contenu des communications nécessite une protection légale importante dans la mesure où il peut révéler des informations sensibles. Toutefois, il est maintenant clair que d'autres informations issues des communications d'un individu, telles que les métadonnées et d'autres formes de données hors contenu, peuvent fournir plus de renseignements sur cette personne que le contenu lui-même. Elles doivent donc bénéficier d'une protection équivalente. Aujourd'hui, qu'elles soient analysées séparément ou conjointement, ces informations peuvent permettre de déterminer l'identité d'un individu et d'en

---

18 Ton Siedsma, Bits of Freedom, <https://www.bof.nl/2013/05/02/dutch-hacking-proposal-puts-citizens-at-risk/> 2 May, 2013

19 Access, Commonwealth of Surveillance States: on the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia, [https://www.accessnow.org/page/-/docs/Commonwealth\\_of\\_Surveillance\\_States\\_ENG\\_1.pdf](https://www.accessnow.org/page/-/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf)

20 The Washington Post, "Agreements with private companies protect U.S. access to cables' data for surveillance," [http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01\\_story.html?Post+generic=%3Ftid%3Dsm\\_twitter\\_washingtonpost](http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html?Post+generic=%3Ftid%3Dsm_twitter_washingtonpost)

21 Principes internationaux sur l'application des droits de l'Homme à la surveillance des communications, <https://fr.necessaryandproportionate.org/text> (ci-après les « 13 Principes internationaux »)

22 "Les gens divulguent les numéros qu'ils appellent ou auxquels ils envoient des SMS à leurs opérateurs mobiles, les URL qu'ils consultent et les adresses e-mail avec lesquelles ils correspondent à leurs fournisseurs de services internet, ainsi que les livres, les articles et les médicaments qu'ils achètent à leurs boutiques en ligne... On ne peut pas considérer que toutes ces informations, volontairement divulguées à certaines personnes dans un but spécifique, sont, de ce seul fait, exclues de la protection du 4e amendement de la Constitution." United States v. Jones, 565 U.S. \_\_\_, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

savoir plus sur son comportement, ses relations, son état de santé, son origine ethnique, sa couleur de peau, son orientation sexuelle, sa nationalité ou ses opinions. Elles peuvent également être utilisées pour établir une carte complète des déplacements et des interactions de cette personne dans le temps<sup>23</sup>, ou de toutes les personnes présentes à un endroit donné, par exemple dans le cadre d'une manifestation ou d'un rassemblement politique. Par conséquent, toutes les informations qui contiennent les communications d'une personne ou sont relatives à ces communications, et qui ne sont pas publiquement et facilement accessibles, doivent être considérées comme des "informations protégées". Elles doivent donc, à ce titre, bénéficier du plus haut niveau de protection au regard de la loi.

Pour évaluer le caractère intrusif de la surveillance des communications par l'État, il convient de prendre en considération non seulement le risque de divulgation des informations protégées, mais également les raisons pour lesquelles l'Etat recherche ces informations. Si la surveillance des communications a pour conséquence de révéler des informations protégées susceptibles d'exposer une personne à des enquêtes, des discriminations ou des violations des droits de l'homme, elle constitue à la fois une violation sérieuse du droit au respect de la vie privée et une atteinte à la jouissance d'autres droits fondamentaux tels que la liberté d'expression, d'association et d'engagement politique. En effet, ces droits ne sont effectifs que si les personnes ont la possibilité de communiquer librement, sans subir l'effet d'intimidation qu'engendre la surveillance gouvernementale. Il est donc nécessaire de rechercher, pour chaque cas particulier, tant la nature des informations collectées que l'usage auquel elles sont destinées.

#### **1.4 Opacité autour de la collecte de données**

La transparence de l'action du gouvernement est une condition préalable essentielle de la responsabilité des Etats et d'une participation libre, entière et sûre de tous les individus au sein de la société. La surveillance s'exerce dans l'ombre depuis trop longtemps – notamment, la déclaration volontaire des types de données collectées, des fins de la collecte et des parties avec lesquelles les données sont partagées est limitée voire inexistante. En effet, les révélations de cet été ont montré que le défaut de transparence a contribué à l'abus systémique des droits de l'homme.

Comme l'a rappelé Louis Brandeis, « on dit souvent que la lumière du soleil est le meilleur des désinfectants » ; une plus grande transparence autour des activités de surveillance menées par les gouvernements et des demandes d'accès aux données des usagers, que ce soit aux fins de la sécurité nationale ou de la répression pénale traditionnelle, est un premier pas fondamental. A cet égard, de nombreuses entreprises impliquées dans le programme PRISM de la NSA, dont Google, Facebook, Yahoo! et Microsoft, ont publié des rapports de transparence et se battent actuellement devant le

---

23 "La surveillance à court terme des déplacements d'une personne sur la voie publique est compatible avec la protection de la vie privée", mais "l'utilisation de systèmes de surveillance GPS à plus long terme dans les enquêtes sur la plupart des infractions empiète sur le respect de la vie privée." United States v. Jones, 565 U.S. \_\_\_, 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

Foreign Intelligence Surveillance Court (tribunal de la surveillance et des renseignements étrangers) pour être affranchies de l'impératif de silence qui les empêchent de communiquer davantage de précisions sur leur implication dans les activités de surveillance menées par l'Etat<sup>24</sup>. Ces entreprises et d'autres se sont associées à plusieurs groupes de la société civile, investisseurs et associations professionnelles dans la Coalition WeNeedToKnow<sup>25</sup> pour faire pression sur le Congrès des Etats-Unis et l'administration Obama afin que ces derniers permettent aux entreprises de rendre compte du nombre précis de demandes qu'elles reçoivent, des lois en vertu desquelles ces demandes sont émises, du nombre précis d'utilisateurs et dispositifs concernés ainsi que des autorités spécifiques qui formulent ces demandes. Par ailleurs, la Coalition demande au gouvernement de publier les mêmes informations, ce qui assurerait une vérification et une reddition de comptes à double sens et crédibles.

Alors que la Direction du renseignement national des Etats-Unis (Office of the US Director of National Intelligence) a affirmé que le gouvernement américain publiera un rapport de transparence, incluant les demandes autorisées par la loi sur la surveillance et les renseignements étrangers (Foreign Intelligence Surveillance Act) et la loi Patriot (Patriot Act), elle est loin de respecter cette norme<sup>26</sup>. D'autre part, à l'heure actuelle, pas un seul membre du Conseil de l'Europe ne publie un rapport de transparence incluant les demandes émises dans le cadre d'enquêtes liées à la sécurité nationale.

Il convient de signaler que plusieurs pays publient des rapports précisant les demandes émises dans le cadre d'enquêtes pénales traditionnelles, apparemment sans effets préjudiciables<sup>27</sup>. Et, même si un mal transparent reste un mal, le fait d'adopter des mesures concrètes pour informer les citoyens sur la façon dont les Etats mettent en œuvre la surveillance permet aux individus, organisations de la société civile, autorités de protection des données et institutions nationales des droits de l'homme de demander des comptes aux gouvernements et entreprises.

Outre une plus grande responsabilisation, les rapports de transparence détaillés permettent un débat public mieux informé sur la surveillance exercée par les Etats et les réformes juridiques nécessaires. De même, des rapports crédibles peuvent aider les autorités de protection des données et les institutions nationales de droits de l'homme à mieux comprendre l'étendue, la nature et l'application de pratiques de surveillance, et elles peuvent ainsi affecter les ressources de manière plus rationnelle pour relever les défis concernant la protection de la vie privée et la protection des données et partant, s'acquitter de leur mandat de façon plus efficace. Enfin, en fournissant des détails sur les abus, les rapports de transparence permettent aux usagers de demander réparation

---

24 Politico, "Yahoo, Facebook file suits on surveillance orders," <http://www.politico.com/story/2013/09/yahoo-facebook-surveillance-orders-96506.html>

25 Access, "We need to know: companies, civil society call for transparency on surveillance," <https://www.accessnow.org/blog/2013/07/18/tech-companies-and-civil-society-join-call-on-the-us-government-to-is>

26 Access, "Obama Administration continues to thwart meaningful transparency on NSA surveillance," <https://www.accessnow.org/blog/2013/08/30/obama-administration-continues-to-thwart-meaningful-transparency-on-nsa-sur>

27 Voir rapport annuel 2012 du Commissaire à l'interception des communications (en anglais), <http://www.iocco-uk.info/docs/2012%20Annual%20Report%20of%20the%20Interception%20of%20Communications%20Commissioner%20WEB.pdf>



pour les préjudices subis, conformément à l'article 13 de la Convention européenne des droits de l'homme.

### *1.5 Atteintes des entreprises aux droits de l'homme*

Une énorme majorité des données que les usagers, entreprises et même les gouvernements génèrent en quantités record et qui sont acquises et analysées dans le cadre de la surveillance ne sont en fait pas collectées par les Etats eux-mêmes, mais plutôt par des entreprises. Et il s'agit d'une activité commerciale non négligeable. Les données à caractère personnel sont souvent qualifiées de « monnaie » de l'ère numérique. L'exploration et la collecte de données à caractère personnel représentent aujourd'hui un chiffre d'affaires de plusieurs milliards de dollars par an. Rien qu'en Europe, la valeur des données des citoyens européens en 2011 s'est élevée à 315 milliards d'euros. D'après les estimations, elle atteindra environ 1 000 milliards d'euros par an d'ici 2020<sup>28</sup>.

Mais les données ne représentent pas tout simplement une valeur monétaire, dans la mesure où il s'agit d'éléments d'information collectées qui concernent la vie privée d'individus. En effet, la Cour européenne des droits de l'homme a reconnu que le simple traitement de données à caractère personnel pourrait représenter une atteinte au droit à la vie privée<sup>29</sup>. Comme l'a reconnu le Conseil de l'Europe, la protection des données à caractère personnel est un droit élémentaire ; en effet, la Convention n° 108 garantit à « toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ("protection des données"). »

Sachant que ce sont les données collectées par les entreprises qui font tourner la machine de la surveillance, les rôles et les responsabilités du secteur privé méritent une attention toute particulière. Les Principes directeurs relatifs aux entreprises et aux droits de l'homme obligent les entreprises à respecter les droits de l'homme et à réparer les abus qui surviennent. Pour compléter les orientations de haut niveau relatives aux Principes, la Commission européenne, en coopération avec le secteur concerné, la société civile et parties intéressées dans le domaine des droits des consommateurs, a récemment publié le document « ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights »<sup>30</sup>, manuel destiné à guider les entreprises du secteur des TIC sur l'observation des obligations découlant des Principes directeurs [des Nations Unies] relatifs aux entreprises et aux droits de l'homme. Les Etats devraient encourager l'élaboration d'orientations à l'intention des entreprises opérant à

---

28 Viviane Redding, « Data protection reform: restoring trust and building the digital single market », Commission européenne, SPEECH/13/720, 17.9.2013 [non disponible en français], [http://europa.eu/rapid/press-release\\_SPEECH-13-720\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-13-720_en.htm)

29 Voir document "Case law of the European Court of Human Rights concerning the protection of personal data", DP(2013)CASE LAW, 30 janvier 2013 [non disponible en français], [http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD\\_documents/DP%202013%20Case%20Law\\_Eng%20%28final%29.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/DP%202013%20Case%20Law_Eng%20%28final%29.pdf)

30 Commission européenne, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights [non disponible en français], [http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business\\_en.pdf](http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf)



l'intérieur de leurs frontières et au-delà dans le but d'assurer une protection globale des droits de leurs citoyens.

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n° 108) établit une base solide pour la protection des données, sachant que la somme des principes y énoncés pourrait servir à réduire les risques concernant la protection de la vie privée qui sont associés à la surveillance électronique des communications. Pour les acteurs étatiques et non étatiques qui collectent des données, cela signifierait, par exemple, collecter moins de données (minimisation des données), s'assurer que les données à caractère personnel sont collectées et stockées à des fins rigoureusement définies et ne sont pas utilisées d'une manière incompatible avec ces fins (article 5) et appliquer des mesures de sécurité appropriées aux données qui sont stockées (article 7). Dans la pratique, cela pourrait signifier la prise en compte du respect de la vie privée dès la conception, ainsi que le préconisent la réglementation de protection des données proposée par l'UE et l'article 8bis (3) des propositions de modernisation de la Convention<sup>31</sup>.

Pour les usagers, le contrôle des données à caractère personnel revêt une importance capitale dans la mesure où il permet aux citoyens de prendre, en connaissance de cause, des décisions sur les personnes qui peuvent avoir accès à leurs données et avec lesquelles ils peuvent partager ces données. L'article 8 de la Convention n° 108 est instructif à cet égard, vu qu'il reconnaît le droit d'accès, d'effacement ou de rectification. Les Etats devraient mettre en place au niveau national des mesures de protection assorties de mécanismes aptes à les faire respecter. La réglementation de protection des données proposée par l'UE est aussi instructive à cet égard, dans la mesure où elle vise à permettre aux citoyens d'exercer un contrôle sur leurs données, à harmoniser les règles et renforcer les pouvoirs d'exécution dans l'UE<sup>32</sup>. Cela étant dit, la valeur finale de la proposition sera déterminée par les résultats du processus en cours, qui a donné lieu à des pressions sans précédent de la part de pays tiers et d'entreprises, dont un bon nombre sont impliqués dans le scandale PRISM<sup>33</sup>.

Considérant que le respect du secret des communications est essentiel pour les libertés d'expression et d'association, les entreprises ont un rôle à jouer en honorant leur devoir de respecter les droits de l'homme à travers un appui à l'expression sous couvert d'anonymat. Dans l'intervalle d'environ une décennie et demie, internet est devenu un outil inestimable dont on dépend pour trouver des informations fiables, parfois à caractère privé, ainsi qu'un forum de discussion et d'expression. Il existe toute une série de motifs pour lesquels un individu peut vouloir communiquer de façon anonyme ou sous un pseudonyme, par exemple le fait d'être un(e) adolescent(e) LGBT, une victime de violence domestique, un militant des droits de l'homme ciblé par son gouvernement

---

31 Voir : T-PD\_2012\_04\_rev2\_fr (16 octobre 2012), [http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD\\_documents/T-PD\\_2012\\_04\\_rev2\\_Fr.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD_2012_04_rev2_Fr.pdf)

32 Voir le document (en anglais) : EDRI, "Key Issues for the Data Protection Regulation" (Spring 2013), <http://protectmydata.eu/briefguide/key-issues/>

33 Voir le document (en anglais) : EDRI and Access, "Lobbying Against the Data Protection Regulation (Spring 2013), <http://www.edri.org/files/eudatap-03.pdf>; voir aussi le document (en anglais) extrait du blog d'EDRI : "US lobbying against the data protection reform intensifies (17 January 2013), <http://www.edri.org/us-eudatap>

en tant qu'opposant, un donneur d'alerte ou journaliste qui lutte pour mettre au jour un abus de pouvoir ou tout simplement quelqu'un qui souhaite préserver le caractère privé de ses activités en ligne. De la manière façon qu'on est plus à l'aise dans l'intimité de sa maison que sur la place publique pour parler de certaines choses, la surveillance en ligne a un effet paralysant sur la liberté d'expression sur la Toile. Il est crucial de veiller à la possibilité de pratiquer des activités en ligne de manière anonyme, et plus généralement au secret des communications, de sorte à ce que les individus puissent communiquer et recevoir des informations sans gêne ni crainte ni représailles.

Le Conseil de l'Europe a déjà reconnu l'importance de l'anonymat pour le renforcement de la liberté d'expression et la libre circulation des idées, dans la Déclaration sur la liberté de la communication sur l'internet (2003)<sup>34</sup>, et a déterminé dans sa stratégie relative à la gouvernance de l'internet 2012-2015 qu'un réexamen de ces normes s'impose. Ce réexamen doit notamment aborder les défis pour l'anonymat et l'utilisation d'un pseudonyme sur la Toile, que pose le non-cryptage du trafic internet et des télécommunications, point qui est examiné dans la partie suivante.

### ***1.6 Non-cryptage du trafic internet et pressions croissantes sur les entreprises privées afin qu'elles introduisent des vulnérabilités en matière de sécurité dans les produits et services***

Lorsque les paquets de données circulent sur internet, des ordinateurs des usagers jusqu'aux serveurs des sites internet, ils transitent par une quinzaine de routeurs intermédiaires, généralement en empruntant les câbles terrestres et sous-marins à fibres optiques qui constituent la dorsale d'internet<sup>35</sup>. Comme mentionné tantôt, The Guardian a révélé que la NSA et le GCHQ ont mis ces câbles à fibres optiques sur écoute, ce qui leur permet d'intercepter et collecter pratiquement toutes les communications, généralement sans même avoir à notifier une ordonnance spécifique à l'entreprise prestataire<sup>36</sup>. Ces services de renseignement peuvent analyser les données en question sans entrave car la majeure partie du trafic internet n'est pas cryptée. Dans le cas où les sites internet cryptent le trafic de leurs usagers, les services de renseignement et les services chargés de l'application de la loi doivent alors plutôt intervenir directement au niveau de ces sites internet pour acquérir les données des usagers, ce qui implique beaucoup plus de garanties procédurales. Si certaines entreprises telles que Blackberry ont été contraintes de livrer leurs clés de cryptage principales à plusieurs gouvernements<sup>37</sup>, d'autres entreprises telles que Microsoft livrent d'elles-mêmes, et apparemment sans y avoir été contraintes, leurs clés de

---

34 Comité des Ministres Déclaration sur la liberté de la communication sur l'internet, <https://wcd.coe.int/ViewDoc.jsp?Ref=Decl-28.05.2003&Language=lanFrench, 28.05.2003>

35 University of Washington - Computer Science and Engineering, Reverse Tracerout Network Diagnostic Utility, <http://revtr.cs.washington.edu/FAQ.html#how>

36 Voir note de bas de page 10.

37 The Economic Times, "Black Berry maker Research in Motion agrees to hand over its encryption keys to India," [http://articles.economictimes.indiatimes.com/2012-08-02/news/33001399\\_1\\_blackberry-enterprise-encryption-keys-corporate-emails](http://articles.economictimes.indiatimes.com/2012-08-02/news/33001399_1_blackberry-enterprise-encryption-keys-corporate-emails)

cryptage pour des services tels que Outlook et Skydrive<sup>38</sup>, le service de stockage dématérialisé de la firme citée.

En même temps que la NSA pratique la surveillance, elle est aussi chargée de protéger la cybersécurité. A cette fin, la NSA collabore étroitement avec des entreprises du secteur des technologies, soi-disant pour les aider à sécuriser leurs réseaux, mais il semble qu'elle y ait aussi installé des portes dérobées (« backdoors ») dans l'optique de les exploiter ultérieurement<sup>39</sup>. Mais ces vulnérabilités ne sont pas accessibles à la NSA uniquement ; des tierces parties, y compris d'autres gouvernements et ou des pirates malveillants peuvent également s'en servir, ce qui nuit à la sécurité de l'ensemble des usagers<sup>40</sup>.

Les Etats-Unis d'Amérique ont réussi un exploit similaire sur le plan de législation. La loi relative à l'assistance dans le domaine des communications aux fins de l'application du droit (« Communications Assistance for Law Enforcement Act » – CALEA) impose à toutes les entreprises de télécommunication de concevoir leurs réseaux de sorte à faciliter les écoutes électroniques. Cependant, elle n'impose pas explicitement aux entreprises qui livrent le trafic internet (y compris les fournisseurs VoIP) d'installer de telles portes dérobées, point que les milieux des services d'application de la loi et de la sécurité nationale essaient actuellement de modifier.

La dernière fois que les organismes américains chargés de l'application de la loi et de la sécurité nationale ont cherché à introduire une porte dérobée dans l'ensemble des systèmes de communication gérant du trafic crypté, c'est-à-dire à l'occasion de l'initiative « Clipper Chip » des années 90, l'algorithme de cryptage classé de la puce s'est finalement avéré peu sécurisé et le protocole Clipper, facile à contourner. Au niveau le plus fondamental, les portes dérobées introduisent dans les systèmes de communication sécurisés une faille qui n'existait pas auparavant, et ainsi, que ces systèmes soient purement algorithmiques ou axés sur un protocole, un intrus déterminé et le temps suffisent pour en venir à bout<sup>41</sup>. L'imposition de l'utilisation d'un produit présentant une faille met en exergue la contradiction inhérente aux portes dérobées : cette démarche conduit à donner à l'utilisateur un produit non sûr au nom de la sécurité de ce même usager. Le public a rejeté cette contradiction il y a déjà vingt ans de cela, mais c'est un problème auquel nous devons toujours faire face aujourd'hui.

---

38 The Guardian, "Microsoft handed the NSA access to encrypted messages,"  
<http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data>

39 The New York Times, "N.S.A. able to foil basic safeguards of privacy on web,"  
<http://www.nytimes.com/2013/09/06/us/nsa-foils-much--encryption.html?pagewanted=all&r=0>

40 Access, "You wouldn't leave your backdoor unlocked: the danger of intentional vulnerabilities,"  
<https://www.accessnow.org/blog/2013/09/20/you-wouldnt-leave-your-backdoor-unlocked-the-danger-of-intentional-vulnerab>

41 Bruce Schneier, "The problems with CALEA II" (4 June 2013),  
[https://www.schneier.com/blog/archives/2013/06/the\\_problems\\_wi\\_3.html](https://www.schneier.com/blog/archives/2013/06/the_problems_wi_3.html)

### ***1.7 La justification de la législation sur la surveillance s'est renforcée au détriment de la nécessité, proportionnalité et finalité légitime***

M. Frank La Rue a souligné dans son récent rapport que l'évolution des technologies s'est accompagnée d'une évolution de l'attitude à l'égard de la surveillance des communications. Aux Etats-Unis, par exemple, cette surveillance (écoutes électroniques, entre autres) a été réalisée sur une base restreinte et n'a été sanctionnée qu'à contrecœur par la justice. Toujours selon M. La Rue, cependant, au fil du temps, les Etats ont étendu les pouvoirs en matière de surveillance, abaissant le seuil et renforçant les justifications de cette pratique<sup>42</sup>.

Il convient de signaler à cet égard l'adoption, à l'échelle mondiale, de la mesure de la conservation de données de communication. Par exemple, la Directive sur la conservation des données, adoptée par l'Union européenne en 2006, impose que toutes les données de télécommunication – y compris celles de la téléphonie mobile et fixe, de la télécopie et du courrier électronique – soient sans distinction collectées et conservées pendant une durée comprise entre six mois et deux ans. Cette conservation à grande échelle de données relatives aux activités des citoyens, en dehors de toute enquête pénale, pose un défi de taille pour les fondements mêmes de l'Etat de droit et du droit international relatif aux droits de l'homme, y compris l'article 8 de la Convention européenne des droits de l'homme.

Dans plusieurs Etats membres, notamment la Roumanie, la Suède, la République tchèque et l'Allemagne, les textes nationaux transposant la Directive ont été contestés avec succès sur la base de la constitutionnalité<sup>43</sup>. Par ailleurs, la Commission européenne n'a jamais pu établir de manière crédible la nécessité et la proportionnalité d'une conservation généralisée de données<sup>44</sup>.

La Cour européenne des droits de l'homme a aussi fait valoir son point de vue, à travers un certain nombre d'arrêts qui ont conclu que la surveillance des données relatives au trafic enfreint l'article 8 de la Convention<sup>45</sup> ; que la conservation de dossiers sur les activités passées constitue une ingérence dans le droit à la vie privée<sup>46</sup> ; que la surveillance est « illicite » si elle est pratiquée sans discernement et ne repose pas sur un régime juridique spécifique<sup>47</sup> ; et enfin, que la surveillance ne peut être considérée

---

42 Frank La Rue, Rapport A/HR/23/40, paragraphe 16.

43 Internet Policy Review, EU Data Retention Directive finally before European Court of Justice, <http://policyreview.info/articles/news/eu-data-retention-directive-finally-european-court-justice/162>

44 Freedom Not Fear, Internal memo on EU communications data retention directive leaked (26 Jan 2012), <http://www.vorratsdatenspeicherung.de/content/view/520/55/lang,en/>

45 Amann c. Suisse, CEDH, requête n° 27798/95, arrêt du 16.2.2000.

46 Rotaru c. Roumanie, CEDH, requête n° 28341/95, arrêt du 4.5.2000.

47 Voir Kruslin c. France, CEDH, requête n° 11801/85, arrêt du 24.4.1990 ; Amann c. Suisse, CEDH, requête n° 27798/95, arrêt du 16.2.2000 ; Kopp c. Suisse, CEDH, requête n° 13/1997/797/1000, arrêt du 25.03.1998.

comme licite que si des garanties efficaces ont été mises en place de manière à réduire au minimum les atteintes aux droits et que toutes les autres solutions substitutives ont été épuisées<sup>48</sup>.

A propos de ce dernier point, il existe des moyens de surveillance substitutifs plus proportionnés, tels que la préservation des données, qui pourraient s'avérer plus efficaces et moins nocifs pour les droits de l'homme. La préservation des données (« data freeze »), par exemple, subordonnerait la préservation à une décision judiciaire, au cas par cas, c'est-à-dire s'il existe des motifs raisonnables de penser que la cible est impliquée dans des activités criminelles ou si elle est visée par une enquête pénale pour des motifs légitimes<sup>49</sup>.

Les études sur la manière dont la surveillance – et la conservation des données en particulier – a des répercussions sur les sociétés laissent à désirer et sont ignorées dans la plupart des évaluations d'impact à l'occasion de l'adoption des lois en question. Cependant, le problème fondamental est que lorsque les citoyens sont placés sous surveillance ils modifient leur comportement ; en toute vraisemblance, moins à l'aise pour s'exprimer, ils s'autocensurent ou s'abstiennent d'utiliser certains canaux de communication. Cet effet paralysant ne relève pas d'une vue de l'esprit. Il ressort d'une étude réalisée en Allemagne après la transposition de la Directive sur la conservation des données en 2008, que 11 % des répondants s'étaient déjà abstenus d'utiliser le téléphone ou le courrier électronique à certaines occasions. De plus, 52 % des répondants ont indiqué qu'ils n'utiliseraient probablement pas les télécommunications en cas de nécessité de confidentialité, par exemple pour s'entretenir avec un conseiller en matière de drogue, psychothérapeute ou conseiller matrimonial, du fait de la pratique de conservation des données<sup>50</sup>.

La Directive est actuellement attaquée devant la Cour de justice européenne (CJUE) au motif d'une possible violation de la Charte européenne des droits fondamentaux<sup>51</sup>. A l'heure actuelle, on ne sait pas quand la CJUE rendra son arrêté, ni les conséquences qu'un tel arrêté aura sur la conservation obligatoire des données dans l'Union européenne.

---

48 Voir rapport : Privacy International, Briefing for Members of the European Parliament on data retention, Chapter II (26 Sep 2006), <https://www.privacyinternational.org/reports/briefing-for-members-of-the-european-parliament-on-data-retention/invasive-and-illegal>

49 Voir: Open Rights Group, "Chapter Five Part I," <https://www.openrightsgroup.org/ourwork/reports/digital-surveillance/chapter-five-part-i> ;

voir aussi : Caspar Bowden, "Submission to the Joint Committee on the draft Communications Data Bill", 23.8.2012.

50 "Data Retention Effectively Changes the Behavior of Citizens in Germany" [www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/](http://www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/), 4.06.2008

51 Internet Policy Review, EU Data Retention Directive finally before European Court of Justice, <http://policyreview.info/articles/news/eu-data-retention-directive-finally-european-court-justice/162>

### 1.8 *Nécessité d'une protection renforcée des sources et des donneurs d'alerte*

Du fait des pratiques qui sapent de manière systématique la sécurité et le secret des communications, les canaux concernés ne sont plus dignes de confiance, ce qui a des effets dévastateurs à l'endroit de la liberté sur internet. En particulier, une valeur de base nécessaire à la réalisation de la liberté des médias – la protection des sources journalistiques, en ligne et hors ligne – est grandement menacée. En effet, l'Assemblée parlementaire a reconnu que « la protection des sources d'information des journalistes constitue une condition essentielle au libre exercice du journalisme et au respect du droit du public d'être informé des questions d'intérêt général, comme l'énonce la Cour européenne des droits de l'homme dans sa jurisprudence relative à l'article 10 de la Convention »<sup>52</sup>.

Après les révélations sur les pratiques de surveillance, il est devenu manifeste que les messages non cryptés transmis via internet sont hautement susceptibles d'être interceptés par quasiment tout service de renseignement du monde<sup>53</sup>. Et aussi, que le gouvernement des Etats-Unis d'Amérique a la volonté et les moyens d'utiliser les enregistrements téléphoniques et internet pour remonter les sources qui divulguent des secrets aux médias, y compris en ciblant des journalistes si nécessaire<sup>54</sup>.

Le journaliste du New York Times James Risen a affirmé dans un entretien que la surveillance exercée par le gouvernement sur les journalistes et les sources potentielles a rendu beaucoup plus difficile le journalisme d'investigation. Il souligne que cela a un effet paralysant sur les agents du gouvernement, qui ont désormais peur de parler aux journalistes<sup>55</sup>.

La protection des donneurs d'alerte est intimement liée à la celle des sources, et le Conseil de l'Europe a déjà accompli des progrès notables dans ce domaine, en particulier à travers le Comité européen de coopération juridique (CDCJ), dont le projet de recommandation sur la protection des donneurs d'alerte sera examiné pour adoption à la prochaine session plénière, et s'il est adopté, transmis au Comité des Ministres au début de 2014<sup>56</sup>. La Résolution 1729 (2010) de l'Assemblée parlementaire sur la protection des « donneurs d'alerte » souligne *« l'importance des "donneurs d'alerte" – toute personne soucieuse qui tire la sonnette d'alarme afin de faire cesser des agissements pouvant représenter un risque pour autrui – car ils permettent de renforcer la responsabilisation et de mieux lutter contre la corruption et la mauvaise gestion, dans le secteur tant public que privé. »* L'APCE invite les Etats à tenir compte du fait que « la législation relative aux donneurs d'alerte devrait chercher avant toute chose à offrir une alternative sûre au silence », et la capacité à garantir la confidentialité des communications est cruciale à cet égard.

---

<sup>52</sup> Assemblée parlementaire, Recommandation 1950 (2011) relative à la protection des sources d'information des journalistes, <http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta11/FREC1950.htm>

<sup>53</sup> Nieman Reports, "How to Keep Sources Secure from Surveillance"? 14.8.2013

<http://www.nieman.harvard.edu/reports/watchdogarticle/100021/How-to-Keep-Sources-Secure-from-Surveillance.aspx>,

<sup>54</sup> *Ibid.*

<sup>55</sup> *Ibid.*

<sup>56</sup> CDCJ(2013)Misc7 final, <http://www.coe.int/t/dghl/standardsetting/cdcj/2013/CDCJ%282013%29Misc7F.pdf>

Malgré ce constat, une culture d'intimidation prévaut dans le monde. Même si Edward Snowden, Glenn Greenwald, Laura Poitras et d'autres ont continué à publier des informations critiques mettant au jour les abus commis dans le cadre de la surveillance exercée par l'Etat, le harcèlement qu'eux-mêmes, leurs employeurs, leurs amis et des membres de leurs familles ont subi est susceptible d'avoir un effet paralysant non négligeable sur d'autres sources et donneurs d'alerte qui seraient tentés de dénoncer des violations des droits de l'homme<sup>57</sup>. En outre, dans cette ère de surveillance omniprésente, quel degré de confidentialité un journaliste peut-il vraiment promettre à une source ?

## Deuxième partie : Recommandations

Le Comité des Ministres et l'Assemblée parlementaire du Conseil de l'Europe ont adopté un certain nombre de déclarations, résolutions et recommandations importantes pour promouvoir la liberté sur internet. Pour faire face à ces défis, atténuer les conséquences futures sur les droits de l'homme et réaliser son agenda relatif à la liberté sur internet, le Conseil de l'Europe devrait prendre en considération ce qui suit :

### ***2.1 Saisir l'occasion de faire de la Convention n° 108 une norme internationale relative à la protection de la vie privée***

Le Conseil de l'Europe a reconnu que la protection de la vie privée et les données à caractère personnel sont indispensables sur internet<sup>58</sup> et devraient constituer une priorité pour les Etats membres. La Convention, premier instrument du genre, signé en 1981 et désormais ratifié par 46 pays, a servi de base solide pour la protection des données à caractère personnel dans l'environnement numérique. La décision d'offrir la possibilité d'adhésion à des Etats non membres du Conseil de l'Europe dans le cadre d'approches plus dynamiques et ouvertes est aussi à saluer, étant donné que la nécessité de développer des normes internationales harmonisées pour la protection des données à caractère personnel n'a jamais été aussi prononcée. Voici quelques recommandations pour le futur :

#### ***2.1.1 Renforcer le contrôle et la mise en œuvre de la Convention actualisée***

L'autorité compétente dans chaque pays signataire devrait désigner un point de contact unique dédié au contrôle et à la mise en œuvre de la Convention au niveau national. Les responsables en question devraient se réunir périodiquement, et peuvent jouer un rôle plus « pratique » en produisant des orientations communes sur des défis et questions spécifiques (par exemple, données volumineuses et données intelligentes). Ce groupe de travail devrait aussi se réunir périodiquement avec un éventail de parties intéressées, telles que des universitaires, représentants de la société civile, groupes de protection des consommateurs, spécialistes de technologies et industriels.

---

<sup>57</sup> The Guardian, "David Miranda, schedule 7 and the danger that all reporters now face,"

<http://www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters>

<sup>58</sup> Voir Stratégie du Conseil de l'Europe relative à la gouvernance de l'internet 2012-2015,

[http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/CoE\\_IGS\\_adopted\\_F.pdf](http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/CoE_IGS_adopted_F.pdf), point n° 10



### ***2.1.2 Comblent autant que possible les lacunes subsistant dans la Convention***

Afin que la Convention modernisée serve de référence en matière de protection des données à caractère personnel, il importe qu'elle comporte le moins de failles possible, sachant que l'efficacité de la Convention dépend de son maillon le plus faible. La Déclaration du Comité des Ministres du Conseil de l'Europe sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux va dans ce sens, lorsqu'elle « encourage les Etats membres à garder à l'esprit ces risques lors des discussions bilatérales avec des pays tiers ». Le Comité consultatif (T-PD) de la Convention n° 108 du Conseil de l'Europe devrait donc veiller à ce que la Convention ne soit pas affaiblie sur des points essentiels – par exemple, le seuil de transfert à des pays tiers – au nom de ce que certains Etats ont appelé une plus grande « interopérabilité » des systèmes de protection des données<sup>59</sup>. Pour assurer une harmonisation maximale et prévenir les failles, le texte devrait [au moins] rester conforme aux instruments existants, y compris la Directive européenne relative à la protection des données et le Règlement proposé.

### ***2.2 Renforcement du rôle des autorités de protection des données***

Conformément aux propositions visant à intégrer le protocole additionnel de la Convention dans la version actualisée de la Convention n° 108<sup>60</sup>, et compte tenu de la Déclaration sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux, il importe de veiller à l'indépendance des autorités compétentes et de s'assurer qu'elles sont dotées de ressources suffisantes pour faire face aux défis évoqués dans le présent document. En particulier, il est nécessaire que les autorités de protection des données agissent en dehors des structures du pouvoir exécutif des Etats membres, et il importe donc d'appuyer vigoureusement l'article 12bis(4) des propositions de modernisation. Par ailleurs, au niveau des Etats membres, il importe de mettre en œuvre – ou appuyer – la réglementation de sorte à renforcer la position des autorités compétentes en matière d'application effective de leur mandat, notamment sur le plan des sanctions administratives (comme à l'article 12bis 2(c)).

### ***2.3 Adoption et mise en œuvre des principes internationaux sur l'application des droits de l'homme à la surveillance des communications***

Les Principes internationaux sur l'application des droits de l'homme à la surveillance des communications élaborés par la société civile (ci-après « les Principes ») sont actuellement approuvés par 280 organisations dans le monde. Les Principes s'inspirent de nombreux traités ayant trait au droit international relatif aux droits de l'homme établissant le droit à la protection de la vie privée, et citent des éléments de jurisprudence régionale relatifs aux droits de l'homme tels que ceux de la Cour

---

<sup>59</sup> Greenleaf, Graham, 'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty? (May 8, 2013). (2013) Computer Law & Security Review, Vol 29, Issue 4; UNSW Law Research Paper No. 2013-33. Available at SSRN: <http://ssrn.com/abstract=2262296>

<sup>60</sup> Voir article 12bis relatif aux autorités de contrôle, T-PD(2012)04rev2, [http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD\\_documents/T-PD\\_2012\\_04\\_rev2\\_fr.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD_2012_04_rev2_fr.pdf)



européenne des droits de l'homme.<sup>61</sup> Le Conseil de l'Europe, à un niveau tant régional que national, devrait jouer un rôle de premier plan dans la promotion de la liberté sur internet à travers l'adoption et la mise en œuvre de ces Principes.

Le Programme européen de formation aux droits de l'homme pour les professionnels du droit (HELP) du Conseil de l'Europe accomplit déjà un travail de premier plan à l'échelle internationale dans la l'éducation et la sensibilisation des professionnels du droit aux nouveaux défis dans ce domaine. HELP devrait intégrer les Principes dans les futures rencontres, mesures de formation et activités diverses qui contribueront à élaborer des normes communes et à renforcer la coopération internationale indispensable en matière d'application du droit relatif aux droits de l'homme à la surveillance des communications.

## ***2.4 Instaurer une plus grande transparence***

Rappelant les engagements formulés dans la Convention du Conseil de l'Europe sur l'accès aux documents publics (STCE n° 205), qui s'inscrivent dans la suite des engagements en matière de gouvernance ouverte souscrits par plusieurs Etats membres du Conseil de l'Europe dans le cadre du Partenariat pour un gouvernement transparent (« Open Government Partnership »)<sup>62</sup>, et tenant compte des défis examinés dans le présent document en ce qui concerne le caractère secret de la surveillance des communications et ses conséquences corrosives sur les principes démocratiques, le Conseil de l'Europe devrait élargir son agenda relatif à la transparence pour inclure les rapports annuels accessibles au public sur les pratiques de surveillance par les Etats. Ces rapports devraient mentionner le nombre précis de demandes, les lois en vertu desquelles ces demandes sont émises, le nombre précis d'utilisateurs et dispositifs concernés ainsi que les autorités spécifiques qui formulent ces demandes. La Résolution de l'Assemblée parlementaire sur la sécurité nationale et l'accès à l'information<sup>63</sup> est instructive à cet égard. Elle encourage les Etats membres à signer et ratifier la Convention du Conseil de l'Europe sur l'accès aux documents publics et, en temps utile, à améliorer la Convention dans l'esprit des Principes globaux de la sécurité nationale et du droit à l'information, et/ou les instruments connexes, tels que les Principes internationaux sur l'application des droits de l'homme à la surveillance des communications (voir point 2.3). Pour renforcer la responsabilité et le contrôle, les Etats membres du Conseil de l'Europe devraient obliger les entreprises à publier les mêmes informations.

---

<sup>61</sup> 13 Principes internationaux.

<sup>62</sup> Open Government Partnership, Open Government Declaration, <http://www.opengovpartnership.org/open-government-declaration>

<sup>63</sup> Résolution 1954 (2013) Version provisoire, <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-FR.asp?fileid=20190&lang=FR>

## 2.5 Rétablir la confiance dans le secteur des entreprises

Le Conseil de l'Europe a déjà accompli des progrès conséquents dans le domaine des entreprises et des droits de l'homme, notamment à travers les « Lignes directrices visant à aider les fournisseurs de services internet »<sup>64</sup>, développées en 2008 en coopération avec l'Association européenne des fournisseurs de services internet (EuroISPA). Cependant, à la lumière des défis spécifiques évoqués dans ce document, il est évident que des orientations supplémentaires, allant au-delà de ce qui est déjà énoncé dans le texte précité et les Principes directeurs [des Nations Unies] relatifs aux entreprises et aux droits de l'homme, sont nécessaires.

Le Conseil de l'Europe et ses Etats membres devraient continuer à adopter des mesures proactives en vue d'élaborer des lignes directrices opportunes et sectorielles et/ou sous-sectorielles spécifiques sur la façon dont les entreprises peuvent s'acquitter de leurs obligations de respecter les droits de l'homme<sup>65</sup>. En particulier, les travaux du Groupe de rédaction sur les droits de l'homme et les entreprises (CDDH-CORP)<sup>66</sup> du Conseil de l'Europe devraient inclure des orientations sur les défis concernant la liberté sur internet.

Au niveau national, les Etats membres devraient aussi s'employer à répondre les défis mentionnés dans le présent document dans le cadre de l'élaboration de leur plan d'action national mettant en œuvre les Principes directeurs [des Nations Unies] relatifs aux entreprises et aux droits de l'homme<sup>67</sup>.

## 2.6 Promouvoir la culture numérique

Le Conseil de l'Europe a déjà reconnu dans sa stratégie relative à la gouvernance de l'internet la nécessité d'une « sensibilisation en milieu scolaire aux droits d'autrui à exercer sa liberté d'expression en se servant des médias sociaux en ligne et d'autres applications web »<sup>68</sup>. Cette ligne d'action peut et devrait être élargie à tout l'éventail des droits qui se rapportent à la liberté sur internet, en particulier la protection de la vie privée et la protection des données. L'éducation est nécessaire, dans le sens où elle donnerait aux étudiants les moyens d'exercer un plus grand contrôle sur leurs données à caractère personnel, faire des choix éclairés concernant leurs habitudes en ligne et être davantage informés des risques potentiels et de la manière dont ils peuvent se protéger.

---

64 Conseil de l'Europe, Lignes directrices visant à aider les fournisseurs de services internet, [http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf\(2008\)009\\_fr.pdf](http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_fr.pdf)

65 Commission européenne, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights [non disponible en français], [http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business\\_en.pdf](http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf), p. 9.

66 Conseil de l'Europe, La responsabilité sociale des entreprises dans le domaine des droits de l'homme, [http://www.coe.int/t/dghl/standardsetting/hrpolicy/other\\_committees/hr\\_and\\_business/default\\_FR.asp](http://www.coe.int/t/dghl/standardsetting/hrpolicy/other_committees/hr_and_business/default_FR.asp)

67 Institute for Human Rights and Business, "UK government prepares to launch National Action Plan on Business and Human Rights - Now the real work begins," <http://ihrb.org/commentary/staff/national-action-plan-on-business-and-human-rights.html>

68 Stratégie du Conseil de l'Europe relative à la gouvernance de l'internet 2012-2015, [http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/CoE\\_IGS\\_adopted\\_F.pdf](http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/CoE_IGS_adopted_F.pdf), point V.13.h

Dans cette optique, les Etats membres du Conseil de l'Europe devraient promouvoir l'utilisation d'outils libres (« open source ») destinés à renforcer la protection de la vie privée, et prévoir – dans le cadre de leur budget réservé à la liberté sur internet – des enveloppes financières spécifiques pour la conception, le développement et le déploiement de telles technologies. Par exemple, l'Agence suédoise de développement international finance le développement du projet Tor<sup>69</sup>.

## ***2.7 Renforcer les mesures de protection pour les donneurs d'alerte***

L'Assemblée parlementaire, dans sa Proposition de résolution sur Les opérations massives de surveillance en Europe a appelé l'ensemble des Etats membres du Conseil de l'Europe à « améliorer la protection contre toutes les formes de représailles à l'égard des donneurs d'alerte de bonne foi qui mettent au jour des abus dans l'intérêt public »<sup>70</sup>. Dans cette optique, le Conseil de l'Europe et ses Etats membres devraient sans délai renforcer les mesures de protection des donneurs d'alerte, afin de limiter tout effet paralysant sur les individus qui souhaiteraient révéler des violations des droits de l'homme dans le futur. Comme indiqué tantôt dans ce document, le travail du CDCJ est exemplaire à cet égard, et le (projet de) recommandation sur la protection des donneurs d'alerte<sup>71</sup> devrait être soutenu avec détermination par le Conseil de l'Europe et chacun de ses Etats membres. En effet, il faut absolument que les Etats membres créent un environnement sûr et favorable pour la démarche des donneurs d'alerte, sachant que, sans ces individus courageux, les violations des droits de l'homme ne seront probablement pas révélées dans bien de cas. Les donneurs d'alertes qui révèlent au grand jour les abus de gouvernements doivent souvent, et en particulier, passer le reste de leur vie dans la crainte de représailles, ce qui montre toute l'importance d'une politique forte et ouverte en matière d'asile à leur endroit.

Le Comité des droits de l'homme des Nations Unies, organe chargé d'assurer une interprétation officielle du Pacte international relatif aux droits civils et politiques (PIDCP), dans son Observation générale n° 31<sup>72</sup>, souligne que « (...) la jouissance des droits reconnus dans le Pacte, loin d'être limitée aux citoyens des États parties, doit être accordée aussi à tous les individus, quelle que soit leur nationalité ou même s'ils sont apatrides, par exemple demandeurs d'asile, réfugiés (...) » (paragraphe 10). Les Etats membres devraient réexaminer leur politique actuelle en matière de droit d'asile et s'assurer qu'elle est conforme à des normes internationales solides telles que celles énoncées dans l'Observation générale n° 31. A ce propos, il convient de constater les difficultés auxquelles Edward Snowden a été confronté lors de ses tentatives de demande d'asile<sup>73</sup>.

---

69 Voir Tor Sponsors, <https://www.torproject.org/about/sponsors.html.en>

70 Assemblée parlementaire, Proposition de résolution, Doc. 13288, 6 août 2013, « Les opérations massives de surveillance en Europe », <http://assembly.coe.int/ASP/XRef/X2H-DW-XSL.asp?fileid=20050&lang=FR>

71 CDCJ(2013)Misc7 final, <http://www.coe.int/t/dghl/standardsetting/cdcj/2013/CDCJ%282013%29Misc7F.pdf>

72 Nations Unies, « Observation générale n° 31 : La nature de l'obligation juridique générale imposée aux États parties au Pacte [80] : 05/26/2004. CCPR/C/21/Rev.1/Add.13. (General Comments) » [http://www.unhchr.ch/tbs/doc.nsf/\(Symbol\)/CCPR.C.21.Rev.1.Add.13.Fr](http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/CCPR.C.21.Rev.1.Add.13.Fr)

73 The BBC, "Fugitive Edward Snowden trapped in Russia - Putin," <http://www.bbc.co.uk/news/world-europe-23318475>

## Conclusion

Le Conseil de l'Europe est de longue date à la pointe de l'action pour les droits de l'homme, et, à ce titre, il serait opportun qu'il contribue aux efforts visant à élargir et renforcer les engagements en faveur de la liberté sur internet. Les révélations de ces derniers mois permettent de penser que la tâche ne sera pas facile. Et ce, d'autant plus que les enjeux sont de taille. En effet, la déclaration d'Edward Snowden à l'intention du Parlement européen est importante à cet égard : « (...) La surveillance de populations entières, plutôt que d'individus, risque d'être le plus grand défi de notre temps en termes de droits de l'homme. Le succès des économies dans les pays développés s'appuie de plus en plus sur leur créativité, et si ce succès doit continuer, nous devons nous rappeler que la créativité est le produit de la curiosité, qui à son tour est le produit de la vie privée. (...) »<sup>74</sup>

Les auteurs attendent avec grand intérêt de collaborer avec le Conseil de l'Europe et ses Etats membres en vue de faire avancer l'agenda relatif à la liberté sur internet et mettre en place des mesures de protection fortes et complètes, de sorte à faire respecter les droits de l'homme internationalement reconnus, notamment le droit à la vie privée, la protection des données à caractère personnel et l'équité procédurale.

\*\*\*

---

<sup>74</sup> Déclaration d'Edward Snowden à l'intention de la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen (3 octobre 2013), voir (en anglais) : <http://www.informationclearinghouse.info/article36412.htm>