Deux ans après Snowden : protéger les droits humains à l'ère de la surveillance de masse

Synthèse

« La vérité est incontestablement que l'utilisation de la technologie de surveillance de masse élimine en fait purement et simplement le droit au secret des communications sur l'Internet. »

Ben Emmerson**,** rapporteur spécial des Nations unies sur les droits de l'homme et la lutte antiterroriste

Le 5 juin 2013, le journal britannique *The Guardian* a rendu publiques de premières révélations sur la surveillance de masse non ciblée exercée par l'Agence nationale de sécurité américaine (NSA) et le service du renseignement du gouvernement britannique (GCHQ). Edward Snowden, lanceur d'alerte et ancien collaborateur de la NSA, a fourni des preuves qui attestent de l'existence de programmes de surveillance des communications mondiales. Ces programmes interceptent l'activité sur Internet et au téléphone de plusieurs centaines de millions de personnes à travers le monde.

Les États peuvent avoir des motifs légitimes de surveiller les communications, tels que la lutte contre la criminalité ou la protection de la sécurité nationale. Cependant, la surveillance portant atteinte à la vie privée et à la liberté d'expression, elle doit être exercée dans le respect de critères stricts : elle doit être ciblée, motivée par une suspicion raisonnable et appliquée conformément à la loi. Elle doit également être un moyen nécessaire et proportionné d'atteindre un objectif légitime, et respecter le principe de non-discrimination. Cela signifie que la surveillance de masse qui intercepte systématiquement les communications d'un grand nombre de personnes ne peut être justifiée. Cette pratique bafoue le droit de tout un chacun au respect de sa vie privée et à la liberté d'expression.

Ce document donne un aperçu des révélations qui ont été faites ces deux dernières années au sujet des programmes de surveillance de masse gérés par les États-Unis, le Royaume-Uni et d'autres États, et présente les principales évolutions juridiques, politiques et technologiques survenues pendant cette période dans le domaine de la surveillance de masse et du droit à la vie privée. Amnesty International et Privacy International exposent également dans ce document un plan d'action en sept points pour garantir la protection des droits humains à l'ère du numérique.

Ces deux dernières années, nous avons découvert l'ampleur des programmes de surveillance de masse menés en priorité par la NSA et le GCHQ, en coopération étroite avec leurs homologues australiens, canadiens et néo-zélandais, dans le cadre de l'alliance dite des « Cinq yeux ». Parmi les informations révélées au grand jour par les médias, à partir de fichiers transmis par Edward Snowden, figurent les points suivants :

- des entreprises, dont Facebook, Google et Microsoft, ont été contraintes de transmettre les données de leurs clients, en réponse à des ordonnances secrètes prises dans le cadre du programme Prism de la NSA ;
- la NSA a enregistré, stocké et analysé les métadonnées de tous les appels téléphoniques et SMS émis au Kenya, au Mexique et aux Philippines ;
- le GCHQ et la NSA ont fait appel aux services des plus grands opérateurs de télécommunications au monde pour placer sur écoute les câbles sous-marins transatlantiques et intercepter les communications privées qui y transitent, dans le cadre respectivement de leurs programmes TEMPORA et Upstream ;
- le GCHQ et la NSA ont piraté le réseau informatique interne de Gemalto, principal fabricant mondial de cartes SIM, et auraient dérobé plusieurs millions de clés de chiffrement servant à protéger la confidentialité des communications mobiles dans le monde entier.

Une opposition de plus en plus marquée de l'opinion publique a été observée à travers le monde. Un sondage réalisé, à la demande d'Amnesty International, auprès de 15 000 personnes dans 13 pays sur tous les continents, a révélé que 71 % des participants étaient fermement opposés à l'espionnage par leur gouvernement des communications par téléphone et sur Internet.

Des institutions et des experts aux échelons régional et international, dont le haut-commissaire aux droits de l'homme des Nations unies et l'Assemblée parlementaire du Conseil de l'Europe, ont fait part de la vive inquiétude que leur inspiraient les programmes de surveillance de masse, mettant en garde contre la menace qu'ils représentaient pour les droits humains. En décembre 2014, l'Assemblée générale des Nations unies a adopté une deuxième résolution sur le droit à la vie privée à l'ère du numérique, où elle s'est dite profondément préoccupée « par l'incidence néfaste que la surveillance ou l'interception des communications, [...] notamment à grande échelle, peuvent avoir sur l'exercice et la jouissance des droits de l'homme[1] ». En mars 2015, le Conseil des droits de l'homme des Nations unies a nommé pour la première fois un rapporteur spécial sur le droit à la vie privée, titulaire d'un mandat permanent. Cette décision historique permettra de veiller à ce qu'une attention prioritaire soit accordée par les Nations unies aux questions de confidentialité dans les années à venir.

Dans certains pays, la justice s'est prononcée contre des pratiques de surveillance de masse et de partage de renseignements. Au Royaume-Uni, en amont des décisions qu'il a rendues en décembre 2014 et février 2015, l'Investigatory Powers Tribunal (IPT), la juridiction chargée de juger les abus de pouvoirs en matière d'enquête, a estimé que les procédures mises en place par les autorités britanniques pour demander, recevoir, stocker et transmettre les communications privées de personnes situées au Royaume-Uni, qui ont été obtenues par les autorités américaines dans le cadre des programmes Prism et Upstream, étaient contraires à la Convention européenne des droits de l'homme. Aux États-Unis, une cour d'appel fédérale a estimé en mai 2015 que la collecte de données téléphoniques américaines à grande échelle était illégale.

Nombre de géants technologiques ont eux aussi dénoncé la surveillance de masse. En 2013, dix entreprises (dont Apple, Facebook, Google, Microsoft, Twitter et Yahoo!) ont lancé une coalition en faveur d'une réforme de l'appareil de surveillance gouvernemental pour demander, entre autres réformes juridiques, qu'il soit mis fin aux pratiques de collecte de masse autorisées par la Loi relative à la prévention du terrorisme (USA Patriot Act).

Plusieurs grandes entreprises ont pris des mesures plus concrètes pour déjouer les activités de surveillance, renforçant le niveau de sécurité et de chiffrement offert par défaut aux utilisateurs de leurs plateformes et services dans le but de mieux protéger les internautes contre la surveillance de masse non ciblée.

Quelques réformes juridiques limitées sont également à noter. Par exemple, une loi adoptée en mai par la Chambre des représentants, le USA Freedom Act, tente de mettre fin à la collecte de masse par les autorités de données téléphoniques aux États-Unis[2]. Cependant, ce texte exige également des entreprises qu'elles conservent, recherchent et analysent des données à la demande des autorités. Il est donc possible de considérer qu'il renforce le fondement juridique de la collecte de données sur une grande échelle au lieu d'y mettre fin. En outre, de nombreuses autres facettes de la surveillance exercée par les États-Unis restent peu encadrées et non contrôlées aux termes de cette nouvelle loi, notamment la surveillance de masse de millions de personnes hors du pays. Il faut faire pression pour que les États démantèlent ces systèmes de surveillance particulièrement intrusifs sur leur territoire comme à l'étranger. Pour cela, il convient de reconnaître dans un premier temps que toute personne, qu'elle soit à l'étranger ou dans son propre pays, a droit au respect de sa vie privée.

Les entreprises sont tenues de respecter le droit à la confidentialité sur Internet. À ce titre, elles doivent prendre des mesures bien plus audacieuses pour renforcer la sécurité de leurs plateformes et services de sorte que les gouvernements n'aient pas librement accès aux données privées des utilisateurs.

On assiste à une mobilisation croissante de l'opinion publique contre la surveillance de masse, mais ce n'est pas suffisant. Des États du monde entier ont promulgué de nouvelles lois leur accordant des pouvoirs de surveillance de masse. Cela a notamment été le cas cette année de la France et du Pakistan, qui jouissent désormais de vastes prérogatives dans ce domaine, tandis que le Danemark, les Pays-Bas, le Royaume-Uni et la Suisse devraient présenter très prochainement de nouveaux projets de loi sur le renseignement.

La protection de la vie privée et, en définitive, de la liberté d'expression, exige une action concertée de particuliers, de spécialistes des technologies, d'experts juridiques, de la société civile, d'organisations internationales, d'entreprises et de gouvernements. Une solution unique n'est pas suffisante. Il faut au contraire associer des réformes juridiques

---

[1] Résolution 68/167 de l'Assemblée générale des Nations unies, « Le droit à la vie privée à l'ère du numérique », A/RES/68/167, 21 janvier 2014, disponible sur http://www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167 (consulté le 28 mai 2015).

[2] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act of 2015), H.R. 2048, 114e session du Congrès (2015-2016).

nationales à des normes internationales solides, à des technologies sophistiquées de protection de la confidentialité, à un engagement des entreprises envers le respect de la vie privée des utilisateurs, ainsi qu'à une action individuelle.

Surveillance de masse des communications par téléphone et sur Internet : les informations obtenues sur les programmes menés par les États-Unis et le Royaume-Uni

Nous savons aujourd'hui, grâce aux révélations d'Edward Snowden, que les services du renseignement américains et britanniques gèrent des programmes de surveillance de masse non ciblée à l'échelle internationale, qui permettent d'intercepter une forte proportion du trafic Internet mondial ainsi que les communications téléphoniques de centaines de millions de personnes. Ces moyens d'interception sont associés à des pratiques généralisées de partage d'informations entre les membres de l'alliance dite des « Cinq yeux », ainsi qu'avec un réseau de services du renseignement situés dans plusieurs dizaines de pays à travers le monde[3]. Il s'agit là de certains des programmes de la NSA et du GCHQ qui ont été rendus publics depuis 2013.

Remarque sur les informations relatives aux pratiques de surveillance des États-Unis et du Royaume-Uni : la plupart des renseignements sur les pratiques de surveillance de masse des États-Unis et du Royaume-Uni disponibles dans le domaine public sont tirés de documents divulgués par le lanceur d'alerte et ancien analyste de la NSA, Edward Snowden. Parmi ces documents figuraient des fichiers internes de la NSA et du GCHQ. Des informations sur les activités de surveillance pratiquées par d'autres pays ont également été divulguées. Les révélations sur les pratiques de surveillance de masse ont été rendues publiques par différents organes de presse dans plusieurs pays.

Le gouvernement américain a confirmé l'existence de certains des programmes révélés au grand jour, à l'image du programme Prism. Toutefois, les renseignements divulgués n'ont été dans leur grande majorité ni confirmés, ni infirmés par les autorités américaines ou britanniques. En l'absence de démenti par les États-Unis ou le Royaume-Uni des informations contenues dans ces révélations, et comme l'authenticité des documents divulgués par Edward Snowden n'a été contestée par aucun de ces deux pays, on peut considérer que les renseignements sur les programmes de surveillance de masse qu'ils contiennent sont corrects.

[3] Pour en savoir plus, voir Privacy International, *The Five Eyes*, disponible sur www.privacyinternational.org/?q=node/51 (consulté le 28 mai 2015).

Les perspectives d'avenir

Deux ans après les révélations d'Edward Snowden, le vaste appareil de surveillance de masse géré par les services du renseignement américains et britanniques reste intact, et rien ne laisse présager une quelconque intention de la part de ces services de mettre fin au déploiement, voire à l'expansion, de leurs moyens.

Malgré les informations révélées au grand jour, les programmes de surveillance de masse des États-Unis et du Royaume-Uni restent entourés du plus grand secret, comme l'illustre la ligne de conduite suivie par le gouvernement britannique, qui consiste à ne pas confirmer ni infirmer ces informations. Face à cette politique, celles et ceux qui ont intenté des actions en justice contre les programmes de surveillance de masse du Royaume-Uni n'ont eu d'autre choix que de fonder leur argumentaire sur des scénarios hypothétiques. Ainsi, des programmes tels que TEMPORA, dont l'existence ne fait aucun doute d'après les documents communiqués par Edward Snowden, ne peuvent faire l'objet d'aucun examen approfondi.

Bien que les pratiques de surveillance de masse des États-Unis et du Royaume-Uni soient largement condamnées et considérées comme des violations des droits humains, et que certaines de ces pratiques aient été jugées illégales par des tribunaux américains et britanniques, personne n'a semble-t-il été tenu pour responsable de l'autorisation de ces programmes intrusifs.

Le message adressé par les États-Unis et le Royaume-Uni, ainsi que par leurs proches partenaires (l'Australie, le Canada et la Nouvelle-Zélande), est clair : ils ne renonceront pas facilement à leurs programmes de surveillance. En outre, au cours des deux années qui se sont écoulées depuis les révélations d'Edward Snowden, un nombre croissant de pays, dont l'Égypte[4], la France[5] et le Pakistan[6], ont cherché à renforcer leurs moyens de surveillance des communications.

Les menaces pesant sur la confidentialité en ligne ne cessent de croître, multipliant de fait les risques pour la liberté d'expression. On assiste toutefois à une mobilisation de plus en plus forte en réponse à ces menaces : des journalistes dévoilent des programmes de surveillance, la société civile conteste la surveillance de masse, des entreprises renforcent les fonctionnalités de protection de la confidentialité offertes dans leurs produits. Avant tout, depuis les révélations d'Edward Snowden, plusieurs centaines de millions d'internautes ont pris des mesures pour assurer le respect de leur vie privée sur Internet[7].

Ce militantisme est notre rempart contre les menaces de surveillance généralisée, où les États espionnent en permanence tous nos faits et gestes. Grâce aux progrès technologiques, les dispositifs de surveillance seront à terme moins onéreux et plus puissants ; nombre des moyens dont seuls la NSA et le GCHQ disposent aujourd'hui seront accessibles à la plupart des pays d'ici quelques années. La protection de la vie privée et, en définitive, de la liberté d'expression à l'ère du numérique exige une action sur plusieurs fronts : l'utilisation généralisée et non limitée d'outils sophistiqués de chiffrement et de préservation de l'anonymat ; des réformes juridiques et politiques à l'échelle nationale ; le respect des normes internationales ; et la protection des lanceurs d'alerte qui divulguent des informations d'intérêt public, telles que des preuves d'atteintes aux droits humains.

Le plan d'action en sept points présenté ci-dessous est destiné à la société civile, aux spécialistes des technologies, aux experts, aux entreprises et aux gouvernements qui souhaitent préserver les valeurs sur lesquelles a été fondé

---

[4] Voir Amnesty International, *Égypte. Le projet de surveillance des réseaux sociaux porte atteinte à la confidentialité sur Internet et à la liberté d'expression*, 4 juin 2014, disponible sur https://www.amnesty.org/fr/press-releases/2014/06/egypt-s-plan-mass-surveillance-social-media-attack-internet-privacy-and-fre/ et Mada Masr, *'You are being watched!' Egypt's mass Internet surveillance*, 29 septembre 2014, disponible sur http://www.madamasr.com/opinion/politics/you-are-being-watched-egypts-mass-internet-surveillance (deux articles consultés le 28 mai 2015).

[5] Voir Amnesty International, *France. Halte à la course à la surveillance*, 4 mai 2015, disponible sur https://www.amnesty.org/fr/articles/news/2015/05/france-surveillance-state/ et *France. Les députés approuvent la surveillance de masse*, 5 mai 2015, disponible sur www.amnesty.fr/Nos-campagnes/Liberte-expression/Actualites/France-les-deputes-approuvent-la-surveillance-de-masse-15061 (deux articles consultés le 28 mai 2015).

[6] Voir Privacy International, *International human rights organisations seriously concerned about the prevention of electronic crimes bill 2015 Pakistan*, 20 avril 2015, disponible sur www.privacyinternational.org/?q=node/566 (consulté le 28 mai 2015).

[7] Bill Schneier, *Over 700 Million People Taking Steps to Avoid NSA Surveillance*, 15 décembre 2014, disponible sur www.schneier.com/crypto-gram/archives/2014/1215.html#7 (consulté le 28 mai 2015).

Internet : la liberté, l'ouverture et l'accessibilité. Nous considérons ces mesures comme indispensables pour garantir la protection des droits humains à l'ère du numérique.

Réformes juridiques et politiques

1. Il faut réviser le droit national de façon à ce que les lois soient conformes au droit international relatif aux droits humains et aux normes internationales en la matière, et interdire en particulier la surveillance de masse non ciblée. Les grands principes à respecter incluent :
    a. s'assurer que la surveillance des communications ne puisse avoir lieu que de façon ciblée, en se basant sur suffisamment de preuves d'actes répréhensibles et avec l'autorisation d'une autorité strictement indépendante, comme celle d'un juge ;
    b. s'assurer de l'existence d'un contrôle judiciaire et parlementaire transparent et indépendant des pouvoirs de surveillance ;
    c. rendre publics tous les règlements et les politiques régissant les pratiques de surveillance, notamment en ce qui concerne le partage d'informations avec d'autres États ;
    d. veiller à ce que les ressortissants d'un pays, les étrangers, les personnes situées sur le territoire d'un État et celles à l'extérieur bénéficient tous du droit à l'égale protection de leur vie privée ;
    e. veiller à ce que le partage de renseignements soit strictement réglementé et conforme aux obligations relatives aux droits humains des États.
2. Les États ne doivent pas rendre illégales les technologies de chiffrement et de préservation de l'anonymat, ni l'utilisation de ces technologies.
3. Les lanceurs d'alerte, dont ceux qui travaillent sur des questions de sécurité nationale, doivent se voir offrir une solide protection juridique contre toute forme de représailles, en particulier contre les poursuites judiciaires qui pourraient être engagées à leur encontre parce qu'ils ont divulgué des informations d'intérêt public telles que des atteintes aux droits humains[8].

Diligence requise des entreprises
Conformément à l'obligation qu'ont les entreprises de respecter les droits humains :

4. Les entreprises qui sont propriétaires d'infrastructures de télécommunications ou Internet, y compris de câbles sous-marins, ou qui exploitent ce type d'infrastructures, ainsi que les entreprises du secteur Internet doivent veiller à ce que l'accès aux données ne soit autorisé que s'il respecte le droit international relatif aux droits humains et les normes internationales en la matière. Elles doivent notamment contester en justice les demandes d'accès global aux données relatives au trafic des communications qui leur sont envoyées par les autorités.
5. Les grandes entreprises des secteurs des télécommunications et d'Internet doivent prendre l'initiative d'utiliser de solides systèmes de chiffrement et d'autres technologies destinées à préserver la confidentialité, et de chiffrer par défaut toutes les données de bout en bout, dans toute la mesure du possible.
6. Les prestataires de services Internet, les opérateurs de télécommunications et les entreprises du secteur Internet doivent informer clairement les utilisateurs des obligations juridiques qu'elles sont tenues de respecter, en particulier de celles relatives à la communication d'informations ou de contenus appartenant aux utilisateurs.

Normes internationales

7. Il convient de procéder à une analyse plus approfondie des moyens et des mesures nécessaires à un meilleur respect des normes internationales relatives aux droits humains applicables à la surveillance des communications, en s'appuyant sur les initiatives d'identification des éléments pertinents qui ont vu le jour ces deux dernières années et parmi lesquelles figurent les rapports du rapporteur spécial sur la liberté d'expression[9], du haut-commissaire aux droits de l'homme des Nations unies, du rapporteur spécial sur la

[8] Voir les Principes globaux sur la sécurité nationale et le droit à l'information (Principes de Tschwane), disponibles sur http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-right-information-tshwane-principles/fr. Voir également la résolution 1954 (2013) de l'Assemblée parlementaire du Conseil de l'Europe, « La sécurité nationale et l'accès à l'information », disponible sur http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=20190&lang=fr (deux pages consultées le 28 mai 2015), où l'Assemblée parlementaire s'est félicitée de l'adoption des Principes de Tschwane.

[9] Conseil des droits de l'homme des Nations unies, rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, A/HRC/23/40, 17 avril 2013, disponible sur

promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste[10], ainsi que des travaux de la société civile tels que les Principes internationaux sur l'application des droits de l'homme à la surveillance des communications[11].

www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (en anglais, consulté le 28 mai 2015).

[10] Assemblée générale des Nations unies, rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, A/69/397, 23 septembre 2014, disponible sur http://www.un.org/ga/search/view_doc.asp?symbol=A/69/397&Lang=F (consulté le 28 mai 2015).

[11] Principes internationaux sur l'application des droits de l'homme à la surveillance des communications, mai 2014, disponible sur https://fr.necessaryandproportionate.org/content/principes-internationaux-sur-l%E2%80%99application-des-droits-de-l%E2%80%99homme-%C3%A0-la-surveillance-des (consulté le 28 mai 2015).