AMNESTY INTERNATIONAL

Questions & Réponses à propos de la « surveillance»

1. Exploration du réseau câblé (Loi sur le renseignement – LRens)

Pourquoi Amnesty critique-t-elle la loi sur le renseignement (LRens) ?

La nouvelle loi sur le renseignement, adoptée en automne 2015 par le Parlement, met à disposition du Service de renseignement de la confédération (SRC) une palette de nouveaux moyens qui sont susceptibles de porter atteinte au droit au respect de la sphère privée. Le SRC pourra ainsi, par exemple, surveiller des espaces privés au moyen de mouchards ou introduire des chevaux de Troie dans des systèmes informatiques étrangers. Sur le plan des droits humains, ces mesures, ainsi que celle de l'exploration du réseau câblé, sont problématiques.

Qu'est-ce que l'exploration du réseau câblé ?

L'exploration du réseau câblé permettra au SRC « d'enregistrer les signaux transmis par réseau filaire qui traversent la Suisse ». Ceci signifie que le SRC pourra enregistrer tous les flux de données qui quittent la Suisse pour l'étranger et les analyser au moyen de mots-clés. Les services de renseignements auront ainsi accès aux métadonnées et au contenu de communications électroniques telles que les e-mails, la téléphonie ou les recherches via internet.

Pourquoi Amnesty critique-t-elle l'exploration du réseau câblé?

Dès lors que la grande majorité des communications Internet en Suisse transitent par des serveurs et des réseaux étrangers, elles seraient en principe toutes concernées par cette surveillance. L'exploration du réseau câblé est une forme de surveillance de masse menée sans même qu'elle n'implique la présence de soupçons. L'ensemble du flux de données est scanné sur la base de mots-clés et le SRC tente alors, au moyen de recherches croisées, de retrouver l'aiguille dans la botte de foin. Ceci conduit inévitablement à de trop nombreuses erreurs et à soupçonner des personnes innocentes. Une recherche de masse non fondée sur des soupçons précis basés sur des indices concrets est illégale et incompatible avec un État de droit démocratique.

Quels sont les droits concernés par la surveillance de masse ?

La surveillance de masse, non fondée sur des soupçons précis, entre en conflit avec plusieurs droits fondamentaux contenus dans la Constitution fédérale et la Convention européenne des droits de l'homme (CEDH). A côté du droit à la protection de la sphère privée et au secret des communications, la liberté d'expression et la présomption d'innocence sont aussi concernées. Si l'on surveille un médecin, un avocat un prêtre ou un journaliste, le secret professionnel ou la protection des sources sont également mis en danger.

La LRens prévoit des limitations : l'exploration du réseau câblé ne doit servir qu'à « chercher des informations sur des événements importants en matière de politique de sécurité se produisant à l'étranger » et les données purement suisses doivent être effacées.

Le SRC aurait accès à toutes les données qui transitent par le réseau câblé vers l'étranger. Même si quelqu'un domicilié en Suisse envoie un courriel à une autre personne en Suisse via son compte GMail, Yahoo ou similaire, ce message transite par l'étranger autorisant ainsi le SRC à y avoir accès, même si l'expéditeur et le destinataire sont tous deux en Suisse.

Les données suisses doivent être effacées: pourquoi se préoccuper de la surveillance à l'étranger ?

La surveillance de personnes à l'étranger doit également rester proportionnelle et ne saurait être ni permanente, ni généralisée. Le droit à la sphère privée est reconnu internationalement (par exemple

dans la CEDH) et doit bénéficier à toute personne, indépendamment de son lieu de résidence, en Suisse comme à l'étranger.

L'exploration du réseau câblé serait soumise à autorisation et serait de plus placée sous surveillance. Pourquoi ces restrictions et ces contrôles sont-ils insuffisants ?

Les critiques à l'encontre de la LRens ont amené le Parlement à introduire quelques restrictions et contrôles. Ceci est à saluer mais ne change rien de fondamental à la critique. Les restrictions et les contrôles prévus limitent certes quelque peu l'utilisation des données mais cela ne change rien au fait que les flux sont enregistrés et analysés. La surveillance débute dès la collecte des données et non au moment de leur analyse. La surveillance et le contrôle des services de renseignements s'avèrent une tâche difficile, comme le montrent de nombreux exemples à travers le monde, y compris en Suisse.

Amnesty est-elle fondamentalement opposée à l'exploration du réseau câblé ?

L'exploration du réseau câblé représente une forme de surveillance de masse préventive et peut être menée en l'absence de tout soupçon basé sur des indices concrets. Nous y sommes fondamentalement opposés.

N'est-ce pas trop restreindre le travail des services secrets dans leur lutte contre la criminalité et le terrorisme ?

La LRens donne au SRC de nouveaux moyens et de nouvelles compétences pour assurer une surveillance ciblée des personnes suspectes. Toutes ces mesures doivent respecter le principe de la proportionnalité ; les droits fondamentaux ne doivent pas être sacrifiés sur l'autel de la sécurité. La criminalité et le terrorisme doivent être combattus par des moyens légaux et respectueux de l'Etat de droit. La poursuite pénale reste pour cela le moyen le plus adéquat. En cas de soupçons fondés sur des indices concrets d'activités terroristes, de criminalité organisée, de transferts illégaux d'armement ou de leurs actes préparatoires, ce sont les autorités de poursuite pénale (Ministère public, polices cantonales) qui doivent intervenir et non les services de renseignement. C'est l'unique façon de garantir des procédures respectueuses de l'Etat de droit.

La surveillance de masse n'est-elle pas nécessaire pour lutter contre le terrorisme ?

Il est fréquemment fait référence à la « sécurité nationale » pour justifier des atteintes aux droits humains. Il n'existe pourtant aucune preuve à ce jour que des mesures de surveillance généralisées, non fondées sur des soupçons précis, aient contribué à renforcer la sécurité.
Une commission d'enquête indépendante, mise en place par le président Obama (PCLOB), a conclu en janvier 2015 que la collecte de données par la *National Security Agency* (NSA) était illégale et représentait une « menace sérieuse pour les droits civiques et la démocratie ». Elle s'est par ailleurs montrée inutile dans la lutte contre le terrorisme : « Il n'y a pas un seul cas dans lequel le programme (de la NSA) a permis de mettre à jour des projets terroristes inconnus ou a contribué à empêcher des attaques terroristes » conclut le rapport de la commission.
Une enquête a également été menée en Allemagne sur l'efficacité des mesures de surveillance généralisée (saisie des métadonnées). Là non plus, l'efficacité des mesures n'a pas été démontrée. Dans la conclusion de son expertise effectuée pour le compte du gouvernement, l'Institut Max Planck conclut : « En comparaison avec les taux de cas élucidés qui ont été atteints en Suisse et en Allemagne en 2009, aucun indice ne laisse croire que la surveillance pratiquée en Suisse depuis environ 10 ans ait mené à un taux systématiquement plus élevé. »

2. Enregistrement des métadonnées (Loi fédérale sur la surveillance de la correspondance par poste et télécommunication -LSCPT)

En quoi consiste l'enregistrement des métadonnées ? Que prévoit la révision de la LSCPT ?

AMNESTY INTERNATIONAL

En Suisse, les fournisseurs de prestations postales, téléphoniques et d'Internet sont tenus de conserver pendant 6 mois les données relatives aux communications de leurs clients (qui, quand, où et avec qui on communique) ; tous les moyens de communication sont concernés (téléphone, Internet, e-mail). Dès lors que nous sommes tous, sans exception, concerné·e·s par ces mesures de surveillance, ceci représente une intrusion grave dans la sphère privée, pourtant protégée par la Constitution fédérale. Avec la révision de la Loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT), le délai de 6 mois devrait être doublé et donc porté à une année. Ces données peuvent actuellement être rendues disponibles pour les autorités de poursuites. Avec la révision de la loi, elles le seront aussi pour le SRC.

Amnesty critique cette saisie des métadonnées, pourquoi ?

La saisie des métadonnées représente une forme de surveillance de masse préventive et non fondée sur des soupçons. En Suisse, nous sommes toutes et tous, sans exceptions, concern·é·e·s par cette mesure de surveillance même si nul soupçon de quoi que ce soit ne pèse sur nous. Même les personnes tenues au secret professionnel ou de fonction comme les médecins ou les avocats ou celles tenues de protéger leurs sources comme les journalistes ne font pas exception. Ces mesures de surveillance représentent donc une atteinte aux droits fondamentaux comme la protection de la sphère privée et la liberté d'expression qui sont garantis dans la Constitution et dans la CEDH.

Que disent les tribunaux à propos de la saisie des métadonnées ? La situation est-elle la même dans d'autres pays ?

Toutes les Cours constitutionnelles qui ont eu à se prononcer sur des réglementations comparables à la législation suisse ont estimé que la saisie systématique des métadonnées constituait une atteinte illégale aux droits fondamentaux et les ont suspendues (Roumanie, 2009 et 2014, Allemagne, 2010, République Tchèque, 2011, Autriche, 2014, Pays-Bas, 2015, Bulgarie, 2015).
En 2014, la Cour européenne de justice a suspendu les lignes directrices de l'Union Européenne en matière de saisie des métadonnées. La cour a estimé que les lignes directrices portaient atteinte à grande échelle et de manière particulièrement grave à la sphère privée. Elle a estimé que le législateur avait franchi, avec ces lignes directrices, les limites à respecter en matière de principe de la proportionnalité.
Le Haut-Commissaire aux droits de l'homme des Nations Unies s'est lui-même exprimé sur la question de la saisie des métadonnées : « La saisie de données sur les communications représente une atteinte à la sphère privée et ceci indépendamment du fait que les données soient ensuite consultées ou pas. Cette intrusion dans la sphère privée a ensuite des répercussions négatives sur la liberté d'opinion et la liberté d'association. »

Quelles sont les données enregistrées ?

La collecte des données porte sur qui a appelé qui, quand et combien de temps a duré la communication, sur qui s'est connecté sur Internet et pour quelle durée, ainsi que sur qui a envoyé un SMS à qui et quand ou s'est connecté sur une boîte aux lettres électronique. La localisation des téléphones mobiles est également enregistrée.
Comme les Smartphones modernes sont connectés sur Internet de manière pratiquement permanente (même en dehors des communications actives), la localisation des propriétaires de téléphones portables est assurée de manière quasi absolue et à quelques centaines de mètres près, ce qui permet d'établir un profil précis des déplacements de tout un chacun.

Dans quels cas les données sont-elles utilisées ?

Pour pouvoir accéder aux données, les autorités de poursuite pénales n'ont besoin que d'un « soupçon urgent en relation avec un crime ou un délit » et même, comme dans le cas « d'utilisation abusive d'une installation de télécommunication », le simple soupçon d'une infraction est suffisant. La

transmission des données n'est donc pas limitée aux crimes les plus graves mais est également possible dans le cas de délits moindres comme un simple vol.
Avec la nouvelle LRens, le SRC sera également autorisé à accéder à ces données, une des mesures de recherche qui, selon la loi, sont « soumises à autorisation ».

Celui qui n'a rien à se reprocher n'a rien à craindre, non ?

Avec la saisie des métadonnées, toute personne est surveillée à titre préventif et sur la base d'un soupçon général. La présomption d'innocence est ici balayée. Il n'y a aucune exception, même pas pour les médecins, les avocats, les prêtres ou les journalistes, toutes des activités tenues au secret professionnel.

Ces données ne sont-elles pas collectées dans le but d'élucider des affaires criminelles ?

Il n'existe que très peu d'études qui analysent le lien entre la saisie des métadonnées et la lutte contre la criminalité (cf. enquêtes aux USA et en Allemagne ci-dessus, page 2). Pour pouvoir porter gravement atteinte aux droits fondamentaux, comme dans le cas de la saisie des métadonnées, il faut une justification solide pour démontrer son exigibilité. Une banale argumentation affirmant que les métadonnées faciliteront le travail des enquêteurs et amélioreront la sécurité n'est pas suffisante. Une restriction aux droits fondamentaux est illégale lorsque l'utilité de la mesure n'est pas prouvée.

Les métadonnées ne sont-elles pas de toute manière collectées par les fournisseurs ?

De nombreuses données, parmi celles enregistrées par les fournisseurs, leur sont utiles pour leur facturation et pour servir, si nécessaire, de justificatifs. Le fait que ces données, collectées pendant 6 mois – ou même un an si la nouvelle loi le décide – puissent être mises à disposition des autorités change profondément le caractère de leur récolte de même que les risques qui y sont liés.

3. La surveillance en général

Qu'est-ce que la surveillance ?

La surveillance est l'observation par l'État des communications, du comportement ou des mouvements d'une personne. Les gouvernements peuvent ordonner des surveillances légales lorsqu'elles sont ciblées et fondées. A l'opposé, elles peuvent être utilisées pour intimider des activistes, pour contrôler la société ou pour museler la dissidence.
Font partie de la surveillance des communications toutes les activités telles que l'observation, la saisie, le stockage, le tri, l'analyse, le partage ou tout autre usage qui peut être fait des données relatives à une communication (métadonnées) ou à son contenu.

Amnesty s'oppose-t-elle par principe à la surveillance ?

Amnesty ne s'oppose pas par principe à toute forme de surveillance mais rejette toute mesure de surveillance massive et indiscriminée, donc fondée sur aucun soupçon. La surveillance n'est justifiée que s'il existe des indices concrets d'une activité illégale et que la mesure est ciblée, nécessaire, proportionnelle et ordonnée par un juge.

Qu'est-ce que la surveillance de masse indiscriminée ?

La surveillance de masse indiscriminée est, par exemple, la surveillance d'Internet et des communications téléphoniques d'un grand nombre de personnes, parfois d'un pays entiers, sans que les personnes surveillées n'aient jamais donné lieu à un quelconque soupçon d'activités illégales.

Existe-t-il une forme légale de surveillance de masse indiscriminée ?

AMNESTY INTERNATIONAL

Non. Les gouvernements peuvent certes légaliser des programmes de surveillance de masse mais ils se mettent alors clairement en porte-à-faux avec le droit international que la plupart des États ont ratifié. Selon Amnesty International, une mesure de surveillance indiscriminée ne peut jamais constituer une atteinte justifiée et proportionnelle aux droits humains.

Quand une surveillance devient-elle légale ?

La surveillance, pour être légale, doit répondre à six conditions :

- elle doit avoir une **base légale** claire ; c'est-à-dire qu'elle doit être réglementée par des dispositions légales accessibles à toutes et tous
- elle doit être **autorisée** par une décision spécifique, prononcée par un **juge** ou une autre autorité indépendante
- elle doit être instaurée pour protéger un **intérêt public légitime**, par exemple pour élucider une enquête pénale ou pour garantir la sécurité nationale
- elle doit être **ciblée** sur une personne, un groupe de personnes précis ou sur un lieu bien défini et permettre d'atteindre un objectif légitime
- elle doit être **nécessaire** ; à savoir qu'il ne doit pas y avoir d'autre moyen utilisable, mois intrusif, pour atteindre le but recherché
- elle doit être **proportionnelle** ; c'est-à-dire que l'atteinte qu'elle occasionne aux droits humains doit être proportionnelle au but légitime recherché

La surveillance des communications Internet et téléphoniques de personnes que l'on soupçonne d'appartenir à un réseau de blanchiment d'argent, par exemple, sera légale si elle respecte ces six conditions. A l'opposé, la surveillance des communications d'un pays entier – comme l'a pratiquée la NSA aux États Unis – est totalement illégale. Une telle surveillance est disproportionnée et les gouvernements ne sont pas en mesure de fournir des preuves concluantes de sa nécessité. De nombreux programmes de surveillance sont, de plus, autorisés par des normes légales floues que les juges aussi bien que le législateur ont de la peine à interpréter. Dans de nombreux pays, la surveillance est ordonnée par des décisions secrètes et sans aucune transparence.

Quelles sont les protections juridiques contre la surveillance ?

- L'article 17 du Pacte international relatif aux droits civils et politiques protège chacun des « immixtions arbitraires ou illégales dans sa vie privée »
- L'article 19 du même texte protège le droit à la liberté d'expression, qui comprend « la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières ».

Les droits humains reconnus au niveau international protègent la sphère privée et la libre expression. Les États sont tenus de les respecter et de les protéger. Le droit international permet aux gouvernements de limiter ces droits dans certaines circonstances. C'est également le cas en ce qui concerne la surveillance des communications. Mais toute atteinte à la sphère privée doit être proportionnelle, ce qui signifie que les mesures de surveillance doivent être nécessaires et adéquates pour atteindre le but poursuivi. Elles doivent être exigibles et représenter la manière la moins intrusive possible pour atteindre le but recherché.

Quel est le rapport entre le droit national et le droit international en ce qui concerne la surveillance ?

Les compétences en matière de surveillance sont réglées par le droit national. Mais le fait que la surveillance soit réglée par une loi ne la rend pas automatiquement légale. Les États ont, en plus de leur propre législation, des obligations à respecter vis-à-vis des normes internationales en matière de droits humains. Une mesure de surveillance qui ne serait pas compatible avec les droits humains est illégale. La surveillance des communications est une atteinte au droit à la sphère privée et à la liberté d'expression, deux droits qui sont garantis, entre autres, par la CEDH.

AMNESTY INTERNATIONAL

En quoi les révélations d'Edward Snowden sont-elles si importantes ?

Les révélations du lanceur d'alerte Edward Snowden ont révélé ce que beaucoup craignaient déjà: des gouvernements enregistrent et analysent secrètement nos données privées ainsi que nos communications, nos E-mails, nos appels téléphoniques et nos SMS. Ils surveillent des millions de personnes, sans aucun contrôle ni transparence. Grâce aux révélations d'un ancien fonctionnaire de la NSA américaine, Edward Snowden, nous pouvons aujourd'hui mesurer l'étendue de la surveillance exercée par les services secrets américains et britanniques. Quelques exemples:

- Les services secrets des USA délivrent chaque jour 200 millions de notes écrites aux services britanniques.
- Les services secrets des USA et du Royaume-Uni sont en mesure d'enclencher le micro de votre téléphone portable et de vous écouter même lorsque votre téléphone est déconnecté.
- Les mêmes services enregistrent des images Webcam de millions d'Internautes alors même qu'aucun soupçon ne pèse sur eux.

Suis-je surveillé ?

Vous utilisez un téléphone mobile ou Internet ? Dans ce cas, il y a de fortes chances pour que vous soyez surveillé·e. Des programmes de surveillance comme « Prism » et « Upstream » utilisés par la NSA ou encore « Tempora » utilisés par le *Government Communication Head Quarter* (GCHQ) britannique, ont accès aux données des grandes firmes d'Internet telles que Google, Facebook et Yahoo. Par ailleurs, ils interceptent les données directement sur les câbles utilisés par Internet pour faire circuler les données. La téléphonie mobile est également très largement surveillée dans de nombreux pays. Vous n'êtes malheureusement rien d'autre qu'un numéro de téléphone, une adresse e-mail ou IP qui est stockée dans des centrales de données.

Quelles données récoltent-ils sur moi ?

Des données personnelles sont générées à chaque fois que les autorités, les entreprises ou des particuliers utilisent une technologie digitale, en retirant de l'argent au Bancomat, en surfant sur Internet, par le biais de caméras de surveillance ou au sein de l'administration publique (Administration fiscale, services de santé). Les programmes de surveillance enregistrent et analysent l'historique de votre navigateur internet, vos recherches, vos e-mails, vos informations instantanées, vos conversations par webcam et vos appels téléphoniques. Ils collectent également les métadonnées (les « données sur les données ») : avec qui, quand, combien de temps et depuis où avez-vous téléphoné ? Où étiez-vous minute après minute, à qui avez-vous envoyé des mails, etc.

Que se passe-t-il avec mes données ?

Le problème est là ! Personne ne sait exactement ce qu'il advient de vos données personnelles et vous ne pouvez pas vous défendre contre leur diffusion. Ce qui est certain, c'est que vos données sont stockées dans de gigantesques banques de données et analysées au moyen de puissants algorithmes. Les données sont échangées entre plusieurs États et rendues accessibles à plusieurs services de renseignements.

Pourquoi la collecte des données est-elle dangereuse ?

En soi et prises séparément, les différentes données et les bribes d'informations récoltées n'ont pas grande valeur. Mais, avec la mise en réseau croissante des divers systèmes, donc le regroupement de données éparses, des profils personnels très détaillés peuvent être effectués. Les opinions politiques, les préférences sexuelles, le style de vie, l'environnement social, le niveau de formation ou encore le potentiel criminel d'une personne sont des éléments que l'on peut récolter.

Comment la surveillance influence-t-elle la liberté d'opinion ?

Le fait de se savoir placées sous contrôle de l'État conduit de nombreuses personnes à s'autocensurer. Telle une épée de Damoclès, la surveillance influence la liberté d'opinion et de réunion. Celui ou celle qui a peur d'être surveillé·e exprime moins volontiers son opinion et fait moins confiance à Internet pour appeler à une manifestation ou pour s'informer sur des thèmes sensibles. Le droit à la sphère privée est une condition de base nécessaire à l'exercice de nombreux autres droits comme la liberté d'opinion et d'information, le droit à se rassembler pacifiquement et l'interdiction de la discrimination.

Comment les gouvernements utilisent-ils la surveillance comme moyen de répression ?

Les plateformes en lignes, les réseaux sociaux, sont de plus en plus utilisées pour appeler à des protestations : le « printemps arabe » est un bon exemple de cette utilisation. De nombreux gouvernements du monde entier restreignent ces nouvelles possibilités de s'exprimer et de s'informer ou les utilisent dans des buts répressifs. La menace sur la liberté d'expression s'illustre notamment par la censure exercée par le gouvernement turc, sur YouTube et Twitter, ou encore par la surveillance globale d'Internet en Chine. Pendant les protestations de Maidan à Kiev en 2014, les possesseurs de téléphone mobile qui se trouvaient dans les environs de la manifestation ont reçu un SMS intimidant qui disait : « Cher destinataire, vous avez été enregistré comme participant à la manifestation ».

Pourquoi me soucier de la surveillance si je n'ai rien à me reprocher ?

La question est mal formulée et on devrait plutôt se demander pourquoi porte-t-on atteinte à ma sphère privée alors que je n'ai rien fait de répréhensible ? Nous n'accepterions jamais que le gouvernement place des caméras vidéos dans nos appartements, ouvre systématiquement notre courrier et écoute toutes nos discussions avec nos amis. C'est pourtant ce qu'il fait avec la surveillance de masse.
Une société qui respecte la liberté et l'État de droit doit également respecter la vie privée de ses citoyen·ne·s à moins qu'il n'existe des soupçons, fondés sur des indices concrets, qu'il ou elles s'adonnent à des activités criminelles. Si ce n'est pas le cas, tous les citoyen·ne·s sont soudain présumé·e·s coupables jusqu'à ce qu'ils aient pu prouver leur innocence.
Il est notoire que les données privées sont utilisées, dans certains pays, pour intimider, opprimer et réduire au silence les opposants et les journalistes. Si vous estimez que ce qui se passe dans ces pays est impossible chez vous, dites-vous bien qu'aucun État n'est à l'abri d'un changement de régime. Si nous ne nous protégeons pas maintenant, nous prenons le risque d'une future société au sein de laquelle la vie privée sera absente.

Pourquoi me soucier d'une surveillance du gouvernement si les grandes firmes d'Internet ont déjà collecté toutes mes données personnelles ?

Vous devriez également vous préoccuper de l'usage que font ces grandes entreprises de vos données. Elles devraient au minimum vous informer de cet usage. Elles sont tenues de les protéger soigneusement et ne sont pas autorisées à les utiliser pour autre chose que ce pourquoi elles ont été collectées. Ceci dit, il y a une énorme différence entre les données collectées par Facebook, par exemple, et celles collectées par le gouvernement : lorsque vous vous annoncez sur un réseau social, vous décidez de votre plein gré de communiquer vos données privées, alors que les services de renseignements prélèvent ces données sans vous demander votre avis. Enfin les entreprises ne sont pas en mesure de collecter les données de tout le monde mais uniquement des personnes qui utilisent leurs produits. C'est bien sûr différent pour les services de renseignements.

Quelles sont les revendications d'Amnesty International ?

Amnesty demande aux gouvernements du monde entier

- de mettre fin sans délai à tous les programmes de surveillance de masse et de garantir que toutes les mesures de surveillance ciblées prennent en compte les normes internationales en matière de droits humains.

- de garantir que la surveillance des communications ne soit exercée qu'en cas de soupçons basés sur des indices concrets et sur décision judiciaire, que les moyens utilisés portent le moins possible atteinte aux droits fondamentaux et que les mesures de surveillance soient ciblées, nécessaires et proportionnelles.
- de garantir la protection de la liberté d'opinion et d'information online et que chacun·e soit en mesure de chercher, de recevoir et de diffuser des informations et des opinions sans considération de frontières.