Principes internationaux pour le respect des droits humains dans la surveillance des communications

International Principles on the Application of Human Rights to Communications Surveillance

(Traduction : Slystone, tradfab, hugo, Pascal22, Hubert Guillaud, sinma, big f, Guillaume, Barbidule, Calou, Asta, wil_sly, chdorb, maugmaug, rou, RyDroid, + anonymes)

Version finale du 7 juin 2013

Alors que se développent les technologies qui leur permettent de surveiller les communications, les États ne parviennent pas à garantir que les lois et réglementations relatives à la surveillance des communications respectent les droits humains et protègent efficacement la vie privée et la liberté d'expression *(Ndt : le choix de traduire human rights par « droits humains » – plutôt que « droits de l'homme » – repose sur le choix délibéré de ne pas perpétuer une exception française sujette à caution.)*. Ce document tente d'expliquer comment le droit international des droits humains doit s'appliquer à l'environnement numérique actuel, à un moment où les technologies et les méthodes de surveillance des communications se généralisent et se raffinent. Ces principes peuvent servir de guide aux organisations citoyennes, aux entreprises et aux États qui cherchent à évaluer si des lois et des pratiques de surveillance, actuelles ou en discussion, sont en conformité avec les droits humains.

Ces principes sont le fruit d'une consultation globale d'organisations citoyennes, d'entreprises et d'experts internationaux sur les aspects juridiques, politiques et

technologiques de la surveillance des communications.

Préambule

Le respect de la vie privée est un droit humain fondamental, indispensable au bon fonctionnement des sociétés démocratiques. Il est essentiel à la dignité humaine et renforce d'autres droits, comme la liberté d'expression et d'information, ou la liberté d'association. Il est consacré par le droit international des droits humains[1]. Les activités qui restreignent le droit au respect de la vie privée, et notamment la surveillance des communications, ne sont légitimes que si elles sont à la fois prévues par la loi, nécessaires pour atteindre un but légitime et proportionnelles au but recherché[2].

Avant la généralisation d'Internet, la surveillance des communications par l'État était limitée par l'existence de principes juridiques bien établis et par des obstacles logistiques inhérents à l'interception des communications. Au cours des dernières décennies, ces barrières logistiques à la surveillance se sont affaiblies, en même temps que l'application des principes juridiques aux nouvelles technologies a perdu en clarté. L'explosion des communications électroniques, ainsi que des informations à propos de ces communications (les « métadonnées » de ces communications), la chute des coûts de stockage et d'exploration de grands jeux de données, ou encore la mise à disposition de données personnelles détenues par des prestataires de service privés, ont rendu possible une surveillance par l'État à une échelle sans précédent[3].

Dans le même temps, l'évolution conceptuelle des droits humains n'a pas suivi l'évolution des moyens modernes de surveillance des communications dont dispose l'État, de sa capacité à croiser et organiser les informations obtenue par différentes techniques de surveillances, ou de la sensibilité

croissante des informations auxquelles il accède.

La fréquence à laquelle les États cherchent à accéder au contenu des communications ou à leurs métadonnées – c'est-à-dire aux informations portant sur les communications d'une personne ou sur les détails de son utilisation d'appareils électroniques – augmente considérablement, sans aucun contrôle approprié[4]. Une fois collectées et analysées, les métadonnées issues des communications permettent de dresser le profil de la vie privée d'un individu, tel que son état de santé, ses opinions politiques et religieuses, ses relations sociales et ses centres d'intérêts, révélant autant de détails, si ce n'est plus, que le seul contenu des communications[5]. Malgré ce risque élevé d'intrusion dans la vie privée des personnes, les instruments législatifs et réglementaires accordent souvent aux métadonnées une protection moindre, et ne restreignent pas suffisamment la façon dont les agences gouvernementales peuvent les manipuler, en particulier la façon dont elles sont collectées, partagées, et conservées.

Pour que les États respectent réellement leurs obligations en matière de droit international des droits humains dans le domaine de la surveillance des communications, ils doivent se conformer aux principes exposés ci-dessous. Ces principes portent non seulement sur l'obligation pesant sur l'État de respecter les droits de chaque individu , mais également sur l'obligation pour l'État de protéger ces droits contre d'éventuels abus par des acteurs non-étatiques, et en particulier des entreprises privées[6]. Le secteur privé possède une responsabilité équivalente en termes de respect et de protection des droits humains, car il joue un rôle déterminant dans la conception, le développement et la diffusion des technologies, dans la fourniture de services de communication, et – le cas échéant – dans la coopération avec les activités de surveillance des États. Néanmoins, le champ d'application des présents principes est limité aux obligations des États.

Une technologie et des définitions changeantes

Dans l'environnement moderne, le terme « surveillance des communications » désigne la surveillance, l'interception, la collecte, le stockage, la modification ou la consultation d'informations qui contiennent les communications passées, présentes ou futures d'une personne, ainsi que de toutes les informations qui sont relatives à ces communications. Les « communications » désignent toute activité, interaction et échange transmis de façon électronique, tels que le contenu des communications, l'identité des parties communiquant, les données de localisation (comme les adresses IP), les horaires et la durée des communications, ainsi que les identifiants des appareils utilisés pour ces communications.

Le caractère intrusif de la surveillance des communications est traditionnellement évalué sur la base de catégories artificielles et formelles. Les cadres légaux existants distinguent entre le « contenu » et le « hors-contenu », les « informations sur l'abonné » ou les « métadonnées », les données stockées et celles en transit, les données restant à domicile et celles transmises à un prestataire de service tiers[7]. Néanmoins, ces distinctions ne sont plus appropriées pour mesurer le niveau d'intrusion causé par la surveillance des communications dans la vie privée des individus. Il est admis de longue date que le contenu des communications nécessite une protection légale importante en raison de sa capacité à révéler des informations sensibles, mais il est maintenant clair que d'autres informations issues des communications d'un individu – les métadonnées et diverses informations autres que le contenu – peuvent révéler encore davantage sur l'individu que la communication elle-même, et doivent donc bénéficier d'une protection équivalente.

Aujourd'hui, ces informations, qu'elles soient analysées séparément ou ensemble, peuvent permettent de déterminer l'identité, le comportement, les relations, l'état de santé,

l’origine ethnique, l’orientation sexuelle, la nationalité ou les opinions d’une personne ; ou encore d’établir une carte complète des déplacements et des interactions d’une personne dans le temps[8]., ou de toutes les personnes présentes à un endroit donné, par exemple une manifestation ou un rassemblement politique. En conséquence, toutes les informations qui contiennent les communications d’une personne, ainsi que toutes les informations qui sont relatives à ces communications et qui ne sont pas publiquement et facilement accessibles, doivent être considérées comme des « informations protégées », et doivent en conséquence se voir octroyer la plus haute protection au regard de la loi.

Pour évaluer le caractère intrusif de la surveillance des communications par l’État, il faut prendre en considération non seulement le risque que la surveillance ne révèle des informations protégées, mais aussi les raisons pour lesquelles l’État recherche ces informations. Si une surveillance des communications a pour conséquence de révéler des informations protégées susceptibles d’accroître les risques d’enquêtes, de discrimination ou de violation des droits fondamentaux pesant sur une personne, alors cette surveillance constitue non seulement une violation sérieuse du droit au respect de la vie privée, mais aussi une atteinte à la jouissance d’autres droits fondamentaux tels que la liberté d’expression, d’association et d’engagement politique. Car ces droits ne sont effectifs que si les personnes ont la possibilité de communiquer librement, sans l’effet d’intimidation que constitue la surveillance gouvernementale. Il faut donc rechercher, pour chaque cas particulier, tant la nature des informations collectées que l’usage auquel elles sont destinées.

Lors de l’adoption d’une nouvelle technique de surveillance des communications ou de l’extension du périmètre d’une technique existante, l’État doit vérifier préalablement si les informations susceptibles d’être obtenues rentrent dans le

cadre des « informations protégées », et il doit se soumettre à un contrôle judiciaire ou à un mécanisme de supervision démocratique. Pour déterminer si les informations obtenues par la surveillance des communications atteignent le niveau des « informations protégées », il faut prendre en compte non seulement la nature de la surveillance, mais aussi son périmètre et sa durée. Une surveillance généralisée ou systématique a la capacité de révéler des informations privées qui dépassent les informations collectées prises individuellement, cela peut donc conférer à la surveillance d'informations non-protégées un caractère envahissant, exigeant une protection renforcée[9].

Pour déterminer si l'État est ou non fondé à se livrer à une surveillance des communications touchant à des informations protégées, le respect de principes suivants doit être vérifié.

Les principes

Légalité: toute restriction au droit au respect de la vie privée doit être prévue par la loi. L'État ne doit pas adopter ou mettre en oeuvre une mesure qui porte atteinte au droit au respect de la vie privée sans qu'elle ne soit prévue par une disposition législative publique, suffisamment claire et précise pour garantir que les personnes ont été préalablement informées de sa mise en oeuvre et peuvent en anticiper les conséquences. Etant donné le rythme des changements technologiques, les lois qui restreignent le droit au respect de la vie privée doivent faire l'objet d'un examen régulier sous la forme d'un débat parlementaire ou d'un processus de contrôle participatif.

Objectif légitime : la surveillance des communications par des autorités étatiques ne doit être autorisée par la loi que pour poursuivre un objectif légitime lié à la défense d'un intérêt juridique fondamental pour une société démocratique. Aucune mesure de surveillance ne doit donner lieu à une discrimination sur le fondement de l'origine, du sexe, de la

langue, de la religion, des opinions politiques, de la nationalité, de l'appartenance à un groupe social, de la richesse, de la naissance ou de tout autre situation sociale.

Nécessité : les lois permettant la surveillance des communications par l'État doivent limiter la surveillance aux éléments strictement et manifestement nécessaires pour atteindre un objectif légitime. La surveillance des communications ne doit être utilisée que lorsque c'est l'unique moyen d'atteindre un but légitime donné, ou, lorsque d'autres moyens existent, lorsque c'est le moyen le moins susceptible de porter atteinte aux droits humains. La charge de la preuve de cette justification, que ce soit dans les procédures judiciaires ou législatives, appartient à l'État.

Adéquation : toute surveillance des communications prévue par la loi doit être en adéquation avec l'objectif légitime poursuivi.

Proportionnalité : la surveillance des communications doit être considérée comme un acte hautement intrusif qui interfère avec le droit au respect de la vie privée, ainsi qu'avec la liberté d'opinion et d'expression, et qui constitue de ce fait une menace à l'égard les fondements d'une société démocratique. Les décisions relatives à la surveillance des communications doivent être prises en comparant les bénéfices attendus aux atteintes causées aux droits des personnes et aux autres intérêts concurrents, et doivent prendre en compte le degré de sensibilité des informations et la gravité de l'atteinte à la vie privée.

Cela signifie en particulier que si un État, dans le cadre d'une enquête criminelle, veut avoir accès à des informations protégées par le biais d'une procédure de surveillance des communications, il doit établir auprès de l'autorité judiciaire compétente, indépendante et impartiale, que :

1. il y a une probabilité élevée qu'une infraction pénale

grave a été ou sera commise ;
2. la preuve d'une telle infraction serait obtenue en accédant à l'information protégée recherchée ;
3. les techniques d'investigation moins intrusives ont été épuisées ;
4. l'information recueillie sera limitée à ce qui est raisonnablement pertinent au regard de l'infraction concernée et toute information superflue sera promptement détruite ou restituée ;
5. l'information est consultée uniquement par l'instance spécifiquement désignée, et utilisée exclusivement aux fins pour lesquelles l'autorisation a été accordée.

Si l'État cherche à avoir accès à des informations protégées via une surveillance des communications à des fins qui ne placeront pas une personne sous le risque de poursuites pénales, d'enquête, de discrimination ou de violation des droits de l'homme, l'État doit établir devant une autorité indépendante, impartiale et compétente que :

1. d'autres techniques d'investigation moins intrusives ont été envisagées ;
2. l'information collectée sera limitée à ce qui est raisonnablement pertinent, et toute information superflue sera promptement détruite ou restituée à la personne concernée ;
3. l'information est consultée uniquement par l'instance spécifiquement désignée, et utilisée exclusivement aux fins pour lesquelles l'autorisation a été accordée.

Autorité judiciaire compétente : les décisions relatives à la surveillance des communications doivent être prises par une autorité judiciaire compétente, impartiale et indépendante. L'autorité doit être (1) distincte des autorités qui effectuent la surveillance des communications, (2) au fait des enjeux relatifs aux technologies de la communication et aux droits humains, et compétente pour rendre des décisions judiciaires dans ces domaines, et (3) disposer de ressources

suffisantes pour exercer les fonctions qui lui sont assignées.

Le droit à une procédure équitable : Une procédure équitable suppose que les États respectent et garantissent les droits humains des personnes en s'assurant que les procédures relatives aux atteintes aux droits humains sont prévues par la loi, sont systématiquement appliquées et sont accessibles à tous. En particulier, pour statuer sur l'étendue de ses droits humains, chacun a droit à un procès public dans un délai raisonnable par un tribunal établi par la loi, indépendant, compétent et impartial[10] sauf cas d'urgence lorsqu'il y a un risque imminent de danger pour une vie humaine. Dans de tels cas, une autorisation rétroactive doit être recherchée dans un délai raisonnable. Le simple risque de fuite ou de destruction de preuves ne doit jamais être considéré comme suffisant pour justifier une autorisation rétroactive.

Notification des utilisateurs : les personnes doivent être notifiées d'une décision autorisant la surveillance de leurs communications, avec un délai et des informations suffisantes pour leur permettre de faire appel de la décision, et elles doivent avoir accès aux documents présentés à l'appui de la demande d'autorisation. Les retards dans la notification ne se justifient que dans les cas suivants :

1. la notification porterait gravement atteinte à l'objet pour lequel la surveillance est autorisée, ou il existe un risque imminent de danger pour une vie humaine ; ou
2. l'autorisation de retarder la notification est accordée par l'autorité judiciaire compétente conjointement à l'autorisation de surveillance ; et
3. la personne concernée est informée dès que le risque est levé ou dans un délai raisonnable, et au plus tard lorsque la surveillance des communications prend fin.

À l'expiration du délai, les fournisseurs de services de communication sont libres d'informer les personnes de la surveillance de leurs communications, que ce soit de leur

propre initiative ou en réponse à une demande.

Transparence : les États doivent faire preuve de transparence quant à l'utilisation de leurs pouvoirs de surveillance des communications. Ils doivent publier, a minima, les informations globales sur le nombre de demandes approuvées et rejetées, une ventilation des demandes par fournisseurs de services, par enquêtes et objectifs. Les États devraient fournir aux individus une information suffisante pour leur permettre de comprendre pleinement la portée, la nature et l'application des lois autorisant la surveillance des communications. Les États doivent autoriser les fournisseurs de service à rendre publiques les procédures qu'ils appliquent dans les affaires de surveillance des communications par l'État, et leur permettre de respecter ces procédures ainsi que de publier des informations détaillées sur la surveillance des communications par l'État.

Contrôle public : les États doivent établir des mécanismes de contrôle indépendants pour garantir la transparence et la responsabilité de la surveillance des communications[11]. Les instances de contrôle doivent avoir les pouvoirs suivants : accéder à des informations sur les actions de l'État, y compris, le cas échéant, à des informations secrètes ou classées ; évaluer si l'État fait un usage légitime de ses prérogatives ; évaluer si l'État a rendu publiques de manière sincère les informations sur l'étendue et l'utilisation de ses pouvoirs de surveillance ; publier des rapports réguliers ainsi que toutes autres informations pertinentes relatives à la surveillance des communications. Ces mécanismes de contrôle indépendants doivent être mis en place en sus de tout contrôle interne au gouvernement.

Intégrité des communications et systèmes : Afin d'assurer l'intégrité, la sécurité et la confidentialité des systèmes de communication, et eu égard au fait que toute atteinte à la sécurité pour des motifs étatiques compromet presque toujours

la sécurité en général, les États ne doivent pas contraindre les fournisseurs de services, ou les vendeurs de matériels et de logiciels, à inclure des capacités de surveillance dans leurs systèmes ou à recueillir et conserver certaines informations exclusivement dans le but de permettre une surveillance par l'État. La collecte et le stockage des données a priori ne doivent jamais être demandés aux fournisseurs de services. Les personnes ont le droit de s'exprimer anonymement, les États doivent donc s'abstenir d'imposer l'identification des utilisateurs comme condition préalable pour l'accès à un service[12].

Garanties dans le cadre de la coopération internationale : en réponse aux évolutions dans les flux d'information et les technologies de communication, les États peuvent avoir besoin de demander assistance à un fournisseur de services étranger. Les traités de coopération internationale en matière de police et de justice et les autres accords conclus entre les États doivent garantir que, lorsque plusieurs droits nationaux peuvent s'appliquer à la surveillance des communications, ce sont les dispositions établissant la plus grande protection à l'égard des individus qui prévalent. Lorsque les États demandent assistance dans l'application du droit, le principe de double-incrimination doit être appliqué *(NdT : principe selon lequel, pour être recevable, la demande de collaboration doit porter sur une disposition pénale existant à l'identique dans les deux pays)*. Les États ne doivent pas utiliser les processus de coopération judiciaire ou les requêtes internationales portant sur des informations protégées dans le but de contourner les restrictions nationales sur la surveillance des communications. Les règles de coopération internationale et autres accords doivent être clairement documentés, publics, et conformes au droit à une procédure équitable.

Garanties contre tout accès illégitime : les États doivent adopter une législation réprimant la surveillance illicite des

communications par des acteurs publics ou privés. La loi doit prévoir des sanctions civiles et pénales dissuasives, des mesures protectrices au profit des lanceurs d'alertes, ainsi que des voies de recours pour les personnes affectées. Cette législation doit prévoir que toute information obtenue en infraction avec ces principes est irrecevable en tant que preuve dans tout type de procédure, de même que toute preuve dérivée de telles informations. Les États doivent également adopter des lois prévoyant qu'une fois utilisées pour l'objectif prévu, les informations obtenues par la surveillance des communications doivent être détruites ou retournées à la personne.

Signataires

- Access Now
- Article 19 (International)
- Bits of Freedom (Netherlands)
- Center for Internet & Society (India)
- Comision Colombiana de Juristas (Colombia)
- Derechos Digitales (Chile)
- Electronic Frontier Foundation (International)
- Open Media (Canada)
- Open Net (South Korea)
- Open Rights Group (United Kingdom)
- Privacy International (International)
- Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (Canada)
- Statewatch (UK)

Notes

[1] Article 12 de la Déclaration universelle des droits de l'homme ; article 14 de la Convention des Nations Unies sur les travailleurs migrants ; article 16 de la Convention des Nations Unies sur la protection des droits de l'enfant ; pacte international relatif aux droits civils et politiques ;

article 17 du pacte international relatif aux droits civils et politiques ; conventions régionales dont article 10 de la Charte africaine des droits et du bien-être de l'enfant, article 11 de la Convention américaine des droits de l'Homme, article 4 de la déclaration de principe de la liberté d'expression en Afrique, article 5 de la déclaration américaine des droits et devoirs de l'Homme, article 21 de la Charte arabe des droits de l'Homme et article 8 de la Convention européenne de la protection des droits de l'Homme et des libertés fondamentales ; principes de Johannesburg relatifs à la sécurité nationale, libre expression et l'accès à l'information, principes de Camden sur la liberté d'expression et l'égalité.

[2] Article 29 de la Déclaration universelle des droits de l'homme ; commentaire général numéro 27, adopté par le Comité des droits de l'Homme sous l'article 40, paragraphe 4, par The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, du 2 novembre ; voir aussi de Martin Scheinin, « Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, » 2009, A/HRC/17/34.

[3] Les métadonnées des communications peuvent contenir des informations à propos de notre identité (informations sur l'abonné, information sur l'appareil utilisé), de nos interactions (origines et destinations des communications, en particulier celles montrant les sites visités, les livres ou autres documents lus, les personnes contactées, les amis, la famille, les connaissances, les recherches effectuées et les ressources utilisées) et de notre localisation (lieux et dates, proximité avec d'autres personnes) ; en somme, des traces de presque tous les actes de la vie moderne, nos humeurs, nos centres d'intérêts, nos projets et nos pensées les plus intimes.

[4] Par exemple, uniquement pour le Royaume-Uni, il y a actuellement environ 500 000 requêtes sur les métadonnées des

communications chaque année, sous un régime d'auto-autorisation pour les agences gouvernementales, qui sont en mesure d'autoriser leurs propres demandes d'accès aux informations détenues par les fournisseurs de services. Pendant ce temps, les données fournies par les rapports de transparence de Google montrent qu'aux États-Unis, les requêtes concernant des données d'utilisateurs sont passées de 8 888 en 2010 à 12 271 en 2011. En Corée, il y a eu environ 6 millions de requêtes par an concernant des informations d'abonnés et quelques 30 millions de requêtes portant sur d'autres formes de communications de métadonnées en 2011-2012, dont presque toutes ont été accordées et exécutées. Les données de 2012 sont accessibles ici.

[5] Voir par exemple une critique du travail de Sandy Pentland, « Reality Minning », dans la Technology Review du MIT, 2008, disponible ici, voir également Alberto Escudero-Pascual et Gus Hosein « Questionner l'accès légal aux données de trafic », Communications of the ACM, volume 47, Issue 3, mars 2004, pages 77-82.

[6] Rapport du rapporteur spécial des Nations Unies sur la liberté d'opinions et d'expression, Frank La Rue, 3 juin 2013, disponible ici.

[7] « Les gens divulguent les numéros qu'ils appellent ou textent à leurs opérateurs mobiles, les URL qu'ils visitent et les adresses courriel avec lesquelles ils correspondent à leurs fournisseurs d'accès à Internet, et les livres, les courses et les médicaments qu'ils achètent à leurs boutiques en ligne… On ne peut présumer 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).

[8] « La surveillance à court terme des déplacements d'une

personne sur la voie publique est compatible avec le respect 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).

[9] « La surveillance prolongée révèle des informations qui ne sont pas révélées par la surveillance à court terme, comme ce que fait un individu à plusieurs reprises, ce qu'il ne fait pas, et ce qu'il fait à la suite. Ce type d'informations peut en révéler plus sur une personne que n'importe quel trajet pris isolément. Des visites répétées à l'église, à une salle de gym, à un bar ou à un bookmaker racontent une histoire que ne raconte pas une visite isolée, tout comme le fait de ne pas se rendre dans l'un de ces lieux durant un mois. La séquence des déplacements d'une personne peut révéler plus de choses encore ; une seule visite à un cabinet de gynécologie nous en dit peu sur une femme, mais ce rendez-vous suivi quelques semaines plus tard d'une visite à un magasin pour bébés raconte une histoire différente. Quelqu'un qui connaîtrait tous les trajets d'une personne pourrait en déduire si c'est un fervent pratiquant, un buveur invétéré, un habitué des clubs de sport, un mari infidèle, un patient ambulatoire qui suit un traitement médical, un proche de tel ou tel individu, ou de tel groupe politique – il pourrait en déduire non pas un de ces faits, mais tous. » 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., participants. « De plus, une information publique peut entrer dans le cadre de la vie privée quand elle est systématiquement collectée et stockée dans des fichiers tenus par les autorités. Cela est d'autant plus vrai quand ces informations concernent le passé lointain d'une personne. De l'avis de la Cour, une telle information, lorsque systématiquement collectée et stockée dans un fichier tenu par des agents de l'État, relève du champ d'application de la vie privée au sens de l'article 8 (1) de la Convention. » (Rotaru

v. Romania, (2000) ECHR 28341/95, paras. 43-44.

[10] Le terme « Due process » (procédure équitable) peut être utilisé de manière interchangeable avec « équité procédurale » et « justice naturelle », il est clairement défini dans la Convention européenne pour les droits de l'Homme article 6(1) et article 8 de la Convention américaine relative aux droits de l'Homme.

[11] Le commissaire britannique à l'interception des communications est un exemple d'un tel mécanisme de contrôle indépendant. L'ICO publie un rapport qui comprend des données agrégées, mais il ne fournit pas de données suffisantes pour examiner les types de demandes, l'étendue de chaque demande d'accès, l'objectif des demandes et l'examen qui leur est appliqué. Voir ici.

[12] Rapport du rapporteur spécial 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, para 84.