NÉCESSAIRES ET PROPORTIONNÉS

PRINCIPES INTERNATIONAUX SUR L'APPLICATION DES DROITS DE L'HOMME À LA SURVEILLANCE DES COMMUNICATIONS

Crédits

Les Principes Internationaux sur l'Application des Droits de l'Homme à la Surveillance des Communications ont été rédigés de manière conjointe par des organisations privées et des experts du monde entier comprenant, sans s'y limiter, à, Access, Article 19, L'Association Civile pour l'Égalité et la Justice, l'Association pour les Droits Civils, l'Association pour la Communication Progressive, Bits of Freedom (Soupçons de Liberté), Center for Internet & Society India (Centre pour Internet et la Société — Inde), la Commission Colombienne des Juristes, la Fondation Frontières Électroniques, le Droits Digitaux Européens, Reporters Sans Frontières, la Fondation Karisma, Open Net Korea (Réseau Ouvert Corée), Open Rights Group (le Groupe pour la Transparence des Droits) , Privacy International, et la Clinique d'Intérêt Public et de Politique d'Internet du Canada Samuelson-Glushko. En outre, nous souhaitons également remercier IP Justice, SHARE Foundation — SHARE Defense, le Réseau IFEX et l'Institut NUPEF afin d'avoir aidé les groupes concernés à se mettre en contact.

Pour plus d'informations, visitez

necessaryandproportionate.org/text

Histoire Générale

Plus de 40 experts en matière de vie privée et de sécurité ont participé à la procédure d'élaboration des Principes au cours de la réunion de Bruxelles au mois d'octobre 2012. Suite à une consultation initiale et globale, au cours de laquelle se tint une deuxième réunion à Rio de Janeiro en décembre 2012, Access, EFF et Privacy International dirigèrent une procédure d'élaboration de manière conjointe qui attira les experts en matière de droits de l'homme et droits digitaux du monde entier. La première version des Principes fut achevée le 10 juillet 2013 et officiellement lancée lors du Conseil des Droits de l'Homme des Nations Unies à Genève, en septembre 2013. Le franc succès et l'adoption globale des Principes par plus de 400 organisations de par le monde avait besoin d'un nombre spécifique, principalement superficielles, de modifications textuelles aux termes des Principes afin de garantir leur interprétation et leur application cohérentes en fonction des ressorts. De mars à mai 2013, une autre consultation fut dirigée afin de déterminer et de rectifier ces problèmes textuels, et d'actualiser les Principes en conséquence. Les effets et l'intention des Principes n'ont pas été altérés par ces modifications. Cette version est le résultat final de ces procédures et la version des Principes faisant autorité.

VERSION FINALE, MAI 2014*

Tandis que les technologies qui facilitent la surveillance étatique des communications progressent, les États ne réussissent pas à garantir que les lois, réglementations, activités, pouvoirs et autorités associés à la Surveillance des Communications adhèrent à la loi et aux normes internationales relatives aux droits de l'homme. Ce document tâche d'éclaircir la manière dont la loi internationale sur les droits de l'homme s'applique à l'environnement digital actuel, en particulier, à la lumière de l'accroissement et des modifications des technologies et des techniques en matière de Surveillance des Communications. Ces principes peuvent doter les groupes de la société civile, l'industrie, les états et autres d'un cadre leur permettant d'évaluer si les lois et les pratiques actuelles ou proposées, relatives à la surveillance, sont cohérentes avec les droits de l'homme.

Ces principes sont le résultat d'une consultation globale auprès des groupes de la société civile, l'industrie et les experts internationaux en matière de lois, politiques et technologies relatives à la Surveillance des Communications.

INTRODUCTION

La vie privée est un droit fondamental et est essentiel à la préservation des sociétés démocratiques. Il est essentiel à la dignité humaine et renforce ses autres droits, tels que la liberté d'expression et le droit à l'information, à la liberté d'association, et est reconnu conformément à la loi internationale sur les droits de l'homme.[1] La Surveillance des Communications interfère avec le droit à l'intimité parmi un certain nombre d'autres droits de l'homme. En conséquence, il ne peut être justifié que si ordonné par la loi, nécessaire à atteindre un objectif légitime, et proportionné à l'objectif poursuivi.[2]

Avant l'adoption publique d'Internet, les principes juridiques bien établis et les fardeaux logistiques inhérents au contrôle des communications créèrent des limites à la Surveillance des Communications par les États. Au cours des décades récentes, ces barrières logistiques à la surveillance ont diminué et l'application des principes juridiques aux nouveaux contextes technologiques est devenue peu claire. L'explosion du contenu des communications digitales et – les informations relatives aux communications personnelles ou utilisation de

dispositifs électroniques – le coût en baisse du stockage et de l'exploitation de grands ensembles de données, ainsi que la fourniture de contenu personnelle par le biais de prestataires de services tiers, rendent possible la Surveillance des Communications par les États à une échelle sans précédents.[3] En attendant, la conceptualisation de la loi existante sur les droits de l'homme n'a pas suivi les technologies et techniques étatiques, modernes et en évolution, de la Surveillance des Communications, ni la capacité de l'État de combiner et d'organiser les informations provenant des différentes technologies et techniques de surveillance, ni la sensibilité accrue des informations auxquelles il est aisé d'avoir accès.

La fréquence avec laquelle les États cherchent à avoir accès à la fois au contenu des communications et aux métadonnées s'accroît de manière spectaculaire, sans surveillance appropriée.[4] Les métadonnées en matière de communications peuvent créer le profil d'une vie personnelle comprenant l'historique médical, les points de vue politiques et religieux, les associations, interactions et intérêts, en les divulguant assez en détail, voire de manière trop détaillée de ce qui devrait ressortir du contenu des communications.[5] Malgré le vaste potentiel intrusif dans la vie d'une personne et les effets effrayants qui s'en dérivent, la politique et autres associations, lois, réglementations, activités, pouvoirs, ou autorités permettent que le niveau de protection des métadonnées en matière de communications soit des moins élevés et ne restreignent pas suffisamment la manière dont elles peuvent être utilisées par les États en conséquence.

PORTÉE D'APPLICATION

Les Principes et l'Introduction sont holistiques et autoréférentiels – chaque principe, ainsi que l'introduction, doivent se lire et s'interpréter comme une partie d'un cadre beaucoup plus ample qui, ensemble, atteignent un but particulier : garantir que les lois, politiques et pratiques relatives à la Surveillance des Communications adhèrent aux lois et normes internationales sur les droits de l'homme et protègent de manière adéquate les droits individuels de l'homme, tels que l'intimité et la liberté d'expression. Ainsi, de manière à ce que les États exécutent leurs obligations internationales en matière de droits de l'homme, associées à la Surveillance des Communications, ils doivent respecter chacun des principes stipulés ci-après.

Ces principes s'appliquent à la surveillance dirigée à l'intérieur d'un État ou hors de son territoire. Les principes s'appliquent également indépendamment de l'objectif de la surveillance — comprenant l'application de la loi, la protection de la sécurité nationale, l'espionnage ou autre fonction gouvernementale. Ils s'appliquent aussi à la fois aux obligations de l'État de respecter et d'honorer les droits individuels de l'homme, ainsi qu'à l'obligation de protéger les droits individuels de l'homme face aux abus d'acteurs non-étatiques, en ce compris les entreprises commerciales.[6] Les entreprises commerciales ont la responsabilité de respecter l'intimité individuelle et autres droits de l'homme, en particulier étant donné le rôle clé qu'elles jouent au moment de concevoir, développer et disséminer les technologies ; de permettre et de fournir les communications ; et de faciliter certaines activités de surveillance de l'État. Néanmoins, ces Principes articulent les devoirs et les obligations des États lorsqu'ils entreprennent une Surveillance des Communications.

TECHNOLOGIE ET DÉFINITIONS EN ÉVOLUTION

"La surveillance des communications" au sein de l'environnement moderne embrasse le contrôle, l'interception, le recueil, l'obtention, l'analyse, l'utilisation, la conservation, la rétention, l'interférence avec, l'accès ou toute action similaire entreprise eu égard des informations qui comprennent, reflètent, dérivent de ou concernent les communications d'une personne dans le passé, le présent ou l'avenir.

Les "communications" comprennent les activités, interactions et transactions transmises par le biais de moyens électroniques, tels que le contenu des communications, l'identité des parties en communication, repérage de l'emplacement, information comprenant des adresses IP, l'heure et la durée des communications, ainsi que les identifiants des équipements de communication utilisé au cours desdites communications.

Les "Informations Protégées" sont des informations qui comprennent, reflètent, dérivent de ou concernent les communications d'une personne qui ne sont pas facilement disponibles ni aisément accessibles au public en général. Traditionnellement, la nature invasive de la Surveillance des Communications a été évaluée sur la base de catégories artificielles et formalistes. Les cadres juridiques existants font la distinction entre le "contenu" ou "le non-contenu", "les

informations relatives au souscripteur" ou "métadonnées," données stockées ou en transit, données détenues à la maison ou en possession d'un prestataire de services tiers.[7] Néanmoins, ces distinctions ne sont plus appropriées afin de mesurer le degré d'intrusion de la Surveillance des Communications dans la vie privée des personnes et associations. Alors qu'il a été longtemps convenu que le contenu des communications mérite une protection juridique significative, en raison de sa capacité à révéler des informations sensibles, il est maintenant devenu clair que d'autres informations dérivées des communications – métadonnées et autres formes de données sans contenu – peuvent en révéler beaucoup plus sur une personne que le contenu en soi, et méritent ainsi une protection équivalente. De nos jours, chacun de ces types d'information peut, analysé de manière individuelle ou collective, révéler l'identité d'une personne, son comportement, ses associations, son historique physique ou médical, sa race, sa couleur, son orientation sexuelle, ses origines nationales ou ses points de vue ; ou permettre la cartographie de l'emplacement de cette personne, ses mouvements et interactions au fil du temps,[8] ou de toutes les personnes à un emplacement donné, voire lors d'une démonstration publique ou autre évènement politique. En conséquence, toutes les Informations Protégées devraient bénéficier de la protection juridique la plus élevée.

Lors de l'évaluation de la nature invasive de la Surveillance Étatique des Communications, il est nécessaire de prendre en considération à la fois le potentiel de la surveillance aux effets de révéler les Informations Protégées, ainsi que le but dans lequel l'État recherche ces informations. Toute Surveillance des Communications interfère avec les droits de l'homme donc, la loi internationale sur les droits de l'homme s'applique. La Surveillance des Communications qui conduira probablement à la divulgation des Informations Protégées, mettant ainsi une personne en danger d'être enquêtée, de discrimination, ou de violation des droits de l'homme constituera une grave violation du droit de la personne à l'intimité, ainsi que minera la jouissance d'autres droits fondamentaux, comprenant le droit à la libre expression, association et participation politique. Ceci se doit au fait que ces droits requièrent des personnes de pouvoir communiquer à l'abri des conséquences effrayantes de la surveillance gouvernementale. Une détermination, à la fois du caractère et des utilisations potentielles des informations recherchées, sera donc nécessaire dans chaque cas particulier.

NÉCESSAIRES ET PROPORTIONNÉS

Lors de l'adoption d'une nouvelle technique de Surveillance des Communications ou de l'expansion de la portée d'une technique existante, l'État doit vérifier si les informations à fournir sont du domaine des Informations Protégées avant d'initier la recherche, et doit se soumettre à une surveillance judiciaire ou autre mécanisme démocratique de supervision. Lors de la prise en considération du fait que les informations obtenues au moyen de la Surveillance des Communications puissent relever du domaine des Informations Protégées, la forme, ainsi que la portée et la durée de la surveillance sont des facteurs pertinents. Parce que le contrôle envahissant ou systématique, ou les techniques invasives utilisées afin d'effectuer la Surveillance des Communications ont la capacité de révéler des informations privées qui excèdent leurs composantes, la surveillance des informations non-protégées peut atteindre un niveau invasif requérant la pleine protection, comme dans le cas des Informations Protégées.[9]

La détermination de la manière dont l'État doit diriger la Surveillance des Communications eu égard aux Informations Protégées doit être conforme aux principes suivants.

LES 13 PRINCIPES

LES 13 PRINCIPES

Légalité

Toute restriction portée aux droits de l'homme doit être ordonnée par la loi. L'État ne doit pas adopter ni mettre en œuvre de mesures interférant avec ces droits en l'absence d'une loi existante et publiquement disponible, qui soit conforme à un standard de clarté et de précision suffisant à garantir que les personnes en ont connaissance à l'avance et peuvent anticiper son application. Étant donné le taux des modifications technologiques, les lois restreignant les droits de l'homme devraient être soumises à une révision périodique au moyen d'une procédure législative participative ou réglementaire.

Objectif Légitime

Les lois devraient exclusivement permettre la Surveillance des Communications par des autorités étatiques spécifiées et afin d'atteindre un objectif qui soit légitime et corresponde à un intérêt juridique principalement important, nécessaire dans une société démocratique. Les mesures ne doivent pas être appliquées de manière à discriminer sur le fondement de la race, la couleur, le sexe, la langue, la religion, les opinions politiques ou autres, l'origine nationale ou sociale, la propriété, la naissance ou autre statut.

Nécessité

Les lois, réglementations, activités, pouvoirs ou autorités en matière de surveillance doivent être limités à ceux qui sont strictement et manifestement nécessaires à atteindre un objectif légitime. La Surveillance des Communications doit seulement être dirigée lorsqu'il s'agit du seul moyen d'atteindre un objectif légitime, ou, en cas de multiples moyens, de celui qui soit le moins propice à violer les droits de l'homme. L'État est toujours responsable d'établir cette justification.

Adéquation

Tous les cas de Surveillance des Communications autorisés par la loi doivent être appropriés à accomplir l'Objectif Légitime spécifique identifié.

Proportionnalité

La Surveillance des Communications doit être considérée comme une intervention hautement intrusive qui interfère avec les droits de l'homme, menaçant les piliers d'une société démocratique. Les décisions en matière de Surveillance des Communications doivent tenir compte de la sensibilité des informations auxquelles elles ont accès et la gravité de la violation des droits de l'homme et autres intérêts en lice.

Ceci requiert de l'État, au minimum, de justifier ce qui suit auprès d'une Autorité Judiciaire Compétente, préalablement à la direction d'une Surveillance des Communications dans le but d'appliquer la loi, de protéger la sécurité nationale ou dans les cas d'espionnage :

1. il existe une forte probabilité qu'un grave crime soit perpétré ou une menace spécifique soit proférée eu égard à un Objectif Légitime, et ;

2. il existe une forte probabilité que la preuve pertinente et matérielle de ce grave crime ou menace spécifique eu égard à un Objectif Légitime soit obtenue en accédant à des Informations Protégées, et ;

3. d'autres techniques moins invasives ont été épuisées ou seraient futiles, de manière que les techniques utilisées sont l'option la moins invasive, et ;

4. l'accès aux informations sera limité à ce qui est pertinent et matériel au grave crime ou à la menace spécifique alléguée eu égard à l'Objectif Légitime, et ;

5. toute information recueillie en excès ne sera pas retenue, mais rapidement détruite ou renvoyée, et ;

6. seules les autorités spécifiées auront accès aux informations, lesquelles seront utilisées dans le seul but et dans les délais pour lesquels l'autorisation a été donnée, et ;

7. que les activités de surveillance requises et les techniques proposées ne minent pas l'essence du droit à l'intimité ou aux libertés fondamentales.

Autorité Judiciaire Compétente

Les déterminations relatives à la Surveillance des Communications doivent être effectuées par une autorité judiciaire compétente qui soit impartiale et indépendante. Cette autorité doit :

1. être distincte et indépendante des autorités qui dirigent la Surveillance des Communications, et ;

2. maîtriser parfaitement les questions associées et compétente afin de rendre des décisions judiciaires en matière de légalité de la Surveillance des Communications, des technologies utilisées et des droits de l'homme, et ;

3. disposer des ressources adéquates aux effets de l'exercice des fonctions qui lui ont été assignées.

Procédure Équitable

La procédure équitable requiert que l'État respecte et garantisse les droits individuels de l'homme en garantissant que les procédures légitimes régissant les interférences avec les droits de l'homme sont correctement énumérées par la loi, mises en pratique de manière cohérente et disponibles au public en général. En particulier, lors de la détermination des droits de l'homme, toute personne a droit à une audience juste et publique dans un délai raisonnable au-devant d'un tribunal indépendant, compétent et impartial établi par la loi,[10] sous réserve des cas urgents où il existe un danger imminent pour la vie humaine. Dans de tels cas, une autorisation rétroactive est nécessaire dans un délai raisonnablement réalisable. Le simple risque de vol ou destruction des preuves ne doit jamais être considéré comme suffisant aux effets de justifier une autorisation rétroactive.

Notification de l'Utilisateur

Les personnes dont les communications sont surveillées doivent être notifiées de la décision autorisant la Surveillance des Communications suffisamment à l'avance et avec toutes les informations nécessaires à leur permettre de remettre en cause la décision ou de chercher d'autres recours, et doivent avoir accès aux matériels présentés à l'appui de l'application de l'autorisation. Tout retard eu égard à cette notification ne peut se justifier que dans les circonstances suivantes :

1. La notification compromettrait gravement le but pour lequel la Surveillance des Communications a été autorisée, ou il existe un danger imminent pour la vie humaine, et ;

2. L'autorisation de retarder la notification a été octroyée par une Autorité Judiciaire Compétente, et ;

3. L'utilisateur affecté est notifié dès que le risque est soulevé, tel que déterminé par une Autorité Judiciaire Compétente.

L'obligation de notifier repose sur l'État, mais les prestataires de services en matière de communications devraient être libres de notifier les personnes de la Surveillance de ses Communications, de manière volontaire ou sur demande.

Transparence

Les états devraient être transparents quant à l'utilisation et la portée des lois, réglementations, activités, pouvoirs ou autorités relatives à la Surveillance des Communications. Il devraient publier, au minimum, des informations globales sur le nombre spécifique de demandes approuvées et refusées, une déségrégation des demandes par prestataire de services et autorité d'enquête, ainsi que type et objectif, et le nombre spécifique de personnes affectés par chacune. Les états devraient fournir aux personnes les informations suffisantes à leur permettre de pleinement comprendre la portée, nature et application des lois permettant la Surveillance des Communications. Les États ne devraient pas interférer avec les prestataires de services dans leur effort afin de publier les procédures qu'ils appliquent lorsqu'ils évaluent et exécutent les demandes

de l'État en matière de Surveillance des Communications, adhérer à ces procédures, et publier les résultats des demandes de l'État en matière de Surveillance des Communications.

Supervision Publique

Les États devraient établir des mécanismes de supervision indépendants afin de garantir la transparence et la responsabilité de la Surveillance des Communications.[11] Les mécanismes de supervision devraient pouvoir : avoir accès à toutes les informations potentiellement pertinentes sur les interventions de l'État, comprenant, si approprié, accès aux informations secrètes ou classées ; évaluer si l'État fait une utilisation légitime de ses capacités légales ; évaluer si l'État a publié de manière exhaustive et précise les informations relatives à l'utilisation et la portée des techniques et pouvoirs en matière de surveillance des Communications, conformément à ses obligations de Transparence; publier des rapports périodiques et autres informations pertinentes en matière de Surveillance des Communications; et de rendre publiques les déterminations relatives à la légitimité de ces actions, en ce compris la mesure dans laquelle elles sont conformes aux présents Principes. Des mécanismes de supervision indépendants devraient être établis en sus de la supervision déjà fournie par une autre agence du gouvernement.

Intégrité des Communications et des Systèmes

Afin de garantir l'intégrité, la sécurité et la confidentialité des systèmes de communication, et en reconnaissance du fait qu'une sécurité compromettant les objectifs de l'État compromet presque toujours la sécurité de manière plus générale, les États ne devraient pas contraindre les prestataires de services ou les vendeurs de matériel informatique ou de logiciels de construire des capacités de surveillance ou de contrôle dans leurs systèmes, ou de recueillir ou retenir des informations particulières exclusivement aux effets de la Surveillance des Communications par l'État. A priori, la rétention ou le recueil des données ne devrait jamais être requis des prestataires de services. Les personnes ont le droit de s'exprimer de manière anonyme ; les États devraient, en conséquence, s'abstenir d'obliger les utilisateurs à s'identifier.[12]

Sauvegardes en matière de Coopération Internationale

En réponse aux changements des flux d'informations, et des technologies et services de communication, les États peuvent avoir besoin d'assistance provenant de prestataires de services et États étrangers. En conséquence, les traits sur l'assistance légale mutuelle (MLATs) et autres accords passés entre les États devraient garantir que, lorsque les lois de plus d'un état sont applicables à la Surveillance des Communications, la norme disponible possédant le niveau le plus élevé en matière de protection des personnes doit s'appliquer. Si les États ont besoin d'assistance dans un but d'application de la loi, le principe de la double criminalité devrait s'appliquer. Les États ne doivent pas utiliser les procédures d'assistance légale mutuelle et demandes d'Informations Protégées étrangères afin de contourner les restrictions juridiques nationales sur la Surveillance des Communications. Les procédures d'assistance légale mutuelle et autres accords devraient être clairement documentés, publiquement disponibles, et soumis aux garanties de l'équité procédurale.

Sauvegardes Contre l'Accès Illégitime

Les États devraient promulguer une législation punissant la Surveillance des Communications illégale, que les acteurs soient publics ou privés. La loi doit mettre à disposition des pénalisations civiles et criminelles, suffisantes et significatives, des protections pour les informateurs, et des possibilités de réparation pour les personnes affectées. Les lois devraient stipuler que toute information obtenue de manière incohérente avec les présents Principes est inadmissible en tant que preuve ou autrement inadmissible au cours de toute procédure, ainsi que toute preuve dérivée de ces informations. Les États devraient également promulguer des lois stipulant qu'une fois le matériel obtenu au moyen de la Surveillance des Communications a été utilisé dans le but pour lequel ces informations ont été fournies, ledit matériel ne doit pas être retenu, sinon détruit ou renvoyé aux personnes affectées.

* Plus de 40 experts en matière de vie privée et de sécurité ont participé à la procédure d'élaboration des Principes au cours de la réunion de Bruxelles au mois d'octobre 2012. Suite à une consultation initiale et globale, au cours de laquelle se tint une deuxième réunion à Rio de Janeiro en décembre 2012, Access, EFF et Privacy International dirigèrent une procédure d'élaboration de manière conjointe qui attira les experts en matière de droits de l'homme et droits digitaux du monde entier. La première version des Principes fut achevée le 10 juillet 2013 et officiellement lancée lors du Conseil des Droits de l'Homme des Nations Unies à Genève, en septembre 2013. Le franc succès et l'adoption globale des Principes par plus de 400 organisations de par le monde avait besoin d'un nombre spécifique, principalement superficielles, de modifications textuelles aux termes des Principes afin de garantir leur interprétation et leur application cohérentes en fonction des ressorts. De mars à mai 2013, une autre consultation fut dirigée afin de déterminer et de rectifier ces problèmes textuels, et d'actualiser les Principes en conséquence. Les effets et l'intention des Principes n'ont pas été altérés par ces modifications. Cette version est le résultat final de ces procédures et la version des Principes faisant autorité.

NOTES DE FIN

1 Article 12 de la Déclaration Universelle des Droits de l'Homme, Article 14 de la Convention des Nations Unies sur les Travailleurs Itinérants, Article 16 de la Convention des Nations Unies sur la Protection Infantile, Convention Internationale sur les Droits Civils et Politiques, Article 17 de la Convention Internationale sur les Droits Civils et Politiques, conventions régionales comprenant l'Article 10 de la Charte Africaine sur les Droits et le Bien-Être Infantiles, Article 11 de la Convention Américaine sur les Droits de l'Homme, Article 4 des Principes de l'Union Africaine sur la Liberté d'Expression, Article 5 de la Déclaration Américaine sur les Droits et les Obligations de l'Homme, Article 21 de la Charte Arabe sur les Droits de l'Homme, Article 21 de la Déclaration des Droits de l'Homme de l'ANASE, Article 8 de la Convention Européenne pour la Protection des Droits de l'Homme et des Libertés Fondamentales, Principes de Johannesburg sur la Sécurité Nationale, la Libre Expression et l'Accès aux Informations, Principes de Camden sur la Liberté d'Expression et l'Égalité.

2 Article 29 de la Déclaration des Droits de l'Homme, Commentaire Général Nº 27 Adopté par le Comité des droits de l'Homme à l'Article 40, Paragraphe 4, de la Convention Internationale sur les droits Civils et Politiques, CCPR/C/21/Rév.1/Add.9, 2 novembre 1999; cf. également Martin Scheinin, "Rapport du Rapporteur Spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales face au terrorisme," 2009, A/HRC/17/34. Cf. également Frank La Rue, "Rapport du Rapporteur Spécial au Conseil des Droits de l'Homme relatif aux implications de la surveillance des communications par un État sur l'exercice des droits de l'homme à l'intimité et à la liberté d'opinion et d'expression," 2013, A.HRC.23.40 EN.

3 Les métadonnées en matière de communications peuvent comprendre des informations concernant nos identités (informations sur le souscripteur et les dispositifs), interactions (origines et destinations des communications, en particulier celles exposant des sites Web visités, des livres et autres matériels lus, les personnes avec lesquelles nous interagissons, amis, famille, connaissances, recherches dirigées, ressources utilisées), et emplacement (lieux et heures, proximité aux autres); en résumé, les métadonnées fournissent une fenêtre sur toute intervention dans le cadre de la vie moderne, nos états mentaux, intérêts, intentions et nos pensées les plus intimes.

4 Par exemple, au Royaume-Uni seulement, il existe environ 500.000 demandes de métadonnées en matière de communications tous les ans, actuellement sous un régime autorisant automatiquement les agences responsables d'appliquer la loi d'autoriser leurs propres demandes afin d'avoir accès aux informations détenues par les prestataires de services. En attendant, les données fournies par les rapports de Transparence de Google montrent que les demandes de données d'utilisateurs provenant seulement des États-Unis sont passées de 8.888 en 2010 à 12.271 en 2011. En Corée, il existe environ 6 millions de demandes d'information sur les souscripteurs/intervenants chaque année, et environ 30 millions de demandes d'autres formes de métadonnées en matière de communications chaque année en 2011-2012, dont la plupart ont été octroyées et exécutées. Les données 2012 sont disponibles sur **http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586**

5 Cf. à titre d'exemples, une critique du travail de Sandy Petland, 'Reality Mining (Exploitation de la Réalité)', dans la Revue Technologique du MIT, 2008, disponible sur http://www2.technologyreview.com/article/409598/tr10-reality-mining/ et également Alberto Escudero-Pascual et Gus Hosein, 'Questioning lawful access to traffic data (Remise en question de la légitimité de l'accès aux données de trafic)', *Communications de l'ACM*, Volume 47 Édition 3, mars 2004, pages 77 - 82.

6 Rapport du Rapporteur Spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, 16 mai 2011, disponible sur **http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf**

7 "Les personnes divulguent les numéros de téléphone qu'elles composent ou envoient à leurs fournisseurs de téléphones portables, les URLS qu'elles visitant et les adresses e-mail correspondant à leurs fournisseurs de services Internet, et les livres, provisions et médicaments qu'elles achètent en ligne aux détaillants . . . Je ne partirai pas du principe selon lequel toute l'information volontairement divulguée à un membre du public dans un but limité, est, pour ce seul motif, dépourvu de la protection du Quatrième Amendement." *United States v. Jones, 565 U.S. ____, 132 S. Ct. 945, 957 (2012)* (Sotomayor, J., avis concordant).

8 "Le contrôle à court terme des mouvements d'une personne dans les rues publiques avec des attentes en matière d'intimité est conforme" mais "le contrôle à long terme moyennant GPS lors d'enquêtes criminelles empiète sur les attentes en matière d'intimité." United States v. Jones, 565 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J. avis concordant).

9 "La surveillance prolongée révèle des types d'information non divulgués au moyen d'une surveillance à court terme, tels que ce qu'une personne fait de manière répétée, ce qu'elle ne fait pas, et ce qu'elle fait dans l'ensemble. Ces types d'information peuvent en révéler plus sur une personne que toute visite individuelle examinée de manière isolée. Les visites répétées à l'église, au gymnase, au bar, ou au bookmaker racontent une histoire qu'aucune visite simple visite pourrait raconter, ainsi que l'absence de visites de ces endroits pendant un mois. La séquence des mouvements d'une personne peuvent en révéler encore plus ; une simple visite au gynécologue en dit peu sur une femme, mais cette visite, suivie d'une autre visite quelques semaines plus tard à un magasin pour bébés raconte une histoire différente.* Une personne qui en sait tout sur les visites d'une autre peut déduire s'il va à l'église toutes les semaines, est un gros buveur, se rend régulièrement au gymnase, est un mari infidèle, un patient externe recevant un traitement médical, l'associé de personnes en particulier ou de groupes politiques – et pas seulement un fait à propos d'une personne, sinon tous les faits." *U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.), p. 562; U.S. v. Jones, 565 U.S. ___, (2012),* Alito, J., avis concordant. "En outre, les informations publiques peuvent devenir du domaine de la vie privée lorsqu'elles sont systématiquement recueillies et stockées dans des fichiers détenus par les autorités. Rien d'aussi vrai si ces informations concernent le passé lointain d'une personne…De l'avis du Tribunal, ces informations, lorsqu'elles sont systématiquement recueillies et stockées dans un fichier détenu par les agents de l'État, deviennent du domaine de la 'vie privée' aux effets de l'Article 8(1) de la Convention." (Rotaru v. Romania, [2000] ECHR 28341/95, paragraphes 43-44.

10 Le terme "procédure équitable" peut être remplacé par "équité procédurale" et "justice naturelle", et est correctement articulé à l'Article 6(1) de la Convention Européenne des Droits de l'Homme et à l'Article 8 de la Convention Américaine des Droits de l'Homme.

11 L'interception du Royaume-Uni du Commissaire aux Communications est un exemple de ce mécanisme de supervision indépendant. L'ICO publie un rapport qui comprend quelques données globales mais il ne fournit pas assez de données afin d'examiner les types de demandes, l'étendue de chaque demande d'accès, l'objectif des demandes, ni la sécurité qui leur est appliquée. Cf. **http://www.iocco-uk.info/sections.asp?sectionID=2&type=top**

12 Rapport du Rapporteur Spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, 16 mai 2011, A/HRC/17/27, paragraphe 84.