Journée mondiale
contre la cyber-censure

LES ENNEMIS D'INTERNET

2014

REPORTERS SANS FRONTIERES
POUR LA LIBERTE DE L'INFORMATION

LES INSTITUTIONS ENNEMIES D'INTERNET

12 Mars 2014

Surveillance Censure Emprisonnement Désinformation

Retrouvez l'intégralité du rapport sur 12mars.rsf.org

REPORTERS SANS FRONTIERES
POUR LA LIBERTE DE L'INFORMATION

ENNEMIS D'INTERNET 2014

LES INSTITUTIONS AU CŒUR DU SYSTÈME DE CENSURE ET DE SURVEILLANCE

En février 2013, Natalia Radzina, rédactrice en chef de Charter97, un site d'information bélarusse régulièrement censuré pour ses positions critiques vis-à-vis du pouvoir, assistait à la conférence sur Internet et la liberté de la presse organisée par l'OSCE à Vienne. Elle y est tombée sur une connaissance qu'elle aurait préféré ne pas croiser : un membre du Centre analytique des opérations, l'organisme qui coordonne les opérations de surveillance et de censure sur Internet au Bélarus. Ce sont ces institutions, peu connues mais souvent au centre des systèmes de surveillance ou de censure de nombreux Etats, que Reporters sans frontières a décidé de mettre en avant dans son rapport « Ennemis d'Internet », publié à l'occasion de la Journée mondiale contre la censure, le 12 mars.

Désigner comme « Ennemis d'Internet » des institutions plutôt que des Etats permet de mettre en évidence la schizophrénie de certains pays lorsqu'il est question des libertés en ligne. Ainsi, sur les **32 institutions** désignées « Ennemis d'Internet » par Reporters sans frontières, trois appartiennent à des démocraties qui se veulent traditionnellement respectueuses des libertés fondamentales : le Centre de développement des télématiques en Inde, le Government Communications Headquarters (GCHQ) au Royaume-Uni et la National Security Agency (NSA) aux États-Unis.

La NSA et le GCHQ ont espionné les communications de plusieurs millions de citoyens, dont de nombreux journalistes, introduit sciemment des failles de sécurité dans les matériels servant à acheminer les requêtes sur Internet et piraté le cœur même du réseau dans le cadre des programmes Quantum Insert pour la NSA et Tempora pour le GCHQ. Internet était un bien commun, la NSA et le GCHQ en ont fait une arme au service d'intérêts particuliers, bafouant au passage la liberté d'information, la liberté d'expression et le droit à la vie privée.

Les pratiques de surveillance massive de ces trois pays, dont certaines ont été révélées par le lanceur d'alerte Edward Snowden, sont d'autant plus intolérables qu'elles seront - et sont déjà - utilisées comme argument par des pays autoritaires tels que l'Iran, la Chine, le Turkménistan, l'Arabie Saoudite ou le Bahreïn pour justifier leurs propres atteintes à la liberté de l'information. Comment les Etats dits démocratiques pourraient-ils désormais s'ériger en donneurs de leçons quant à la protection des acteurs de l'information alors qu'ils adoptent les pratiques qu'ils dénoncent chez ces régimes anti-démocratiques ?

SOCIÉTÉS PRIVÉES ET COLLABORATIONS ENTRE ETATS

Dans la liste des Ennemis d'Internet 2014, on trouve également les « dealers de la surveillance » que sont les trois salons d'armement ISS World, Technology Against Crime et Milipol. Ces forums mettent en relation des sociétés spécialisées dans l'interception des communications ou le blocage de contenus en ligne avec des officiels et des représentants des gouvernements iranien, chinois, bahreïni, etc. Là encore, il convient de pointer le comportement ambivalent des démocraties occidentales : en 2013, TAC et Milipol étaient tous deux accueillis par la France. En décembre de la même année, cette dernière publiait pourtant un avis contraignant les sociétés françaises exportatrices de matériel de surveillance hors Union européenne à demander une autorisation auprès de la DGCIS (Direction générale de la compétitivité, de l'industrie et des services).

La censure et la surveillance par les institutions ennemies d'Internet ne seraient pas possibles sans les outils développés par les sociétés privées fréquentant les allées et les stands de ces salons. L'agence de sécurité des réseaux d'information (INSA) en Ethiopie a traqué des journalistes jusqu'aux Etats-Unis grâce à des logiciels espions fournis par la société italienne Hacking Team, désignée « Ennemi d'Internet » par Reporters sans frontières en 2013. La NSA elle-même a fait appel aux services de la société française Vupen spécialisée dans la découverte et l'exploitation de failles de sécurité.

Les entreprises privées ne sont pourtant pas les seules à équiper les pays Ennemis d'Internet en technologies de surveillance. La Russie a exporté son système de surveillance, SORM, chez ses proches voisins. Au Bélarus, le décret n°60 sur « les mesures à prendre pour améliorer l'utilisation du réseau national d'Internet » impose aux fournisseurs d'accès Internet l'installation de SORM.

L'Iran peine à créer son « Internet halal », un réseau national déconnecté du Web et placé sous le contrôle absolu des autorités. La Chine, passée maître dans le contrôle de l'information en ligne depuis l'édification de sa

«Grande Muraille électronique», vient à la rescousse des Gardiens de la révolution, du Conseil suprême du cyberespace et du Groupe de travail de détermination de contenus criminels. Cette collaboration a été annoncée par le vice-ministre de l'information iranien, Nasrolah Jahangiri, à l'occasion d'une visite du State Council Information Office de la République populaire de Chine.

Les élans pédagogiques de la Chine ne s'arrêtent pas là : le site d'information indépendant *Zambian Watchdog* a fait état en février 2013 de la collaboration des autorités zambiennes avec la Chine pour installer un système de surveillance du réseau Internet. Les blocages des sites Zambia Watchdog et Zambia Reports entre juin et juillet 2013 témoignent de la volonté de la Zambie de contrôler l'information en ligne.

La Chine est également présente en Ouzbékistan par l'intermédiaire de la société ZTE. Celle-ci, qui y a ouvert un bureau en 2003, est devenue le principal fournisseur du pays en modems et routeurs.

LA PROTECTION DU TERRITOIRE INSTRUMENTALISÉE

La NSA, le GCHQ, l'Agence de sécurité des réseaux d'information (INSA) en Ethiopie, l'Unité des services d'Internet (ISU) en Arabie Saoudite, le Centre analytique des opérations (OAC) au Bélarus, le FSB en Russie, le Service national de la sûreté et du renseignement (NISS) au Soudan sont autant d'agences de protection du territoire qui ont largement outrepassé leur mission originelle pour espionner ou censurer les acteurs de l'information.

Cette tendance à instrumentaliser la sécurité nationale pour justifier des atteintes aux libertés fondamentales se retrouve dans d'autres institutions que celles épinglées dans ce rapport. En Colombie, une cellule de surveillance numérique, vraisemblablement pilotée par le gouvernement, a intercepté plus de 2600 emails entre les porte-parole des Forces armées révolutionnaires de Colombie (FARC) et des journalistes internationaux.

En France, le Parlement a adopté fin 2013 à la hussarde, malgré les protestations de nombreuses organisations de défense de droits de l'Homme, la loi de programmation militaire. L'article 20 de cette loi autorise la surveillance des communications téléphoniques et Internet en temps réel, sans intervention d'un juge. Les motifs invoqués sont larges et évasifs et vont de la «recherche de renseignements intéressant la sécurité nationale» à «la sauvegarde des éléments essentiel du potentiel économique de la France» en passant par «la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous».

En Tunisie, Le 12 novembre 2013, le Journal officiel de la République tunisienne (JORT) annonçait la création de l'Agence technique des télécommunications (ATT). Cette agence, destinée à surveiller les communications dans le cadre des investigations judiciaires relatives aux "crimes d'information et de la communication" a aussitôt réveillé les inquiétudes. Son apparition brutale, par décret, et sans concertation avec la société civile, ravive le souvenir de l'ATI, symbole de la censure sous Zine El-Abidine Ben Ali. L'absence de gardes fous et de mécanisme de contrôle prévus pour encadrer les activités de cette agence est inquiétante.

UN MONOPOLE DANGEREUX DES INFRASTRUCTURES

Au Turkménistan, en Syrie, au Vietnam ou au Bahreïn, la mainmise des autorités sur les infrastructures du réseau facilite le contrôle de l'information en ligne. En Syrie ou en Iran, le débit de la bande passante est régulièrement ralenti pour empêcher la diffusion d'images de manifestations.

Des solutions plus drastiques sont parfois employées : en novembre 2012, les autorités syriennes ont coupé les réseaux Internet et téléphoniques pendant plus de 48 heures. En Chine le 22 janvier 2014, pour bloquer la révélation d'un scandale financier éclaboussant les élites chinoises, les autorités ont coupé Internet pendant plusieurs heures. Au Soudan, le 25 septembre 2013, pour empêcher l'organisation de manifestations via les réseaux sociaux, les autorités ont coupé le réseau dans tout le pays pendant 24 heures.

LES INTERMÉDIAIRES TECHNIQUES ENRÔLÉS PAR LES CENSEURS

Les autorités demandent de plus en plus souvent aux intermédiaires techniques, fournisseurs d'accès et hébergeurs, de jouer les gendarmes du Net.

Certains cas extrêmes sombrent dans le ridicule, comme en Somalie où la milice islamiste Al-Shabbaab a déclaré illicite l'usage d'Internet en janvier 2013. La milice ne disposant ni des compétences ni des capacités techniques pour couper Internet, elle a intimé l'ordre aux fournisseurs d'accès de mettre un terme à leurs services sous quinze jours. Ironie de l'histoire, cette mesure, afin d'être portée à la connaissance de la population, a été mise en ligne sur des sites Internet favorables aux « shebab » (les jeunes).

Plus insidieux, en France, les lois sur l'égalité homme-femme et la lutte contre la prostitution ont contribué à augmenter la responsabilité des intermédiaires techniques dans le filtrage des contenus après notification. L'article 17 du projet de loi sur l'égalité femmes-hommes oblige les fournisseurs d'accès à Internet et les hébergeurs à identifier et à signaler tout contenu incitant ou provoquant à la haine sur une base sexiste, handiphobe ou homophobe.

Au Venezuela, le président Nicolás Maduro a obligé les FAI à filtrer des informations jugées sensibles. Elles ont été sommées de bloquer une cinquantaine de sites qui traitaient du taux de change et de l'inflation galopante, des thèmes contribuant à alimenter la « guerre économique » contre le pays. Ce qui n'a pas empêché de multiples mouvements contestataires de se développer face aux déséquilibres économiques et aux problèmes d'insécurité. Vendredi 24 février 2014, alors que de nombreuses photos des manifestations circulaient sur Twitter, les autorités vénézuéliennes ont à nouveau ordonné aux fournisseurs d'accès de bloquer le service d'images du réseau social Twitter.

En Turquie, les derniers amendements à la loi n°5651 sur Internet, votés le 5 février 2014, ont transformé les FAI en véritables instruments de censure et de surveillance. Ces amendements visent à les réunir au sein d'une nouvelle structure censée centraliser les demandes de blocage et de retrait de contenu. Les FAI n'auront d'autre choix que d'y adhérer et de mettre en place les outils de surveillance imposés par les autorités, sous peine de mettre la clé sous la porte. Le projet de loi impose également aux intermédiaires techniques de conserver des données de connexion des internautes pour une durée de un à deux ans. Ils devront les transmettre aux autorités compétentes sur simple demande. Le texte ne précise pas quelles données devront être fournies, sous quelle forme, ni quel usage en sera fait. D'après les experts, il serait question de l'historique des sites et réseaux sociaux visités, des recherches effectuées, des adresses IP, voire des titres des emails.

CADRES JURIDIQUES LIBERTICIDES

Le cadre juridique constitue souvent le premier outil pour museler l'information en ligne.

Au Vietnam, en plus des articles 88 et 79 du Code pénal, le ministère de l'Information et des Communications n'hésite pas à légiférer afin de créer un cadre législatif toujours plus répressif. Ainsi, le décret 72, en vigueur depuis le 1er septembre 2013, définit une utilisation extrêmement restrictive des blogs et des réseaux sociaux puisqu'il limite leur utilisation à la « diffusion » ou au « partage » d'informations « personnelles », interdisant aux internautes d'aborder des sujets d'actualité ou d'intérêt général.

En juillet 2013, la **Gambie** s'est dotée d'un nouvel outil législatif avec l'ajout de nouveaux amendements à la législation principale qui définit les limites de la liberté de l'information. Ceux-ci prévoient jusqu'à 15 ans d'emprisonnement ou une amende de 3 millions de dalasis (64 000 euros) pour « la diffusion de fausses nouvelles concernant le gouvernement de la Gambie ou ses fonctionnaires ».

Au **Bangladesh**, la loi sur les crimes numériques adoptée en 2006 et amendée en août 2013 a permis l'inculpation de cinq personnes, dont quatre blogueurs et le secrétaire général de l'ONG Odhika. L'interprétation des « crimes numériques » est extrêmement large et imprécise puisque cette loi y inclut la « publication en ligne d'informations fallacieuses ou à caractère obscène ou diffamatoire ».

A **Grenade**, une récente loi sur les crimes électroniques interdit l'utilisation de « systèmes électroniques » pour publier des « informations grossièrement offensantes ou ayant un caractère menaçant ». Là encore, des motifs vagues et imprécis constituent une réelle menace pour la liberté de l'information.

PERMIS DE PUBLIER

La mise en place de licences pour les sites d'information est également une pratique courante pour contrôler l'information en ligne.

A **Singapour**, en juin 2013, les autorités ont mis en place une véritable barrière économique pour les médias en ligne. Les sites recevant plus de 50 000 visiteurs mensuels et publiant plus d'un article par semaine sur le pays doivent acquérir une licence individuelle facturée 50 000 SGD (29 000 euros) et renouvelable tous les ans.

Depuis 2007, en **Ouzbékistan**, les sites d'information sont assimilés aux autres types de médias et ont l'obligation de s'enregistrer auprès des autorités. La procédure d'enregistrement est arbitraire et l'accréditation soumise à un examen du contenu.

En **Arabie Saoudite**, depuis 2001, les sites de médias traditionnels doivent demander une licence auprès du ministère de l'Information et de la Culture. Celle-ci doit être renouvelée tous les trois ans.

Ce tour de la censure et de la surveillance sur Internet est loin d'être exhaustif. Il est fort probable que les documents d'Edward Snowden, feuilletonnés depuis juin 2013 par le journaliste Glenn Greenwald, nous apprendront l'existence d'autres pratiques au cours des mois à venir. La dernière en date, et peut-être la plus scandaleuse, l'existence d'un programme Optic Nerve destiné à capturer les images de webcams de millions d'internautes utilisateurs des services de Yahoo, semble démontrer la totale absence de limites des agences de renseignement.

Quels sont alors les axes de riposte possibles pour préserver la liberté de l'information en ligne ? Il est essentiel :

- d'agir au niveau des institutions internationales pour renforcer le cadre juridique relatif à la surveillance d'Internet, à la protection des données et à l'exportation de matériel de surveillance informatique (lire les recommandations de Reporters sans frontières)

- de former les acteurs de l'information à la protection de leurs données et communications ; Reporters sans frontières s'est engagée sur ce terrain depuis plusieurs années et organise des ateliers de sensibilisation en France, en Suisse, en Egypte, en Tunisie, en Turquie, en Thaïlande, en Afghanistan, au Tadjikistan, etc.

- de continuer à informer sur les pratiques de surveillance et de censure. C'est tout l'objet de ce rapport.

RECOMMANDATIONS

La censure et la surveillance d'Internet ont des incidences directes sur l'exercice des droits fondamentaux. La liberté d'expression en ligne facilite le libre débat sur des sujets d'intérêt général, ainsi que le développement, la bonne gouvernance et le respect des garanties démocratiques. Ainsi, le 5 juillet 2012, le Conseil des droits de l'homme de l'ONU a affirmé que les droits en vigueur dans le monde physique doivent être reconnus également sur Internet, indépendamment des frontières. La résolution appelle les Etats« à promouvoir et à faciliter l'accès à Internet et la coopération internationale visant à faciliter le développement des médias et des communications dans tous les pays ».

Dans les faits, la surveillance des réseaux continue de s'amplifier. Elle permet d'identifier les internautes et leurs contacts, de lire leur correspondance, de les localiser. Dans les pays répressifs, cette surveillance entraîne l'arrestation et les mauvais traitements de défenseurs des droits de l'homme, de journalistes, de net-citoyens et d'autres acteurs de la société civile. La lutte pour les droits de l'homme a basculé en ligne, et les prisons sont de plus en plus peuplées de dissidents dont les communications sur Internet ont été interceptées par les autorités.

Au niveau international et régional, au sein des Nations unies comme de l'Union européenne et dans la plupart des législations nationales, le cadre juridique relatif à la surveillance d'Internet, à la protection des données et à l'exportation de matériel de surveillance informatique est à ce jour incomplet et insuffisant au regard des normes et standards internationaux de protection des droits de l'homme. Dès lors, l'adoption d'un cadre juridique protecteur des libertés sur Internet est primordiale, tant pour la question générale de la surveillance d'Internet que du problème particulier des entreprises exportatrices de matériel de surveillance.

SURVEILLANCE D'INTERNET

RSF rappelle

- Que le droit à la vie privée est consacré internationalement dans la Déclaration universelle des droits de l'homme (art. 12), dans le Pacte international relatif aux droits civils et politiques (art. 17) ainsi que dans la Convention Européenne des droits de l'homme (art. 8) et la Convention américaine des droits de l'homme (art. 11)
- Que le rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression des Nations Unies, Frank La Rue, consacré à la surveillance témoigne de l'impact de cette dernière sur les droits de l'homme en général et la liberté d'information en particulier

- Que les 13 principes internationaux sur l'application des droits humains à la surveillance des communications, élaborés avec les ONG Access, EFF et Privacy International et un groupe d'expert internationaux, et qui ont pour objectif de créer un cadre de référence pour la société civile, les entreprises et les États, afin que la législation et les pratiques en matière de surveillance en vigueur dans chaque pays respectent les droits de l'homme, ont reçu le soutien de plus de 360 organisations dans 70 pays. Ils peuvent être soutenus sur le site thedaywefightback.

RSF recommande

Aux Nations unies

- De réfléchir à la mise en place d'**un groupe de travail sur les libertés numériques**, rattaché au Conseil des droits de l'homme, chargé de réunir toutes les informations concernant les libertés numériques, la surveillance d'Internet, la protection de la vie privée en ligne, la censure et les autres atteintes aux libertés numériques dans les Etats membres, ainsi que toutes les informations concernant des cas individuels de violation des libertés numériques, et de faire des recommandations aux Etats.

A l'Union européenne

- D'inclure l'accès libre à l'Internet de garantir les liberté numériques dans la Charte des droits fondamentaux de l'UE
- D'intégrer la promotion et la protection de la liberté numérique dans l'ensemble des actions extérieures et des politiques et instruments de financement de l'Union, notamment ses programmes de développement et d'aides, comme les négociations relatives aux accords de libre-échange (ALE)
- De conditionner l'aide au développement au respect des libertés numériques
- D'insister sur l'importance de la liberté de l'accès à Internet et des libertés numériques dans les critères d'adhésion à l'UE (critères de Copenhague), et de renforcer le suivi du respect de ces critères
- De considérer, dans les relations entre membres de l'UE et avec les États tiers ainsi que dans les instances internationales, notamment l'OMC, les mécanismes de surveillance d'Internet comme des mécanismes protectionnistes et des barrières aux échanges, et de les combattre comme tels.

Aux États

- D'inclure l'accès libre à Internet et la garantie des libertés numériques dans les droits fondamentaux
- D'adopter des lois garantissant les libertés numériques, notamment la protection de la vie privée et des données personnelles face aux intrusions des forces de l'ordre ou des services de renseignement, et de mettre en place des mécanismes de recours appropriés

- De s'assurer que les mesures de surveillance des communications respectent strictement les principes de légalité, de nécessité et de proportionnalité conformément à l'article 19 du Pacte international relatifs aux droits civils et politiques
- De favoriser une plus grande transparence quant aux demandes de surveillance qu'elles adressent aux entreprises, leur nombre, leurs bases légales, et leurs objectifs.

ENTREPRISES ET DROITS DE L'HOMME

Reporters sans frontières a dénoncé à plusieurs reprises la coopération criminelle de certaines entreprises des nouvelles technologies avec des régimes autoritaires. Elles fournissent aux dictatures des logiciels de surveillance des communications qui permettent aux forces de l'ordre et aux services de renseignement d'espionner, voir d'arrêter dissidents et opposants. Fin février 2014, au moins 167 net-citoyens étaient emprisonnés à travers le monde pour leurs actions d'information. Les entreprises qui collaborent avec ces gouvernements doivent être sanctionnées et les Etats doivent mettre en place des législations à même de contrôler les exportations de matériel de surveillance informatique et de poursuivre les entreprises qui se livrent à ce commerce.

RSF rappelle

- Les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, approuvés à l'unanimité par le Conseil des droits de l'homme en 2011
- Les actions permanentes de RSF auprès des Etats et des Nations unies et ses diverses interventions sur le thème de la surveillance, notamment sa soumission écrite au second Forum des Nations unies intitulé« Business and human rights », qui s'est tenu du 2 au 4 décembre 2013 à Genève
- La *Position de principe* de RSF de novembre 2012, relative à l'exportation de technologies de surveillance européennes
- Ses nombreuses alertes et communiqués sur le sujet, depuis le début des années 2000, et en particulier en 2011 : « *Des sanctions doivent s'appliquer aux entreprises qui coopèrent avec les dictatures* »
- Les rapports de diverses instances et organes, tel le Groupe de travail des Nations Unies sur la question des droits de l'homme et des sociétés transnationales, notamment celui du 14 mars 2013, ou celui du 24 octobre 2013 « *Entreprises et droits de l'homme : avis sur les enjeux de l'application par la France des Principes directeurs des Nations unies* » de la Commission nationale consultative des droits de l'homme (CNCDH).
- Son engagement au sein d'une coalition internationale, **The Cause** (Coalition Against Unlawful Surveillance Exports), contre l'export illégal

de technologies de surveillance aux côtés d'ONG telles qu'Amnesty International, Human Rights Watch, Privacy International ou Digitale Gesellschaft.

RSF recommande

Aux Nations unies :

- De **renforcer le mandat du Groupe de travail des Nations unies** « Droits de l'homme et société transnationales », notamment en l'habilitant à recevoir des plaintes individuelles et à enquêter sur les cas individuels de violations des droits de l'homme liées à des entreprises

- De réfléchir à l'élaboration d'**une convention internationale relative à la responsabilité des entreprises en matière de droits de l'homme**, reprenant et approfondissant les Principes directeurs des Nations unies

- De réfléchir à l'élaboration d'une **convention internationale relative à l'exportation de technologies de surveillance de l'Internet**, permettant un contrôle des exportations et de la fourniture de technologies liberticides et dangereuses pour les net-citoyens, instaurant un organe de surveillance et de vigilance indépendant des Etats et prévoyant des sanctions dissuasives. Cette convention doit établir des règles permettant d'interdire l'exportation, dès lors qu'il existe un risque substantiel que ces matériels servent à commettre ou à faciliter des violations graves des droits de l'homme.

Aux Etats participants à l'Arrangement de Wassenaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage :

RSF se félicite de la prise en compte par l'Arrangement de Wassenaar de deux nouvelles catégories de technologies de surveillance, qui ont été incluses dans la liste de contrôle des biens et technologies à double usage : les « logiciels d'intrusion » et les« systèmes de surveillance du réseau IP ». Cependant, RSF considère opportun de recommander, à l'attention des Etats participant à l'Arrangement :

- De favoriser une plus grande transparence et un meilleur accès de la société civile et des Institutions nationales des droits de l'homme (INDH) au sein des délibérations de l'Assemblée plénière de l'Arrangement
- De réfléchir à la mise en place de règles contraignantes quant à l'export ou au transfert de technologies à double usage vers certains pays, valables pour tous les Etats participants, de façon uniforme
- De renforcer les obligations pesant sur les États, notamment en matière de surveillance du respect de l'obligation de notification pesant sur les exportateurs.
- A l'Union européenne :
- De mettre en place au niveau européen un mécanisme renforcé de contrôle de l'exportation des technologies de surveillance

- De considérer certains systèmes et services ciblés de brouillage, de surveillance, de contrôle et d'interception comme des biens à usage unique dont l'exportation doit être soumise à autorisation préalable
- D'assurer l'harmonisation et l'uniformisation des procédures et sanctions visant la surveillance et le contrôle des technologies de surveillance.

Aux États :

- De contrôler de façon plus rigoureuse les exportations de matériel de surveillance d'Internet, notamment vers les zones de conflit armé et les États ne respectant pas les libertés fondamentales
- D'amender la législation en vigueur et de renforcer les mécanismes de recours, notamment
- Par l'introduction de dispositions relatives à la responsabilité pénale des entreprises en cas de collaboration avec des régimes coupables de violations des droits de l'homme
- Par l'inscription dans la loi d'une obligation de« diligence raisonnable » en matière de droits de l'homme aux entreprises ; doit en découler une obligation de vigilance de l'Etat qui accueille le siège de ces entreprises en tant que garant de ses obligations internationales
- Par l'introduction dans la loi, pour lutter contre l'impunité et assurer l'effectivité des mécanismes judiciaires nationaux, d'une extension aux droits de l'homme de l'exception au principe d'autonomie des sociétés, afin de permettre une responsabilisation des sociétés-mères pour des actes commis par leurs filiales à l'étranger
- Par l'extension des compétences extraterritoriales des juridictions pénales nationales. Celles-ci devraient pouvoir se reconnaître compétentes à l'égard de certains délits commis à l'étranger par une entreprise.

Aux entreprises :

- De respecter les droits de l'homme internationalement reconnus
- D'adopter des chartes éthiques et des mécanismes de traçabilité efficaces
- De mettre en place des mécanismes d'information et de sensibilisation des personnels à la thématique des droits de l'homme
- De formuler des engagements relatifs au respect des Principes directeurs des Nations unies, notamment de faire preuve de diligence raisonnable en matière de droits de l'homme et de transparence
- De prévoir des mécanismes de réparation quand leurs activités ont eu des incidences négatives sur les droits de l'homme.

Directrice de la recherche
Lucie Morillon
lucie.morillon@rsf.org

Responsable du bureau Afrique
Cléa Kahn-Sriber
afrique@rsf.org

Responsable du bureau Asie
Benjamin Ismaïl
asie@rsf.org

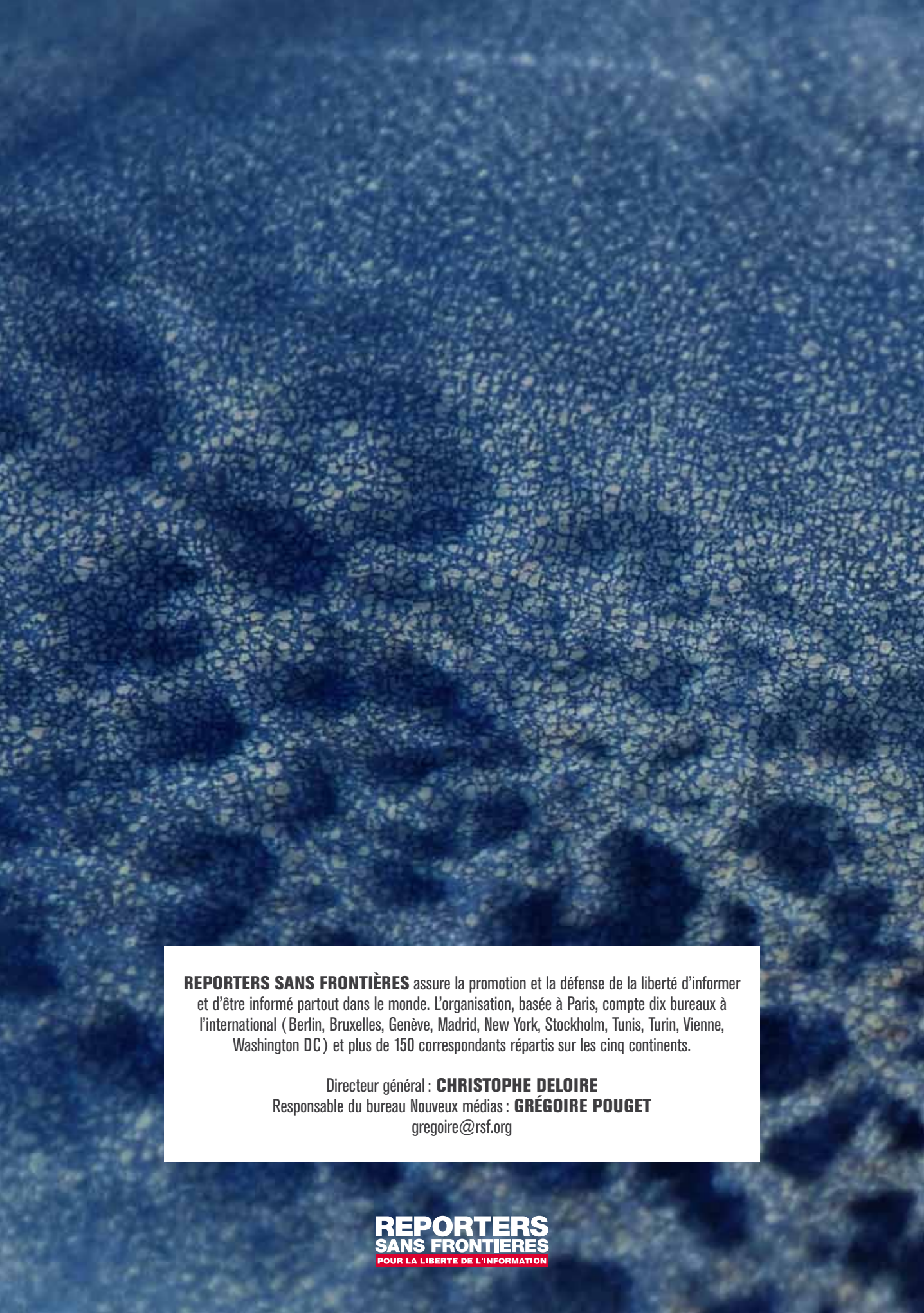
Responsable du bureau Europe centrale et Europe de l'Est
Johann Bihr
europe@rsf.org

Responsable du bureau Maghreb & Moyen-Orient
Soazig Dollet
moyen-orient@rsf.org

Responsable du bureau Amériques
Camille Soulier
ameriques@rsf.org

Responsable du bureau Persan
Reza Moini
persan@rsf.org

Responsable du bureau Union européenne et Balkans
Antoine Héry (+33 1 44 83 84 65)
ue@rsf.org



REPORTERS SANS FRONTIÈRES assure la promotion et la défense de la liberté d'informer et d'être informé partout dans le monde. L'organisation, basée à Paris, compte dix bureaux à l'international (Berlin, Bruxelles, Genève, Madrid, New York, Stockholm, Tunis, Turin, Vienne, Washington DC) et plus de 150 correspondants répartis sur les cinq continents.

Directeur général : **CHRISTOPHE DELOIRE**
Responsable du bureau Nouveux médias : **GRÉGOIRE POUGET**
gregoire@rsf.org

REPORTERS
SANS FRONTIERES
POUR LA LIBERTE DE L'INFORMATION