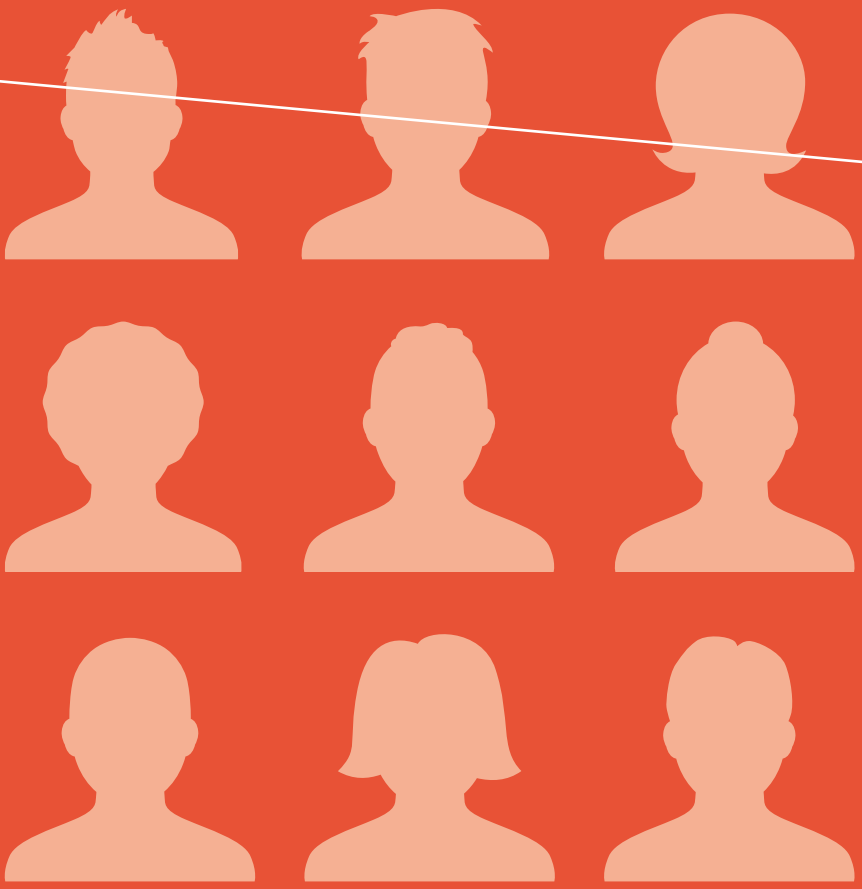
ARTICLE 19



Le droit à l'anonymat en ligne

Mai 2015

Document D'Orientation

ARTICLE 19
Free Word Centre
60 Farringdon Road
London,
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

ISBN: 978-1-910793-19-0

Résumé

L'anonymat et le chiffrement ne sont pas des phénomènes nouveaux : l'anonymat facilite depuis longtemps l'expression d'idées controversées et la dissidence dans de nombreux pays du monde ; l'usage de messages chiffrés et de codes pour protéger le caractère privé des communications a une histoire tout aussi longue.

La protection de l'anonymat est une composante vitale de la protection tant du droit à la liberté d'expression que du droit au respect de la vie privée. L'anonymat permet à des individus de s'exprimer sans crainte de représailles, et il est particulièrement important dans les pays où la liberté d'expression est lourdement censurée. Il permet aux lanceurs d'alerte de se manifester et aux individus de révéler leurs préoccupations les plus profondes sur de multiples questions dans les espaces de discussion en ligne. Il permet également à des usagers de se joindre à tous types de discussions qu'ils pourraient, sinon, être tentés d'éviter.

Des gouvernements à travers le monde tentent régulièrement de restreindre l'anonymat et l'usage d'outils de chiffrement pour diverses raisons, telles que leur utilisation potentielle pour des activités illégales ou terroristes.

La nécessité de protéger l'anonymat et le chiffrement dans le droit international est par conséquent plus importante que jamais.

Dans ce document de synthèse, élaboré initialement en tant que contribution au rapport sur l'anonymat et le chiffrement du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, ARTICLE 19 cherche à démontrer les enjeux de l'anonymat et du chiffrement pour le droit à la liberté d'expression à l'ère du numérique. Nous identifions également comment l'anonymat en ligne et le chiffrement sont protégés par le droit international, et nous analysons quelles restrictions des outils d'anonymat et de chiffrement sont compatibles avec le droit à la liberté d'expression. Nous concluons par des recommandations sur la meilleure manière de protéger l'anonymat et le chiffrement en ligne.

Recommandations clés

- Les Etats devraient explicitement reconnaître dans leur législation nationale et garantir dans la pratique que le droit à la liberté d'expression inclut le droit à l'anonymat ;
- Les Etats devraient également reconnaître le droit au discours anonyme, le droit à la lecture anonyme, et le droit de naviguer en ligne anonymement ;
- Les Etats devraient abroger toutes les lois, réglementations et politiques qui exigent un enregistrement sous une véritable identité, lesquelles constituent une violation des droits à la liberté d'expression et au respect de la vie privée ;
- Les médias sociaux et les sites d'information ne devraient pas exiger la mise en place de régimes d'enregistrement sous une véritable identité, mais au minimum, garantir que l'anonymat est une option véritable ;
- Les Etats devraient adopter des lois, des réglementations et des politiques qui confèrent à des tribunaux plutôt qu'à des autorités chargées du maintien de l'ordre, le pouvoir de restreindre le droit à l'anonymat ;
- Toute restriction de l'anonymat et du chiffrement doit respecter pleinement les critères du triple test relatif aux restrictions de la liberté d'expression, et devrait être soumise à de solides garanties procédurales ;
- Les Etats et les entreprises devraient promouvoir l'usage d'outils tels que le logiciel Tor et le protocole https:// qui permettent de naviguer sur Internet anonymement ;
- Les Etats devraient reconnaître dans leur législation et dans leurs pratiques que le chiffrement est une exigence fondamentale pour la protection de la confidentialité et de la sécurité de l'information, et qu'en tant que tel, il est essentiel à la protection du droit à la liberté d'expression en ligne.

- Les Etats devraient abroger et s'abstenir d'adopter des lois qui requièrent une autorisation du gouvernement pour utiliser des produits cryptographiques;
- Les Etats devraient abroger ou s'abstenir d'adopter des lois qui requièrent le décryptage de données cryptées ou la divulgation de clés de cryptage dans toutes circonstances autres que sur injonction d'un tribunal ;
- Les Etats devraient s'abstenir d'adopter des mesures qui requièrent ou promeuvent l'installation de « trappes » (*backdoors*) dans des logiciels et/ou des produits de cryptographie ;
- Les Etats devraient lever les restrictions excessives sur l'importation/exportation de logiciels et produits de cryptographie ;
- Les Etats devraient abolir ou s'abstenir d'adopter des systèmes de séquestre de clés ;
- Les entreprises devraient s'abstenir d'affaiblir les standards techniques et devraient mettre en place des services de cryptage de bout en bout ;
- Les Etats et les entreprises devraient mettre en place des programmes pour la promotion du chiffrement dans les communications sur Internet ;
- Les Etats et les entreprises devraient promouvoir le cryptage de bout en bout en tant que standard de base pour la protection du droit à la vie privée en ligne. Ils devraient également promouvoir l'usage de logiciels ouverts et investir dans ce domaine afin qu'ils soient entretenus de manière régulière et indépendante, et contrôlés pour détecter les vulnérabilités.

Table of contents

Introduction

L'anonymat et le chiffrement ne sont pas des phénomènes nouveaux : l'anonymat facilite depuis longtemps l'expression d'idées controversées et la dissidence dans de nombreux pays du monde ; l'usage de messages chiffrés et de codes pour protéger le caractère privé des communications a une histoire tout aussi longue.

La protection de l'anonymat est une composante vitale de la protection tant du droit à la liberté d'expression que du droit au respect de la vie privée. L'anonymat permet à des individus de s'exprimer sans crainte de représailles, et il est particulièrement important dans les pays où la liberté d'expression est lourdement censurée. Il permet aux lanceurs d'alerte de se manifester et aux individus de révéler leurs préoccupations les plus profondes sur de multiples questions dans les espaces de discussion en ligne. Il permet également à des usagers de se joindre à tous types de discussions qu'ils pourraient, sinon, être tentés d'éviter.

Toutefois, l'anonymat présente aussi des inconvénients : il peut être utilisé par des individus mal intentionnés dans des activités criminelles ou d'autres types d'actes répréhensibles tels que le harcèlement ou les intimidations en ligne.

Des gouvernements à travers le monde tentent régulièrement de restreindre l'anonymat et l'usage d'outils de cryptage pour des raisons multiples. Par exemple :

- En Chine, le gouvernement a bloqué les réseaux privés virtuels (*Virtual Private Networks - VPN*) qui permettent à ses citoyens de contourner les pare-feux nationaux.

- Aux Etats-Unis, l'anonymat a été fustigé en tant qu'outil facilitant des activités illégales.[1]

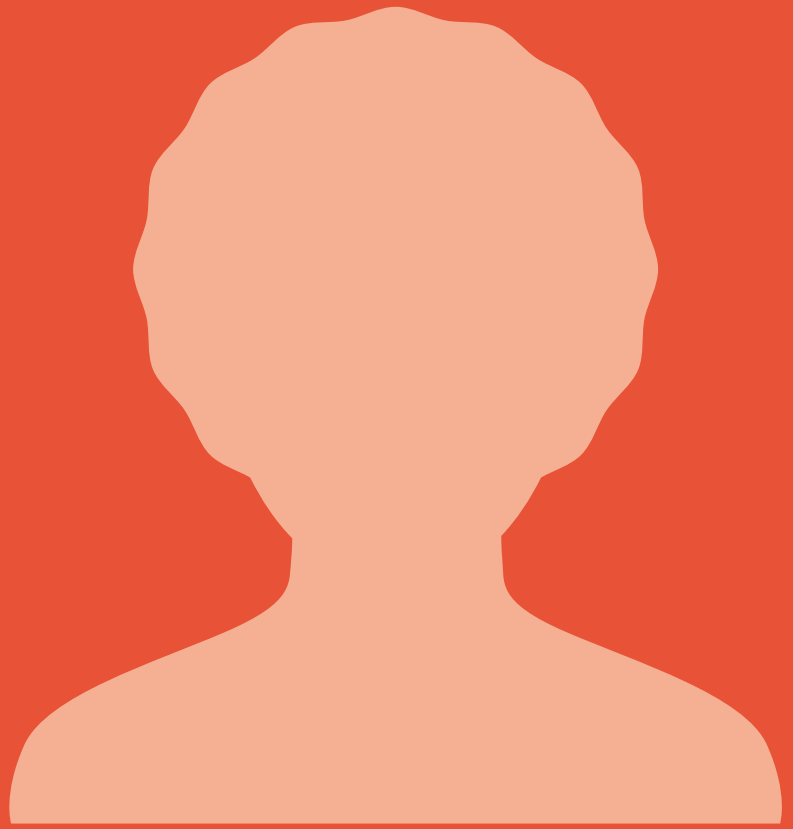
- A la suite des attaques contre *Charlie Hebdo* en janvier 2015, plusieurs gouvernements occidentaux ont appelé à prendre des mesures susceptibles d'entraver gravement l'usage à la fois de l'anonymat et du chiffrement, des mesures qui – en retour – porteraient atteinte au droit à la liberté d'expression et au respect de la vie privée en ligne. Le premier ministre britannique David Cameron a appelé à interdire le chiffrement des communications en ligne,[2] tandis que le gouvernement français cherche des moyens de renforcer la surveillance sur l'Internet.[3]

La protection accordée à l'anonymat et au chiffrement dans la législation et dans les pratiques est par conséquent plus importante que jamais.

En mai 2015, le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression (Rapporteur spécial sur la liberté d'expression) a publié un rapport tout à fait innovant sur l'anonymat et le chiffrement en ligne. Le rapport affirme que les tentatives par les gouvernements d'accéder aux communications des individus ou d'affaiblir sciemment les standards de cryptage constituent une violation du droit international. ARTICLE 19 a soumis des commentaires lors de consultations sur ce rapport, et proposé diverses recommandations sur les implications de l'anonymat et du chiffrement en ligne pour le droit à la liberté d'expression à l'ère du numérique.[4]

Dans ce document de synthèse, ARTICLE 19 élabore dans le détail une première proposition préparée en réponse au rapport du Rapporteur spécial. Nous identifions également les moyens par lesquels l'anonymat et le chiffrement en ligne sont protégés dans le droit international et analysons dans quelle mesure certaines restrictions des outils de chiffrement et d'anonymat sont compatibles avec le droit à la liberté d'expression. Nous concluons ce document avec quelques recommandations sur le meilleur moyen de protéger l'anonymat et le chiffrement en ligne.

Section I: Anonymat



Section I: Anonymat

Considérations d'ordre général

L'anonymat est un concept essentiel de la protection de la liberté d'expression ainsi que du droit au respect de la vie privée. Dans sa forme la plus simple, l'anonymat est *le fait* de ne pas être identifié et, dans ce sens, il relève de l'expérience quotidienne ordinaire de la plupart des individus, par ex. marcher au sein d'une foule ou faire la queue parmi des étrangers. De ce fait, une activité peut être anonyme tout en étant publique.

Dans certains contextes – notamment le vote à bulletin secret, le discours politique,[5] l'expression artistique et la protection des sources journalistiques[6] –, l'anonymat est depuis longtemps reconnu comme une garantie importante pour la protection de l'exercice des droits fondamentaux. Cependant, avec la progression des technologies numériques, il est devenu clair que l'importance de l'anonymat (y compris l'usage de pseudonymes) ne pouvait se limiter à ces seules sphères d'activité. Dans ce sens, l'anonymat protège non seulement la liberté des individus de communiquer des informations et des idées qu'ils pourraient sinon s'abstenir d'exprimer ou être dans l'incapacité de diffuser, mais il protège aussi la liberté des individus de vivre leur vie sans faire l'objet d'un contrôle inutile ou disproportionné.

Le droit à l'anonymat en ligne dans le droit international

A ce jour, le droit à l'anonymat en ligne n'a été reconnu que partiellement dans le droit international. Traditionnellement, la protection de l'anonymat en ligne a été liée à la protection du droit au respect de la vie privée et à la protection des données à caractère personnel :

- En mai 2015, le Rapporteur spécial sur la liberté d'expression a publié son rapport annuel sur le chiffrement et l'anonymat à l'ère du numérique. Le rapport a mis en lumière les problèmes suivants, en particulier :
  - Le Rapporteur spécial a clairement affirmé qu'un Internet ouvert et sécurisé devrait compter parmi les conditions préalables à la jouissance de la liberté d'expression aujourd'hui, et devrait de ce fait être protégé par les gouvernements. Le chiffrement et l'anonymat doivent être fortement protégés et promus car ils fournissent la protection de la vie privée et la sécurité nécessaires à l'exercice significatif du droit à la liberté d'expression et d'opinion à l'ère du numérique ;[7]
  - Le Rapporteur spécial a souligné que le discours anonyme est nécessaire pour les défenseurs des droits humains, les journalistes, et les manifestants. Il a noté que toute tentative d'interdire ou d'intercepter des communications anonymes durant des manifestations était une restriction injustifiée du droit à la liberté de réunion pacifique en vertu de la *Déclaration universelle des droits de l'homme* (DUDH) et du *Pacte international relatif aux droits civils et politiques* (PIDCP).[8] Il a également recommandé que la législation et les réglementations qui protègent les défenseurs des droits humains et les journalistes comprennent des dispositions qui autorisent l'accès à, et fournissent un soutien à l'usage de, technologies qui sécuriseraient leurs communications ;

- Il a également souligné que les restrictions du chiffrement et de l'anonymat doivent respecter le test en trois parties des limites au droit à la liberté d'expression en vertu du droit international. Le Rapporteur spécial a recommandé que les projets de loi et les politiques régissant les restrictions au chiffrement et à l'anonymat fassent l'objet de commentaires de la part du public et soient adoptées uniquement après une procédure législative habituelle – et non une procédure accélérée. Il a également souligné que de fortes garanties procédurales et judiciaires devraient être appliquées pour garantir le droit à un procès équitable pour tout individu dont l'usage du chiffrement et de l'anonymat est soumis à des restrictions ;[9]

- Le Rapporteur spécial a déclaré que les interdictions générales d'utiliser individuellement des technologies de chiffrement restreignent de manière disproportionnée le droit à la liberté d'expression. Il a également noté que les règles (a) requérant des licences pour l'utilisation de chiffrement ; (b) établissant des standards techniques faibles pour le chiffrement ; et (c) imposant le contrôle de l'import/export d'outils de chiffrement, équivalaient à une interdiction générale et constituaient de ce fait une restriction disproportionnée de la liberté d'expression ;[10]

- Le Rapporteur spécial a également noté que l'accès par des « trappes » (*backdoors*) aux communications des individus par les gouvernements, les systèmes de séquestre de clés (permettant un accès potentiel d'une tierce partie à des clés de cryptographie), et l'affaiblissement délibéré des standards de chiffrement, constituent des restrictions disproportionnées du droit à la liberté d'expression et du droit au respect de la vie privée. En particulier, il a souligné que les gouvernements qui proposent un accès par des « trappes » n'avaient pas fourni de preuves que l'usage criminel ou terroriste du chiffrement constitue un obstacle insurmontable aux objectifs des autorités chargées du maintien de l'ordre. En vertu du droit international, les Etats sont contraints de prouver, publiquement et de manière transparente, que d'autres moyens moins intrusifs (tels que des écoutes téléphoniques, une surveillance physique, et bien d'autres) sont indisponibles ou ont échoué, et que seules des mesures très intrusives, comme les « trappes », peuvent atteindre le même objectif. Les systèmes de séquestre de clés constituent également une menace pour l'exercice du droit à la liberté d'expression. En effet le rôle accordé aux tierces parties dans la protection des clés de chiffrement en sécurité, et le risque qu'elles soient contraintes de les donner à d'autres, représentent une source inhérente de vulnérabilité ;[11]

-

- Le Rapporteur spécial a également jugé que les interdictions générales de l'anonymat en ligne, et l'enregistrement obligatoire sous une véritable identité ou de la carte SIM, vont bien au-delà de ce qui est permis en vertu du droit international ; au contraire, il a noté que du fait que l'anonymat facilite considérablement l'expression et l'opinion en ligne, les Etats devraient le protéger et, en général, ne pas restreindre les technologies qui le rendent possible.[12]

- Le rapport reconnaît aussi le rôle des entreprises dans la protection et la promotion de standards de chiffrement solides. En particulier, les entreprises sont invitées à analyser comment leurs propres politiques restreignent le chiffrement et l'anonymat.

- Le rapport 2013 du Rapporteur spécial sur la liberté d'expression a mis en lumière le lien important entre le droit au respect de la vie privée et le droit à la liberté d'expression dans le cyberespace.[13] Le rapport observait également que les restrictions de l'anonymat facilitent la surveillance des communications par les Etats et ont un effet paralysant sur l'expression libre d'informations et d'idées.[14]

- Plusieurs instruments qui ont émergé dans ce domaine proviennent à l'origine du Conseil de l'Europe et de l'Union européenne.[15] Par exemple, le Comité des ministres du Conseil de l'Europe a adopté la *Déclaration sur la liberté de la communication sur l'Internet* en mai 2003. Le Principe 7 relatif à l'anonymat stipule que :

  Afin d'assurer une protection contre les surveillances en ligne et de favoriser l'expression libre d'informations et d'idées, les Etats membres devraient respecter la volonté des usagers de l'Internet de ne pas révéler leur identité. Cela n'empêche pas les Etats membres de prendre des mesures et de coopérer pour retrouver la trace de ceux qui sont responsables d'actes délictueux, conformément à la législation nationale, à la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales et aux autres traités internationaux dans le domaine de la justice et de la police.[16]

– Dans sa jurisprudence, la Cour européenne des droits de l'homme (Cour européenne) a reconnu l'importance de l'anonymat pour le droit à la liberté d'expression et le droit au respect de la vie privée. Dans le même temps, la Cour a bien spécifié que l'anonymat n'était pas absolu et qu'il pouvait être limité afin de protéger d'autres intérêts légitimes, en particulier la protection des groupes vulnérables.[17] Plus spécifiquement, la Cour a déclaré que l'anonymat et la confidentialité sur Internet ne doivent pas conduire les Etats à refuser de protéger les droits des victimes potentielles, en particulier lorsque des personnes vulnérables sont concernées :[18]

> (…) si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales, et si les utilisateurs des télécommunications et des services internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue et doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui.

La Cour européenne a exprimé un point de vue similaire dans l'affaire *Delfi c. Estonie*[19] lorsqu'elle a observé que :

> [C]onsciente de l'importance du souhait des internautes de ne pas divulguer leur identité lorsqu'ils exercent leur liberté d'expression. Cependant, la généralisation de l'accès à internet et la possibilité – qui est à certains égards un risque – que les contenus qui y sont publiés continuent indéfiniment de circuler dans la sphère publique commande d'exercer une certaine prudence.

La Cour européenne a considéré qu'en permettant la publication de commentaires par des usagers non enregistrés, une plateforme d'information en ligne devait assumer une part de responsabilité à l'égard de ces commentaires. Cet aspect de la décision de la Cour européenne a attiré de multiples critiques car beaucoup craignent que cela mène à la fin des commentaires d'internautes ou à l'adoption de politiques et de lois imposant un enregistrement sous une véritable identité dans la région du Conseil de l'Europe.[20] En mai 2015, un réexamen de la décision était attendu devant la Grande Chambre.

–

– Le lien entre l'anonymat et le droit à la liberté d'expression a été mis en évidence dans un rapport plus récent de la Commission interaméricaine des droits de l'homme (CIDH) en 2013, *La liberté d'expression et l'Internet*.[21] Entre autres, le CIDH a recommandé que les plateformes anonymes soient encouragées et que les services d'authentification soient utilisés de manière proportionnée.[22]

L'anonymat dans la pratique

Considérant le caractère limité de la protection juridique de l'anonymat, de nombreux internautes se sont tournés vers des méthodes techniques pour préserver leur anonymat en ligne. Dans la pratique, plusieurs initiatives ont été lancées à ces fins.[23] Cela inclut le navigateur Tor, qui masque les adresses IP des internautes lorsqu'ils naviguent sur le réseau,[24] et le protocole https://, qui encrypte les communications sur certains sites Internet.[25] Toutefois, ces outils techniques ont été eux aussi restreints par la législation de certains pays.

Section II: Chiffrement

Section II: Encryption

Considérations d'ordre général

Le chiffrement a été ainsi défini :

> Le processus de cryptage ou « brouillage » du contenu d'une donnée ou d'une communication vocale à l'aide d'un algorithme et d'une variable sélectionnée de manière aléatoire associée à l'algorithme, connue sous le nom de « clé ».[26]

Le chiffrement signifie que l'information ne peut être décryptée que par le destinataire de la communication qui détient la clé. Dans la plupart des cas, la clé est essentiellement « une série de chiffres ; plus la clé est longue, plus la sécurité est renforcée ».[27]

Le chiffrement peut servir à protéger des données en transit ou stockées qui incluent des courriers électroniques, des fichiers, des disques et des connexions Internet. Toutefois, si le chiffrement protège généralement la confidentialité du message ou des données du contenu, il ne masque pas nécessairement les adresses IP de l'expéditeur ou du destinataire (métadonnées) *vis-à-vis* de tierces parties, bien que les adresses IP puissent aussi être masquées à l'aide d'autres technologies telles que le navigateur TOR. En ce sens, le chiffrement seul ne garantit pas l'anonymat dans la mesure où il est possible de remonter jusqu'aux internautes, et par conséquent de les identifier.

De même, le chiffrement peut servir à vérifier l'authenticité et l'intégrité des communications, par ex. à travers l'utilisation de signatures numériques. Une signature numérique est « l'assurance cryptographiquement fondée qu'un document particulier a été créé ou transmis par une personne donnée ».[28] Les signatures numériques sont parfois certifiées par un « tiers de confiance » (*Trusted Third Party* - TTP), notamment une autorité de certification (*certification authority*) qui émet des certificats numériques. Dans la pratique, cependant, les tiers de confiance ne sont pas plus dignes de confiance que leur maillon le plus faible. De ce fait, les mécanismes de cryptage de bout en bout sont généralement préférables car ils permettent à un internaute de vérifier directement l'identité prétendue d'un autre usager, sans recourir à un tiers de confiance, lequel ne peut alors accéder aux données de la communication. En d'autres termes, le cryptage de bout en bout est une forme plus sûre de chiffrement.

Le chiffrement : une condition préalable à des communications en ligne sécurisées

Le chiffrement est une caractéristique fondamentale de l'Internet. Sans les techniques d'authentification découlant du chiffrement, il serait impossible de sécuriser des transactions en ligne. Sans le chiffrement lui-même, les communications électroniques de tout individu, ainsi que de toute entreprise ou agence gouvernementale, pourraient faire l'objet d'une surveillance et d'abus. Pour ces raisons, le chiffrement est utilisé sur une base quotidienne pour des informations et des activités telles que la banque en ligne, les échanges privilégiés entre avocat et client, les données médicales, les dossiers fiscaux et les grandes infrastructures telles que les réseaux électriques ou les centrales électriques. Le chiffrement est particulièrement important pour les défenseurs des droits humains, les lanceurs d'alerte, les journalistes et les militants qui font souvent l'objet d'une surveillance par les services de renseignement ou les autorités chargées du maintien de l'ordre.

Le chiffrement est étroitement lié à la cybersécurité, qui se préoccupe généralement du développement de standards techniques, y compris le chiffrement, afin de protéger des systèmes d'information. A cet égard, tout en restant distincte, la cybersécurité est liée à la cybercriminalité, un terme traditionnellement utilisé pour décrire des délits commis par un individu qui s'immisce illégalement dans des systèmes d'information.[29] La plupart des pays ont adopté une législation sur la cybercriminalité visant à pénaliser l'accès illégal ou les atteintes à l'intégrité des données ou systèmes d'information.[30] La législation sur la cybercriminalité pose un problème important dans la mesure où elle tend à prévoir des délits liés au contenu, tels que la diffamation ou le blasphème. On trouve quelques exemples de ces législations dans plusieurs pays tels que le Pakistan, le Kenya[31] et le Bangladesh.[32]

Chiffrement et droit international

Au niveau international, la protection d'un « droit de chiffrement » a été jusque-là limitée. Elle est traditionnellement liée à la protection du droit au respect de la vie privée et du droit à la protection des données à caractère personnel plutôt qu'à la liberté d'expression.

– A cet égard, l'instrument clé est le rapport 2015 du Rapporteur spécial sur la liberté d'expression, mentionné dans le chapitre précédent. Par ailleurs, dans son rapport 2013, le Rapporteur spécial sur la liberté d'expression a d'abord fait le lien entre la liberté d'expression, le chiffrement et les communications anonymes.[33]

– Les *Lignes directrices régissant la politique de cryptographie* de 1997 de l'Organisation de développement et de coopération économiques (OCDE) identifient les questions clés à examiner par les Etats membres lors de l'adoption de politiques de cryptographie, à la fois au niveau national et international. En particulier, l'OCDE a recommandé les principes fondamentaux suivants :[34]

  1) Les méthodes cryptographiques devraient susciter la confiance afin que les utilisateurs puissent se fier aux systèmes d'information et de communication ;

  2) Les utilisateurs devraient avoir le droit de choisir toute méthode cryptographique, dans le respect de la législation applicable ;

  3) Les méthodes cryptographiques devraient être développées en réponse aux besoins, aux demandes et aux responsabilités des personnes, des entreprises et des gouvernements ;

  4) Des normes, critères et protocoles techniques applicables aux méthodes cryptographiques devraient être élaborés et instaurés aux échelons national et international ;

5) Les droits fondamentaux des individus au respect de leur vie privée, notamment au secret des communications et à la protection des données de caractère personnel, devraient être respectés dans les politiques nationales à l'égard de la cryptographie et dans la mise en œuvre et l'utilisation des méthodes cryptographiques ;

6) Les politiques nationales à l'égard de la cryptographie peuvent autoriser l'accès légal au texte en clair ou aux clés cryptographiques de données chiffrées. Ces politiques doivent respecter dans toute la mesure du possible les autres principes énoncés dans les lignes directrices ;

7) Qu'elle soit établie par contrat ou par voie législative, la responsabilité des personnes et entités qui proposent des services cryptographiques, détenant des clés cryptographiques, ou y ayant accès, devrait être clairement énoncée ;

8) Les gouvernements devraient coopérer en vue de coordonner les politiques à l'égard de la cryptographie. Dans le cadre de cet effort, les gouvernements devraient veiller à la levée, ou éviter de créer au nom de la politique de cryptographie, des obstacles injustifiés aux échanges.

Dans son rapport explicatif, l'OCDE a souligné l'importance fondamentale de la cryptographie pour la protection du droit au respect de la vie privée et la confidentialité des informations :[35]

> Le respect de la vie privée et la confidentialité des données de caractère personnel sont des valeurs importantes dans une société démocratique. Pourtant, la vie privée est aujourd'hui davantage menacée dans l'infrastructure de l'information et des communications qui se met en place car ni les réseaux ouverts, ni les nombreux types de réseaux privés ont été conçus en ayant à l'esprit la confidentialité des communications et du stockage des données. Toutefois, la cryptographie constitue la base

d'une nouvelle génération de technologies susceptibles de contribuer à renforcer le respect de la vie privée. L'utilisation d'une cryptographie efficace dans un environnement de réseau peut aider à protéger la confidentialité des informations de caractère personnel et le secret des informations confidentielles. Le fait de ne pas utiliser la cryptographie dans un environnement où les données ne sont pas complètement sûres peut nuire à certains intérêts, notamment à la sécurité publique et à la sécurité nationale. Dans certains cas, en particulier lorsque la législation impose la garantie de la confidentialité des données ou la protection d'infrastructures essentielles, les gouvernements peuvent demander l'emploi d'une cryptographie offrant une robustesse minimale.

– La Commission interaméricaine des droits de l'homme (CIDH) a proposé des recommandations relatives à la protection des communications anonymes et des outils de cryptage dans son rapport sur *La liberté d'expression et l'Internet* de 2013, où elle affirme que :[36]

  L'interdiction d'utiliser des outils de contournement pour protéger légitimement le droit à l'anonymat de la communication ou pour une utilisation légitime de la propriété d'un individu ne sera pas considérée comme une mesure de protection légitime du droit d'auteur.

– En 2012, le Comité des ministres du Conseil de l'Europe a recommandé que ses Etats membres s'engagent avec le secteur privé à :

  Veiller à ce que les mesures de sécurité les plus adaptées soient appliquées à la protection des données à caractère personnel contre tout accès illicite par des tiers. Cela devrait comprendre des mesures de cryptage de bout en bout (end-to-end) des communications entre l'utilisateur et le site des services de réseaux sociaux.[37]

– Le rapport 2015 de l'Assemblée parlementaire du Conseil de l'Europe (PACE) sur les opérations massives de surveillance condamne fermement les efforts de la National Security Agency (NSA) en vue d'affaiblir les standards de chiffrement et l'utilisation de « trappes » (backdoors). Le rapport conclut que :

  (L)a création de « trappes » ou toute autre technique visant à fragiliser ou à contourner les mesures de sécurité, ou à exploiter les failles existantes, devrait être rigoureusement interdite ; l'ensemble des établissements et entreprises privés qui conservent des données à caractère personnel devraient être tenus d'appliquer les mesures de sécurité les plus efficaces disponibles.[38]

Le chiffrement est également essentiel à la protection d'autres droits, y compris le droit à ne pas s'auto-incriminer et le droit à un procès équitable. Des mesures telles que la cession obligatoire de clés de décryptage peuvent enfreindre le droit de ne pas s'auto-incriminer.

La jurisprudence de la Cour européenne et plusieurs cours au niveau national affirment que le droit à ne pas s'auto-incriminer n'est pas absolu[39] et qu'il peut être mis en œuvre uniquement s'il résulte d'un acte de témoignage, contrairement à la production de documents ou matériels préexistants.[40] Cependant, les approches des cours sont très divergentes lorsqu'il s'agit de savoir si des clés de décryptage ressemblent davantage à des clés matérielles[41] (matériel préexistant) ou à des codes de sécurité (témoignage).[42] Bien que la Cour européenne ait encore à statuer spécifiquement sur l'obligation de révéler des clés de décryptage, la jurisprudence actuelle indique qu'elle chercherait surtout à savoir si le procès a été équitable dans son ensemble, eu égard au poids de l'intérêt public dans l'enquête et à la poursuite de l'infraction en question, la nature et le degré de coercition, le type d'information recherché et comment cette information a été utilisée devant la cour.[43]

Enfin, il convient de signaler que, hormis les standards des droits humains, le chiffrement a été principalement régi par des accords internationaux relatifs à la réglementation de l'import/export de produits technologiques à double usage, tels que l'*Arrangement de Wassenaar*.[44]

Par ailleurs, l'Internet Engineering Task Force (IETF) a souligné à plusieurs reprises l'importance du chiffrement et recommandé qu'il soit encouragé et disponible pour tous.[45] Dans sa déclaration de 2014, l'IETF a clairement indiqué que « l'usage du chiffrement protège contre une surveillance envahissante et d'autres attaques passives ».[46]

Section III: Restriction de l'anonymat et du chiffrement

Section III: Restriction de l'anonymat et du chiffrement

Anonymat

Considérant l'énorme quantité d'informations collectées sur nos vies privées tant par des entreprises privées que par des entités publiques, il est évident que le droit au respect de la vie privée, le droit à la liberté d'expression et le droit à l'anonymat en ligne doivent être maintenant protégés plus vigoureusement et plus systématiquement que jamais. En premier lieu, le droit à l'anonymat devrait être expressément reconnu comme une composante essentielle du droit à la liberté d'expression.

Position d'ARTICLE 19
Selon ARTICLE 19, pour que le droit à la liberté d'expression soit significatif dans l'ère du numérique, il doit nécessairement englober le droit à l'anonymat, y compris le droit au discours anonyme, le droit à la lecture anonyme, et le droit de naviguer en ligne anonymement.

Cela est conforme aux meilleures pratiques établies dans plusieurs pays[47] où le droit au discours anonyme, le droit à la lecture anonyme et, plus généralement, le droit à l'anonymat en ligne ont été reconnus. Cela est également conforme à l'objectif de la législation relative à la protection des données, qui vise à empêcher que les individus soient identifiés par suite du traitement des données personnelles par des systèmes informatiques automatisés.

De plus, toute restriction de l'anonymat devrait respecter les critères du triple test en vertu de l'Article 19 (3) du *Pacte international relatif aux droits civils et politiques* (PIDCP), à savoir qu'elle devrait:

- Etre fixée par la loi : les restrictions doivent être précises et clairement stipulées dans le respect du principe de l'état de droit. Cela signifie que des restrictions vagues ou formulées dans des termes généraux, ou des restrictions qui laissent un trop grand pouvoir discrétionnaire aux autorités exécutives, sont incompatibles avec le droit à la liberté d'expression ;

- Poursuivre un but légitime, explicitement énuméré dans l'Article 19 (3) du PIDCP, à savoir le respect des droits ou de la réputation d'autrui, et la protection de la sécurité nationale et de l'ordre public, et de la santé et la moralité publiques. La liste des buts est exhaustive et par conséquent toute entrave qui ne poursuit pas l'un de ces buts est en violation de l'Article 19 ;

- Etre nécessaire et proportionnée au but légitime poursuivi.[48] Le terme « nécessaire » signifie que la restriction doit répondre à un « besoin social pressant » ;[49] que les raisons invoquées par l'Etat pour justifier la restriction doivent être « pertinentes et suffisantes », et que l'Etat doit fournir la preuve que l'entrave est proportionnée au but poursuivi.[50]

Dans les chapitres suivants, ARTICLE 19 expose les principaux types de restrictions qui se présentent dans le contexte de l'anonymat en ligne, ainsi que l'approche que nous considérons comme appropriée pour de telles restrictions.

Recommandations d'ARTICLE 19 :
- Les Etats devraient explicitement reconnaître dans leur législation nationale et dans leurs pratiques que le droit à la liberté d'expression inclut le droit à l'anonymat ;

- Les Etats devraient également reconnaître explicitement le droit au discours anonyme, le droit à la lecture anonyme, et le droit de naviguer en ligne anonymement.

Enregistrement sous une véritable identité

Des lois sur l'enregistrement sous une véritable identité ont été récemment adoptées ou examinées dans plusieurs pays.[51] Elles permettent généralement aux autorités locales chargées du maintien de l'ordre de retrouver la trace des internautes plus facilement. ARTICLE 19 estime que ces lois sont une entrave particulièrement brutale aux droits à la liberté d'expression et au respect de la vie privée en ligne. Ces lois sont généralement conjuguées à des obligations pour les internautes de s'identifier dans les cybercafés, et des obligations pour les propriétaires des cybercafés de retrouver la trace et enregistrer les activités en ligne de leurs clients.[52]

Position d'ARTICLE 19

Selon le point de vue d'ARTICLE 19, les régimes d'enregistrement obligatoire sous une véritable identité vont bien au-delà de ce qui est admissible en vertu du droit international relatif aux droits humains et devraient être abolis :[53]

- Comme mentionné précédemment, l'anonymat est un élément essentiel de la liberté d'expression en ligne. Il fait partie intégrante de la culture et de la fonction de l'Internet. Il permet à des individus d'exprimer des opinions controversées qu'ils n'auraient peut-être pas partagées dans le monde hors ligne. Les régimes d'enregistrement obligatoire sous une véritable identité ont un effet paralysant sur la liberté d'expression car les individus craignent d'exercer leur droit à la liberté d'expression. Par exemple, des personnes peuvent être moins susceptibles de révéler des informations compromettantes sur des personnalités puissantes par peur d'être sanctionnés ou de faire l'objet de poursuites coûteuses.

- Les régimes d'enregistrement sous une véritable identité encouragent également la collecte d'informations qui pourraient faire facilement l'objet d'abus par les autorités et devenir un outil de répression, menant à la persécution et au harcèlement d'individus sur la base de leur expression. Dans de nombreux pays, la critique à l'encontre du gouvernement est illégale et seule la publication anonyme de telles informations en ligne peut garantir que les auteurs ne risquent pas des représailles.[54]

- Les obligations d'enregistrement sous une véritable identité sont inefficaces dans la pratique, dans la mesure où les individus peuvent toujours utiliser d'autres moyens techniques et outils de sécurité comme le chiffrement, les VPN, ou la navigation anonyme sur Internet pour préserver leur anonymat.

- L'anonymat ne se limite pas à l'Internet et existe encore dans la « vraie vie ». Par exemple, des individus peuvent envoyer des lettres anonymes, passer des appels téléphoniques anonymes, ou distribuer des tracts ou autres publications anonymement. Bien que l'Internet permette d'atteindre un grand nombre de personnes plus facilement et à un moindre coût, toute obligation d'identification sous une véritable identité pourrait restreindre les communications sur Internet plus que toute autre forme de communication quotidienne (par ex. les services postaux ne sont pas tenus d'authentifier l'adresse de renvoi pour des courriers contenant des matériels délictueux ; l'identification sous une véritable identité n'est pas non plus exigée pour des appels téléphoniques).

De même, ARTICLE 19 estime que, en tant que principe général, les médias sociaux et les sites d'information ne devraient pas exiger l'usage de régimes d'enregistrement sous une véritable identité.

- Bien que les entreprises ne soient pas tenues de respecter les obligations du droit international relatif aux droits humains d'un point de vue strictement juridique, ARTICLE 19 estime qu'elles ont néanmoins le devoir de respecter les droits humains conformément aux *Principes directeurs de Ruggie sur les droits de l'homme et les entreprises*.[55]

- L'usage d'un enregistrement sous une véritable identité par les médias sociaux et les sites d'information en tant que condition préalable à l'utilisation de leurs services peut avoir un impact négatif sur les droits à la vie privée et à la liberté d'expression, en particulier pour les minorités ou les groupes vulnérables, qui peuvent être empêchés d'affirmer leur identité.[56]

- Alors que les politiques d'identité véritable sont généralement présentées comme un outil efficace contre le trolling sur Internet, ou pour promouvoir la culture du respect mutuel entre les internautes, leurs inconvénients excèdent leurs avantages. En particulier, l'anonymat est vital pour protéger les enfants, les victimes de crimes, et les individus appartenant à des groupes minoritaires et autres groupes vulnérables, qui pourraient être ciblés par des criminels ou d'autres tiers malveillants susceptibles d'abuser de ces politiques. A cet égard, l'anonymat concerne autant la sécurité en ligne que l'auto-expression.

– L'enregistrement sous une véritable identité ou l'obligation de fournir une identification quelconque (au moment de s'abonner à un service, tel qu'un compte email) soulève également de sérieuses préoccupations pour la protection des données, sachant que nombre de ces systèmes contraignent les internautes à fournir une somme considérable de données personnelles sensibles pour vérifier leur identité.[57]

Recommandations d'ARTICLE 19 :

– Les Etats devraient abroger les lois, règlementations et politiques qui requièrent un enregistrement sous une véritable identité, lequel constitue une violation des droits à la liberté d'expression et au respect de la vie privée.

– Les médias sociaux et les sites d'information ne devraient pas imposer des régimes d'enregistrement sous une véritable identité. A tout le moins, les opérateurs d'Internet devraient assurer que l'anonymat reste une option véritable.

Accès aux données à caractère personnel et divulgation de l'identité

Accès par les autorités chargées de l'application des lois

Dans la plupart des pays, les lois relatives à l'enregistrement sous une véritable identité ne sont pas nécessaires dans la mesure où les autorités chargées de l'application des lois ont déjà le pouvoir d'exiger la divulgation de l'identité d'internautes anonymes.[58]

Position d'ARTICLE 19

ARTICLE 19 reconnaît que le droit à l'anonymat en ligne n'est pas absolu et peut être levé dans certaines circonstances limitées, dans le strict respect des standards internationaux relatifs à la liberté d'expression en vertu du triple test mentionné ci-dessus. Toute levée de l'anonymat devrait être soumise à de fortes garanties procédurales. En particulier, par principe, la divulgation obligatoire de l'identité en ligne d'un individu ne devrait être ordonnée que par des tribunaux, lesquels sont les mieux placés pour préserver un juste équilibre entre le droit à l'expression anonyme et d'autres intérêts.[59]

De plus, le seuil devrait être plus élevé si l'individu en question exerce une activité journalistique. Dans une telle situation, la cour devrait examiner l'impact sur la liberté d'expression et déterminer si la divulgation permet de défendre un intérêt public plus élevé.

Les autorités chargées du maintien de l'ordre devraient être habilitées à accéder aux données à caractère personnel des individus sans injonction d'un tribunal uniquement dans des cas d'urgence, par exemple en cas de risque imminent et spécifique de préjudice pour un individu particulier.

Accès par des tiers

ARTICLE 19 reconnaît également que l'anonymat peut être légitimement levé dans le but de lancer des procédures civiles (telles que la diffamation ou d'autres actions privées), mais cela doit faire l'objet de fortes garanties procédurales.

Position d'ARTICLE 19
A cet égard, ARTICLE 19 souligne que, par principe, les tribunaux sont le mieux placés pour préserver un équilibre approprié entre le droit à l'expression anonyme et d'autres intérêts, et ordonner de ce fait la divulgation obligatoire de l'identité en ligne d'un individu si nécessaire. Cela est conforme aux meilleures pratiques dans des pays où les tribunaux ont reconnu que l'anonymat pouvait être levé dans des cas spécifiques, après examen minutieux.[60] Dans les cas de diffamation, par exemple, cela nécessite de répondre à un certain nombre de conditions, y compris l'envoi d'une notification à l'internaute anonyme qui a posté le contenu, les détails des expressions diffamatoires présumées, les preuves *prima facie* pour tous les faits essentiels de son dossier contre la personne anonyme qui a posté le matériel, et l'équilibre entre le droit au discours anonyme et les preuves prima facie, en tenant compte de la nécessité de divulguer l'identité afin que le cas soit jugé.[61]

Autres mesures
ARTICLE 19 est opposé à des mesures qui limitent le discours anonyme en encourageant les intermédiaires d'Internet à supprimer des contenus postés par des internautes anonymes plutôt que des interlocuteurs identifiables, par peur de s'exposer eux-mêmes à des poursuites judiciaires.[62] Selon nous, de telles mesures ont un effet paralysant sur la liberté d'expression et ne devraient pas être adoptées.

De même, le filtrage d'Internet susceptible de permettre à des détenteurs de droits d'auteur de retrouver la trace d'internautes qui utilisent des réseaux pair-à-pair et autres sites de partage de fichiers dans un relatif anonymat (par exemple à l'aide de proxies ou de réseaux privés virtuels) sont incompatibles avec les droits à la liberté d'expression et à la vie privée et devraient être interdits.[63]

Recommandations d'ARTICLE 19 :
- Les Etats devraient adopter des lois, des réglementations et des politiques qui confèrent uniquement aux tribunaux le pouvoir d'ordonner la levée de l'anonymat – plutôt qu'à des autorités chargées de l'application des lois ;
- Toute restriction devrait respecter intégralement le triple test des restrictions à la liberté d'expression et devrait faire l'objet de fortes garanties procédurales ;
- Les Etats et les entreprises devraient promouvoir l'usage d'outils tels que le logicielTor et le protocole https:// qui permettent de naviguer sur Internet en préservant son anonymat.

Chiffrement

Le chiffrement est essentiel pour assurer la sécurité de l'information, l'intégrité des communications et le droit au respect de la vie privée en ligne. C'est également un outil vital pour la protection de la liberté d'expression sur Internet ainsi que le contournement de la surveillance et de la censure. Comme mentionné dans le rapport du Rapporteur spécial sur la liberté d'expression, des normes de chiffrement faibles ou des « trappes » – obligatoires ou non – sapent la confiance des individus dans l'Internet et constituent une atteinte sérieuse aux droits fondamentaux.

Les restrictions à l'utilisation du chiffrement (y compris le cryptage) peuvent revêtir des formes très diverses. De manière générale, elles peuvent inclure les restrictions suivantes :

Restrictions imposées aux utilisateurs finaux
Nombre de gouvernements prévoient des interdictions pures et simples ou des restrictions importantes à l'utilisation du chiffrement par les utilisateurs finaux (par ex. la Chine,[64] l'Inde,[65] le Sénégal,[66] l'Egypte[67] ou le Pakistan[68]).

Position d'ARTICLE 19
ARTICLE 19 estime que les restrictions à l'utilisation de produits cryptograpqhiques par les internautes sont une violation flagrante du droit au respect de la vie privée et du droit à la liberté d'expression. Comme mentionné précédemment, le chiffrement est essentiel pour la protection de la confidentialité des communications et des données à caractère personnel. Interdire l'usage du chiffrement équivaut à empêcher des individus de poser des cadenas sur leurs portes ou des rideaux à leurs fenêtres. De ce fait, c'est une restriction disproportionnée des droits à la vie privée et à la liberté d'expression et cela ne peut jamais être justifié.

Selon ARTICLE 19, toute restriction des standards de chiffrement doit respecter strictement le test en trois parties en vertu de l'Article 19 (3) du PIDCP. Cela signifie que toute restriction du chiffrement doit être fixée par la loi, poursuivre un objectif légitime et être nécessaire et proportionnée à cet objectif. En premier lieu, la nécessité de telles mesures doit être évaluée en se référant au large éventail des pouvoirs de surveillance disponibles pour les services de renseignements et les autorités chargées de l'application des lois, pouvoirs déjà largement critiqués et considérés comme superflus et excessifs.[69]

Recommandations d'ARTICLE 19 :

- Les Etats devraient reconnaître dans leur législation et dans leurs pratiques que le chiffrement est une condition fondamentale de la protection de la confidentialité des informations et de leur sécurité et que, de ce fait, il est essentiel à la protection du droit à la liberté d'expression en ligne ;

- Toute restriction du chiffrement doit respecter strictement le test en trois parties en vertu de l'Article 19 (3) du PIDCP et faire l'objet de garanties procédurales et d'une procédure régulière ;

- Les Etats devraient abolir ou s'abstenir d'adopter des lois requérant une autorisation du gouvernement pour utiliser des produits cryptographiques ;

- Les Etats devraient abolir ou s'abstenir d'adopter des lois requérant le décryptage de données cryptées ou la divulgation de clés de chiffrement dans toutes circonstances autres que sur injonction d'un tribunal.

Exigences techniques obligatoires

Plusieurs gouvernements cherchent aussi à prendre le contrôle des systèmes d'information en accordant à une agence gouvernementale, en général liée au ministère de la Défense, de l'Intérieur ou des Transports, le pouvoir général de réviser et approuver tous les standards, techniques, systèmes et équipements (par ex. l'Inde,[70] la Chine [71] et l'Egypte[72]).

Position d'ARTICLE 19

ARTICLE 19 considère que des mesures telles que les spécifications techniques imposées par des gouvernements pour affaiblir les standards de chiffrement, ainsi que l'installation de « trappes » compromettant l'intégrité des logiciels des communications privées, sont disproportionnés et, de ce fait, impossibles à justifier en vertu du droit international. Selon ARTICLE 19 :

- De telles mesures équivalent à demander à des serruriers de produire des serrures et des pênes fragiles afin de faciliter l'accès du gouvernement à des domiciles privés. Une telle intrusion dans la vie privée est à la fois inacceptable et dangereuse ;

- Loin de faciliter pour les forces de l'ordre la capture de criminels, l'adoption de standards de chiffrement faibles est plus susceptible de faciliter des activités criminelles ;

-

- De plus, considérant la fréquence et la sévérité croissantes des cyberattaques tant au niveau national qu'international, il semble très douteux que des standards de chiffrement faibles puissent jamais être une réponse proportionnée.

Recommandations d'ARTICLE 19 :

- Les Etats devraient s'abstenir d'adopter des mesures qui requièrent ou promeuvent l'installation de trappes techniques dans des logiciels et/ou des matériels de cryptage.

Contrôles à l'importation/exportation

Des gouvernements ont également cherché à exercer un contrôle sur le chiffrement grâce au contrôle des importations/exportations. En particulier, ces gouvernements ont été traditionnellement peu disposés à exporter des produits de cryptage solides par peur d'affaiblir les capacités de leurs services de renseignements à espionner des cibles étrangères. Cependant, le marché international exige un cryptage solide. Par le passé, ces intérêts conflictuels ont été utilisés par des gouvernements pour façonner la politique nationale. Par exemple, les Etats-Unis ont utilisé des règles de contrôle à l'export pour contraindre les fabricants de logiciels et de matériels informatiques à adopter des produits cryptographiques plus faibles ou un système de séquestre de clés sur leur territoire.[73]

Cependant, avec Internet, ces contrôles se sont largement relâchés.[74] Il semble néanmoins que plusieurs pays (par ex. la France[75] et le Sénégal)[76] préservent les contrôles à l'export sur certaines catégories de matériels et de logiciels qui permettent le cryptage. Cela concerne généralement des produits autres que ceux qui garantissent l'authentification ou la protection de l'intégrité des systèmes d'information, ainsi que les marchandises à double usage. De plus, l'exportation de certaines catégories de produits cryptographiques, en particulier ceux à usage militaire, reste dans une certaine mesure touchée par l'*Arrangement de Wassenaar* (voir ci-dessus).

Enfin, certains pays (par ex. la Chine[77] et l'Ethiopie) continuent d'imposer des restrictions importantes sur l'importation de tous les programmes informatiques ou équipements qui permettent la cryptographie. Cela parce que les gouvernements craignent généralement d'importer des produits qui pourraient contenir des trappes, ou parce qu'ils souhaitent préserver leurs capacités de surveillance nationales.[78]

Position d'ARTICLE 19
ARTICLE 19 estime que l'application de contrôles à l'import/export de produits cryptographiques est une restriction disproportionnée des droits à la liberté d'expression et au respect de la vie privée. De telles mesures constituent une menace réelle pour la confidentialité des communications des internautes en les rendant plus vulnérables à la surveillance nationale ou étrangère. Dans des pays où la critique des politiques et des représentants du gouvernement constitue un délit, cela expose les journalistes, les défenseurs des droits humains, les militants et autres groupes vulnérables à des risques de représailles.

Recommandations d'ARTICLE 19 :
– Les Etats devraient lever les restrictions disproportionnées à l'import/export des logiciels et matériels de cryptographie.

Système de séquestre de clés ou tiers de confiance
Dans un système de séquestre de clés, de longues clés de cryptage sont autorisées mais les internautes sont tenus de déposer leurs clés auprès d'agences gouvernementales ou d'un « tiers de confiance » (généralement autorisé par le gouvernement ou ayant des liens avec ce dernier).[79]

Bien que les efforts en vue de l'adoption du système de séquestre de clés au niveau international n'aient pas abouti, ces systèmes sont actuellement mis en œuvre dans plusieurs pays (par ex. en Inde et en Espagne[80]).

Position d'ARTICLE 19
ARTICLE 19 estime que les systèmes de séquestre de clés sont une restriction disproportionnée des droits à la vie privée et à la liberté d'expression. Ces systèmes équivalent à donner au gouvernement les clés du domicile d'un individu. Alors que les variantes du système de séquestre de clés avec autorisation d'un tribunal peuvent séduire, leur mise en œuvre est coûteuse et ils fournissent finalement une protection assez faible de la vie privée dans la mesure où la protection est aussi forte que son maillon le plus faible. Plus le nombre d'entités et d'individus impliqués est important, plus forte est la probabilité qu'ils subissent des pressions indirectes du gouvernement et d'autres acteurs.

Recommandations d'ARTICLE 19 :
– Les Etats devraient abolir ou s'abstenir d'adopter des systèmes de séquestre de clés.

Divulgation obligatoire de clés de cryptage
Dans certains pays, en tant qu'alternative aux systèmes de séquestre de clés, les autorités chargées de l'applications des lois ou les tribunaux peuvent exiger la divulgation de clés de cryptage ou ordonner le décryptage de données chiffrées à une personne suspectée d'avoir commis un crime ou, dans certains pays, à une tierce partie. Tout refus d'obtempérer est considéré généralement comme un délit pénal, passible d'une peine d'emprisonnement et/ou d'une amende.[81]

Position d'ARTICLE 19
Etant donné que des organes chargés de l'application des lois ou des services de renseignements peuvent, dans des cas exceptionnels, requérir le pouvoir d'ordonner la divulgation d'une clé ou le décryptage de communications pertinentes, ARTICLE 19 considère que le moyen le moins intrusif serait de contraindre ces organes respectifs à obtenir un ordre du tribunal exigeant que la personne en question fournisse l'information sous un format décrypté.

Selon ARTICLE 19, la divulgation d'une clé de décryptage entraînerait inévitablement une restriction disproportionnée du droit au respect de la vie privée dans la mesure où la clé pourrait potentiellement révéler des informations privées qui vont bien au-delà du but recherché par la divulgation obligatoire de la clé.

Alors que des ordres de décryptage peuvent être admissibles dans des cas exceptionnels, aucun tribunal ne devrait émettre un tel ordre à moins qu'il ne soit convaincu que l'entrave aux droits à la vie privée et à la liberté d'expression de la personne soit à la fois nécessaire dans les circonstances et proportionnée. Les autorités chargées de l'application de la loi devraient être tenues de démontrer que la personne en question est raisonnablement suspectée d'être impliquée dans une activité criminelle sérieuse. Par ailleurs, un tribunal ne devrait émettre l'ordre que pour des communications spécifiques et non pour tous les fichiers cryptés sur un ordinateur.

En émettant un ordre de décryptage, la cour devrait se demander si l'usage de tels pouvoirs coercitifs constituerait une violation du droit à ne pas s'auto-incriminer, c'est-à-dire si l'usage du matériel obtenu par l'exercice de tels pouvoirs aurait un effet négatif sur le caractère équitable des poursuites pénales subséquentes.

Enfin, pour garantir que tout pouvoir coercitif enjoignant de décrypter des communications ne fasse pas l'objet d'abus, tout décryptage ne devrait être effectué qu'en présence d'un avocat indépendant ou d'une autorité chargée de la protection des données.

Dans tous les cas, les juges devraient exercer leur pouvoir discrétionnaire et exclure les preuves obtenues suite à l'usage de tels pouvoirs coercitifs permettant d'exiger la divulgation de clés de cryptage ou le décryptage d'informations, si la recevabilité de telles preuves pouvait avoir un effet négatif sur l'équité de la procédure. En particulier, si des informations décryptées étaient obtenues illégalement et en violation du droit au respect de la vie privée, les juges devraient, selon nous, statuer que l'information obtenue par suite de la divulgation est irrecevable.

Toutefois, si l'ordre a été émis légalement et que la personne refuse de s'y soumettre, elle peut faire l'objet des sanctions appropriées pour outrage à la cour. Dans le même temps, si la non-divulgation des clés de cryptage est pénalisée, ARTICLE 19 estime que tout délit de ce type devrait, au minimum, reconnaître des défenses telles que l'absence de connaissance ou possession de la clé.

Autres pouvoirs de surveillance

Il devrait être mentionné que dans des circonstances où les autorités chargées de l'application des lois et les services de renseignement ont été incapables d'obtenir des pouvoirs plus importants afin de casser l'algorithme de cryptage ou de demander la divulgation des clés de cryptage, elles ont généralement demandé d'autres pouvoirs de surveillance.[82]

Position d'ARTICLE 19

ARTICLE 19 estime que le recours au piratage par des responsables gouvernementaux est, en général, une violation flagrante des droits au respect de la vie privée et à la liberté d'expression, sachant qu'il implique un accès à des informations privées sans permission ou notification, et qu'il porte atteinte à l'intégrité des mesures de sécurité propres à la cible. Contrairement aux mandats de perquisition où la personne serait au moins prévenue que son domicile ou son bureau serait perquisitionné, le piratage a généralement lieu à l'insu de la personne. Il équivaut à une intrusion de la police dans le domicile d'une personne.

Considérant le caractère clairement intrusif d'une telle mesure, il ne devrait être autorisé que par un juge dans les circonstances les plus exceptionnelles, et soumis à des conditions strictes. En particulier, le piratage ne devrait être disponible que pour les délits les plus graves et en dernier recours, lorsque d'autres méthodes moins intrusives ont déjà été épuisées.

Recommandations d'ARTICLE 19 :

- Les entreprises devraient s'abstenir d'affaiblir les standards techniques et devraient mettre en place la prestation de services avec un cryptage de bout en bout solide ;

- Les Etats et les entreprises devraient mettre en place des programmes en vue de promouvoir le cryptage des communications sur Internet ;

- Les Etats et les entreprises devraient promouvoir le cryptage de bout en bout en tant que standard de base pour la protection du droit au respect de la vie privée en ligne. Ils devraient également promouvoir l'utilisation de logiciels ouverts et investir dans ces derniers pour s'assurer qu'ils sont entretenus régulièrement et indépendamment et qu'ils sont contrôlés pour détecter des vulnérabilités.

A propos d'ARTICLE 19

ARTICLE 19 œuvre pour l'élaboration de normes progressistes relatives à la liberté d'expression et la liberté d'information aux niveaux international et régional, et pour leur mise en œuvre dans les systèmes juridiques nationaux. ARTICLE 19 a produit un grand nombre de publications sur les législations nationales et comparées et les bonnes pratiques dans des domaines tels que la diffamation, l'accès à l'information, et la réglementation de l'audiovisuel.

Sur la base de ces publications et de l'expertise juridique globale d'ARTICLE 19, l'organisation publie chaque année plusieurs analyses juridiques, commentaires sur des projets de loi et des lois existantes qui portent atteinte au droit à la liberté d'expression, et élabore des documents d'orientation et autres. Ce travail analytique mené depuis 1998 pour soutenir des réformes positives de la législation à travers le monde entier, conduit fréquemment à des améliorations importantes des projets de loi ou des lois nationales en vigueur. Toutes nos analyses légales et documents d'orientation peuvent être consultés sur **http://www.article19.org/resources.php/legal.**

Si vous souhaitez discuter plus amplement de ce document de synthèse, ou si vous souhaitez attirer l'attention du Programme juridique d'ARTICLE 19 sur un sujet particulier, vous pouvez nous contacter par courriel à l'adresse **legal@article19.org.**

Ce document de synthèse est entièrement financé par l'Agence suédoise de coopération pour le développement SIDA. L'Agence SIDA n'adhère pas systématiquement aux opinions exprimées dans ce document. ARTICLE 19 assume l'entière responsabilité de son contenu.

Références

1. Voir, par exemple, le rapport du Groupe de travail du président des Etats-Unis sur les conduites illégales sur Internet **The electronic frontier: the challenge of unlawful conduct involving the use of the Internet**, mars 2001, qui stipule que « les individus qui souhaitent utiliser l'ordinateur en vue de faciliter des activités illégales peuvent penser que l'Internet fournit un moyen étendu, bon marché et potentiellement anonyme de commettre des actes tels que des fraudes, la vente ou la diffusion de pornographie infantile, la vente d'armes ou de drogues ou d'autres substances réglementées sans protection réglementaire ».

2. Voir ARTICLE 19 **Crackdown on End-to-End Encryption Threatens Free Expression and the Right to Privacy**, janvier 2015.

3. Numerama, Manuel Valls annonce une surveillance renforcée sur Internet, 21 janvier 2015

4. Voir, ARTICLE 19, ARTICLE 19 to UN Watchdog: Online Anonymity and Encryption Must Be Protected, contribution à l'appel à commentaires du Rapporteur spécial des Nations Unies sur la liberté d'expression sur l'anonymat et le chiffrement pour son rapport thématique 2015 au Conseil des droits de l'homme, février 2015.

5. Voir par exemple, Lord Neuberger, président de la Cour Suprême du Royaume-Uni, **What's in a name? Privacy and anonymous speech on the Internet**, 30 Septembre 2014; Lord Neuberger a souligné que la véritable identité de Junius, écrivain politique anglais célèbre et anonyme de la fin du XVIIIe siècle, demeure secrète jusqu'à ce jour.

6. Voir Comité des droits de l'homme, **Observation générale no. 34**, par. 45; la Déclaration conjointe de 2008 sur la diffamation des religions, et les lois relatives à la lutte contre le terrorisme et l'extrémisme ; **Goodwin c. Royaume-Uni**, [GC], no. 17488/90, par. 39, 27 mars 1996 ; Commission africaine des droits de l'homme et des peuples, **ACHPR / Res.62(XXXII)02** (2002); OEA, **Report on Terrorism and Human Rights**, OEA/Ser.L/V/II.1 16 Doc. 5 rev. 1 corr. (22 octobre 2002).

7. Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/29/32, 29 mai 2015 (Rapport 2015 du RS sur la liberté d'expression), par. 12, 16 et 56.

8. *Ibid.*, par. 53.

9. *Ibid.*, par. 31-35.

10. *Ibid.*, par. 40-41.

11. *Ibid.*, par. 36, 42-44.

12. *Ibid.*, par. 49-51.

13. Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/23/40, 17 avril 2013 (Rapport 2013 du RS sur la liberté d'expression), par. 47.

14. *Ibid.*, par. 48-49.

15. Par exemple, dans la **Recommandation No.R (99)5 sur la protection de la vie privée sur Internet (1999)**, le Comité des ministres du Conseil de l'Europe a noté « la nécessité de développer des techniques garantissant l'anonymat des personnes concernées et la confidentialité des informations échangées par le biais des « inforoutes » dans le respect des droits et libertés d'autrui et des valeurs d'une société démocratique. »

16. *Ibid.*

17. Cour européenne, **K.U. c. Finlande**, Appl. No. 2872/02, 2 décembre 2008, par. 49. La Cour européenne a jugé que la Finlande avait violé le droit au respect de la vie privée car elle avait manqué de mettre en place un cadre législatif permettant aux tribunaux et aux autorités chargées du maintien de l'ordre d'exiger la divulgation de l'identité des clients des FAI à des fins d'enquête criminelle.

18. Cour européenne des droits de l'homme, « Internet : la jurisprudence de la Cour européenne des droits de l'homme », 2011. http://www.echr.coe.int/Documents/Research_report_internet_FRA.pdf

19. Cour européenne, **Delfi c. Estonie**, App. No.64569/09, 10 octobre 2013.

20. Voir Access, **Access intervenes for the right to be anonymous online**, juin 2014.

21. Rapporteur spécial de l'OEA sur la liberté d'expression, **Freedom of Expression and the Internet**, 31 décembre 2013.

22. Ibid. par. 23; et par. 133-137.

23. Pour une revue de ces initiatives, voir **UNESCO, Etude mondiale sur le respect de la vie privée sur l'Internet et la liberté d'expression, 2012**, pp. 24-26.

24. Pour plus d'informations sur TOR, voir EFF, **7 Things You Should Know About TOR**, juillet 2014

25. Voir l'initiative de EFF, HTTPS everywhere: **https://www.eff.org/HTTPS-EVERYWHERE** ; https// protège la confidentialité des communications et ne confère pas l'anonymat en tant que tel.

26. D. Banisar, *Stopping Science: the Case of Cryptography*, Health Matrix, Vol 9:253, 1999. Dans le cadre de ce document, le « cryptage » se réfère au cryptage électronique. Toutefois, les principes généraux s'appliquent aussi à des formes analogues de cryptage.

27. *Ibid.* D'autres formes de clés peuvent comporter des mots de passe, voire même des données biométriques telles que des empreintes digitales.

28. *Ibid.*

29. Ce point souligne lui-même une série de problèmes additionnels qui dépassent le cadre de ce document. On peut toutefois remarquer que les délits informatiques peuvent entraver la recherche en sécurité selon la manière dont ces délits sont définis.

30. Voir en particuler la Convention sur la cybercriminalité du Conseil de l'Europe, 2001.

31. ARTICLE 19, **Legal Analysis of Kenya Cybercrime and Computer-Related Crimes Bill 2014** (en attente).

32. Commission internationale des juristes, **Bangladesh: Information Communication Technology Act Draconian Assault on Free Expression**, 20 novembre 2013.

33. Rapport 2013 du RS sur la liberté d'expression, *op.cit.* par. 89 et 92.

34. La recommandation intégrale est disponible **ici**.

35. Le rapport est disponible **ici**.

36. Voir Commission interaméricaine des droits de l'homme (CIDH), op. cit. par. 83.

37. Voir Recommandation CM/Rec(2012)4 sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, 2012.

38. Voir Assemblée parlementaire du Conseil de l'Europe, Commission des questions juridiques et des droits de l'homme, **Rapport sur les opérations massives de surveillance**, AS/Jur (2015) 01, 26 janvier 2015.

39. Cour européenne, *Murray c. Royaume-Uni*, (1996) 22 EHRR 29, par. 45; *Stott c. Brown*, [2000] UKPC D3; *Doe c. Etats-Unis*, 487 U.S. 201, 219.

40. Cour européenne, *Saunders c. Royaume-Uni,* App.No. 19187/91, [GC], 17 décembre 1996; Etats-Unis, *Fisher c. Etats-Unis*, 425 US 391.

41. Au Royaume-Uni, les clés de cryptage sont généralement considérées comme des clés physiques, voir *R c. S &A* [2008] EWCA Crim 2177

42. Aux Etats-Unis, la divulgation obligatoire des clés de cryptage est généralement considérée comme un témoignage soumis à un certain nombre d'exceptions, voir, entre autres, *Doe c. Etats-Unis,* 487 U.S. 201, 219 Justice Stevens dissenting.

43. *Ibid.*

44. **Arrangement** de Wassenaar; voir également Règlement (EC) No 428/2009, instituant un régime européen de contrôle des exportations.

45. Voir IETF, **RFC 1984** de 1996, **RFC 2804** de 2000 ou **RFC 3365** de 2002.

46. Voir IETF, **RFC 7435** de décembre 2014.

47. Voir Cour suprême des Etats-Unis, **Talley c. California**, 362 U.S. 60 (1960); Cour suprême des Etats-Unis, **McIntyre c. Ohio Elections Commission**, 514 U.S. 334 (1995), Cour suprême des Etats-Unis, **United States v Rumely, 345 US 41, 57; John Doe v 2theMart.com Inc**. 140 F Supp 2d 1088 (2001); voir également Cour suprême du Canada, **R c. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212.**

48. Par exemple, *Rafael Marques de Morais c. Angola*, Communication No. 1128/2002, 18 avril 2005, par. 6.8

49. Par exemple, *Hrico v. Slovakia*, 27 juillet 2004, Application No. 41498/99, par. 40.

50. Voir, par exemple Comité des droits de l'homme, *Rafael Marques de Morais c. Angola*, par 6.8. Le Comité des droits de l'homme a observé que « le critère de la nécessité implique la proportionnalité, c'est-à-dire que l'ampleur des restrictions imposées à la liberté d'expression doit être en rapport avec la valeur que ces restrictions visent à protéger ».

51. Par exemple en Chine, voir Reuters, **China to ban online impersonation accounts, enforce real-name registration**, 4 février 2015; ou en Russie où des blogueurs dans la catégorie "3 000 visiteurs" doivent s'enregistrer auprès de l'agence publique de régulation des médias, en utilisant des noms véritables et des renseignements personnels. S'ils manquent de le faire, les régulateurs peuvent demander aux fournisseurs d'accès ou aux administrateurs des sites concernés de fournir les noms et renseignements aux autorités. L'absence d'enregistrement ou de fourniture des informations personnelles est passible d'amendes administratives : voir HRW, **Russia: Veto Law to Restrict Online Freedom**, mai 2014.

52. Par exemple en Iran, voir Freedom House, Freedom on the Net report 2014, Iran country report; ou au Vietnam, voir Freedom House, **Freedom on the Net report 2014, Vietnam country report**.

53. Voir ARTICLE 19, Right to Blog (2013), pp. 17-18.

54. C.f., la **Recommandation CM/Rec (2011)7 on the new notion of media** stipule que des "dispositions peuvent être requises pour autoriser le recours à des pseudonymes (par exemple dans des réseaux sociaux) lorsqu'une divulgation de l'identité risque d'entraîner des mesures de rétorsion (par exemple en tant que conséquence de l'activisme dans le domaine politique ou des droits de l'homme) ».

55. Les **Principes directeurs relatifs aux entreprises et aux droits de l'homme,** Haut-Commissariat des droits de l'homme des Nations Unies, 2011.

56. Par exemple, les membres de la communauté gay tels que les Sisters of Perpetual Indulgence ont déploré que la politique de Facebook requérant de fournir sa véritable identité les a privés de la capacité d'affirmer leur identité. Voir Huffington Post, **Facebook Still Forcing LGBT People and Others to 'Authenticate' their Identities**, 27 mars 2015; pour des recommandations sur les bonnes pratiques, voir K.A. Heatherly, A. L. Fargo & J.A. Martin, **Anonymous Online Comments: the Law and Best Media Practices from Around the World**, octobre 2014, p. 14.

57. Voir Facebook, **What type of ID does Facebook accept?**

58. C'est le cas, par exemple, dans des pays aussi différents que le Vietnam, voir Freedom House, Rapport pays sur le Vietnam, op.cit.; ou le Royaume-Uni, voir Ss 21 et 22 de la Regulation of Investigatory Powers Act 2000.

59. C'est le cas, par exemple, dans des pays comme la France, voir The Verge, **Twitter Must Disclose Authors of Anti-Semitic Tweets, French Appeals Court Rules**, juin 2013; le Canada, voir par exemple l'affaire **R c. Spencer 2014 SCC 43** dans laquelle la Cour suprême canadienne a soutenu qu'un mandat a été requis pour que les FAI divulguent les informations des abonnés dans une enquête concernant la pornographie infantile ; ou le Royaume-Uni, voir Freedom House, **Freedom on the Net report 2014, US country report**.

60. Voir par ex. Etats-Unis, Dendrite International Inc c. John Doe 775 A 2s 758 (2000).

61. *Ibid.* Voir aussi au Royaume-Uni, *mith c. ADVFN Ltd* [2008] EWHC 1797 (QB), *Sheffield Wednesday c. Hargreaves* [2007] EWHC 2375 (QB) et J*ane Clift c. Martin Clarke* [2011] EWHC 1164. Les tribunaux britanniques ont refusé de délivrer des injonctions à Norwich Pharmacal dans la mesure où une ordonnance exigeant la divulgation de l'identité d'un utilisateur ayant posté des messages non diffamatoires, à peine diffamatoires ou un peu plus qu'abusifs aurait été disproportionnée ou aurait constitué une ingérence injustifiable.

62. Voir par ex. le Defamation Act 2013 au Royaume-Uni.

63. **Affaire C-70/10 Scarlet Extended SA c. Société belge des auteurs compositeurs et editeurs (SABAM)** (24 novembre 2011); la CJEU a jugé que les systèmes généralisés de filtrage d'Internet installés par les FAI pour empêcher l'échange de fichiers au moyen de logiciels d'échange d'archives (dits « peer-to-peer ») étaient incompatibles avec les droits fondamentaux. Le jugement a été fortement confirmé dans l'affaire **C-360/10 Sabam c. Netlog** (16 février 2012) qui a soulevé la même question liée aux réseaux sociaux.

64. En Chine, les utilisateurs finaux chinois peuvent utiliser des produits encryptés approuvés faits en Chine sans autorisation mais ces produits ne sont disponibles que par des canaux autorisés ; pour de plus amples informations sur la réglementation du chiffrement en Chine, voir également **Freshfields Bruckhaus Deringer**.

65. En Inde, les Directives prévoient que des individus ou des organisations sont autorisés à utiliser le chiffrement uniquement jusqu'à une longueur de clé de 40 bits sans autorisation du concédant (i.e. the DOT). L'utilisation d'une clé de chiffrement plus forte, en revanche, doit être autorisée. La clé de décryptage, divisée en deux parties, doit être déposée auprès du concédant ; voir CIS, **Encryption Standards and Practices** ou Peter Swire et Kenesa Ahmad, op.cit.

66. L'utilisation de clés de chiffrement d'une certaine longueur est également réglementée au Sénégal, voir Article 13 de la Loi N°2008-41 du 20 août 2008 relative à la Cryptologie.

67. En Egypte, l'Article 64 de la loi sur les telecommunications 2003 interdit le cryptage des communications personnelles sans le consentement des autorités et accorde aux opérateurs des télécommunications le droit de collecter des informations et des données précises sur leurs utilisateurs.

68. En 2011, l'autorité pakistanaise de régulation des télécommunications a enjoint tous les FAI d'interdire tout cryptage sur Internet ; voir ARTICLE 19, Pakistan: **Ban on Internet Encryption A Violation of Freedom of Expression**, septembre 2011. Ces ordres étaient vraisemblablement fondés sur la Section 54 du Pakistan Telecommunication (Re-Organisation) Act de 1996, qui autorise le gouvernement fédéral à accorder le droit à toute personne ou à des personnes d'intercepter des appels et des messages, ou de localiser des appels sur tout système de télécommunication « dans l'intérêt de la sécurité nationale ou par crainte d'une infraction ».

69. Pen America, **Global Chilling: The Effect of Mass Surveillance on International Writers**, 5 janvier 2015; HRW, **With Liberty to Monitor All: How Large Scale US Surveillance is harming Journalism, Law and American Democracy**, juillet 2014.

70. En Inde, par exemple, la section 84A de l'Information Technology (Amendment) Act de 2008 stipule que le « Gouvernement central peut, en vue de sécuriser l'utilisation des médias électroniques et de promouvoir la e-gouvernance et le e-commerce, prescrire les modes ou méthodes de cryptage » ; voir **l'Information Technology (Amendment) Act 2008**. De plus, les Directives élaborées par le Département des Télécommunications ('DOT') en 2007 pour l'octroi de licences d'exploitation des services Internet stipulent que l'utilisation du chiffrement de masse par des titulaires de licences n'est pas permis ; voir **Internet Services Guidelines**, 24 août 2007.

71. En Chine, le chiffrement est une affaire politique étroitement contrôlée par le gouvernement. En vertu des Réglementations relatives à l'administration du chiffrement commercial de 1999, la fabrication, l'utilisation, l'importation ou exportation de produits de cryptage doivent être approuvés par le gouvernement. Par exemple, les prduits cryptés ne peuvent être fabriqués que par des entreprises agréées par l'Etat, qui ne sont autorisées à produire que certains types et catégories de produits de cryptage. Voir Christopher T. Cloutier et Jane Y. Cohen, **Casting a Wide Net, China Encryption Restrictions**, 2011.

72. En Egypte, l'Article 13(8) de la Loi sur la réglementation des télécommunications de 2003 prévoit que l'Autorité nationale de régulation des télécommunications approuve les caractéristiques et les normes techniques des équipements de télécommunications. Il fixe également les règles et procédures régissant leur importation, leur vente et leur utilisation. De plus, l'Article 64 donne mandat aux opérateurs de télécommunications de fournir tous les équipements techniques, systèmes, logiciels et communications, qui permettent aux forces armées et aux agences de sécurité nationale d'exercer leur autorité dans le cadre de la loi.

73. Voir Banisar, *op. cit.*

74. Par exemple, les contrôles des exportations aux Etats-Unis ont été levés pour la plupart des produits depuis janvier 2000; voir **Export Administration Regulation**.

75. Voir Article 30 de la Loi no. 2004-575, 21 juin 2004 pour la confiance dans l'économie numérique.

76. Voir Article 14 de la Loi no. 2008-41 du 20 août 2008 sur la cryptologie.

77. Voir Christopher T. Cloutier et Jane Y. Cohen, op. cit.

78. En Ethiopie, par exemple, le gouvernement a récemment promulgué la Proclamation no. 761/2012 relative aux infractions de fraude dans les télécommunications, qui punit la fabrication, l'assemblage, l'importation ou les offres de vente de tout équipement de télécommunications sans autorisation du ministère du Développement des technologies de l'information et de la communication. Des peines de 10 à 15 ans de prison et des amendes de 100 000 à 150 000 Birr sont prévues. Par ailleurs, en vertu de la Section 3 (3), le ministère a le pouvoir de fixer les types de technologies qui ne nécessiteront pas des permis, et leurs normes techniques ; voir ARTICLE 19, **Ethiopia: Legal Analysis of Proclamation on Telecom Fraud Offences**, août 2012.

79. Aux Etats-Unis, les systèmes de séquestre de clés et la dénommée Clipper Chip ou puce Clipper ont été des sujet de conflit importants durant les Crypto Wars. En 1993, le gouvernement américain a exigé des fabricants de matériels de communications avec chiffrement intégré d'installer une puce créée par la NSA, la Clipper Chip. La clé de cryptage des appareils de communication serait scindée et transmise à deux agences gouvernementales qui la divulgueraient aux autorités chargées du maintien de l'ordre et aux agences de renseignement quand nécessaire. Cependant, le système a attiré des critiques généralisées à la fois à cause de l'implication de la NSA dans le processus et parce que le gouvernement devait détenir les clés. Dans une proposition ultérieure, le gouvernement a annoncé des mesures incitatives pour les fabricants de logiciels afin de développer des programmes dont les clés de chiffrement seraient déposées dans des bases de données gérées par des entités indépendantes ou des « tiers de confiance ». Chaque entité détiendrait une partie de la clé, et la divulguerait sur présentation d'une décision de justice par les forces de l'ordre et les agences de renseignements. Cette initiative n'a pas été plus fructueuse et les efforts déployés par le gouvernement américain en vue de l'adoption d'un système de séquestre de clés à l'échelon international ont échoué. Voir, Banisar, *op. cit.*

80. En Espagne, l'Article 43 de la Loi de 2014 sur les télécommunications stipule que le chiffrement peut être utilisé pour protéger la confidentialité des communications, mais son usage peut être soumis à certaines conditions. En particulier, il est possible d'imposer l'obligation de fournir des algorithmes ou des procédures de chiffrement aux agences gouvernementales en accord avec la loi. Cette disposition existait déjà dans la Loi 2003 relative aux télécommunications. On ignore si cette disposition a jamais été mise en place.

81. Au Royaume-Uni, par exemple, le non-respect d'une injonction de la cour requérant la divulgation est passible par mise en accusation de 5 ans d'emprisonnement dans des cas de sécurité nationale ou d'actes indécents à l'encontre d'enfants ou de deux années dans tout autre cas ; voir **Part III of the Regulation of Investigatory Powers Act 2000.** Pour une analyse détaillée des dispositions relatives au chiffrement dans cette loi, voir JUSTICE, **Freedom From Suspicion: Surveillance Reform for a Digital Age** (2011), pp 120-132. En France, en vertu de l'Article 36 de la Loi no. 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, la divulgation de clés de cryptage doit être autorisée par un juge. Le non-respect de cette disposition est passible d'une amende de 7500 EUR et 6 mois d'emprisonnement.

82. Par exemple, en 2012, le gouvernement des Pays-Bas a envisagé une loi qui aurait permis aux autorités chargées du maintien de l'ordre et aux agences de renseignement de s'ingérer à distance dans les systèmes informatiques, notamment l'effacement de données et l'installation de malwares ; voir Bits of Freedom, **Dutch Proposal to search and destroy foreign computers**, 18 octobre 2012; voir également la Loi sur le renseignement et la sécurité de 2002 (**Wet op de inlichtingen- en veiligheidsdiensten 2002**). De la même manière, le gouvernement britannique a récemment publié un Code de bonnes pratiques pour consultation publique qui autoriserait l'ingérence dans tout équipement produisant des émissions électromagnétiques, acoustiques et autres, ainsi que dans les contenus et les données des communications ; voir **Equipment Interference Code of Practice**, Projet pour consultation publique février 2015.

DEFENDING FREEDOM OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org