https://fr.necessaryandproportionate.org/text

Principes internationaux sur l’application des droits de l’Homme à la surveillance des communications

Translation revised by Reporters Sans Frontières

Version finale du 10 juillet 2013

Alors que les technologies de surveillance des communications ne cessent de progresser, les États manquent à leurs obligations de garantir que les lois et les régulations relatives à la surveillance des communications respectent les droits de l’homme et protègent de manière adéquate les droits à la vie privée et à la liberté d’expression. Ce document tente d'expliquer comment le droit international relatif aux droits de l'homme s'applique à l'environnement numérique actuel, en particulier dans le contexte de la généralisation et de l'évolution des technologies et des méthodes de surveillance des communications. Ces principes peuvent servir de guide aux organisations de la société civile, aux entreprises et aux États qui cherchent à déterminer si les lois et pratiques de surveillance en vigueur ou envisagées sont en conformité avec les droits de l'homme.

Ces fondements sont le fruit d'une consultation globale menée auprès des organisations de la société civile, des entreprises et des experts internationaux sur les aspects juridiques, politiques et technologiques de la surveillance des communications.

Préambule

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

Avant la démocratisation d'Internet, la surveillance des communications par l'État était limitée par l'existence de principes juridiques bien établis et par des obstacles logistiques inhérents au contrôle des communications. Au cours des dernières décennies, les barrières techniques à la surveillance se sont estompées. Dans le même temps, l'application des principes juridiques aux nouvelles technologies a perdu en clarté. L'explosion des communications numériques et des informations relatives à ces communications, également appelées "métadonnées des communications" (termes qui désignent les informations portant sur les communications d'une personne ou sur son utilisation d'appareils électroniques), la baisse des coûts de stockage et d'exploration de grands ensembles de données, ou encore la mise à disposition de données

personnelles par le biais de prestataires de service tiers, ont conféré à l'État des pouvoirs de surveillance sans précédent.[3]Parallèlement, notre conception des droits de l'homme n'a pas encore intégré les récentes évolutions et la modernisation des moyens de surveillance des communications utilisés par l'État, de la capacité de ce dernier à combiner et organiser les informations obtenues par différentes techniques de surveillance, ou de la sensibilité croissante des informations accessibles.

La fréquence à laquelle les États cherchent à accéder au contenu des communications ou aux métadonnées associées augmente considérablement, sans contrôle approprié.[4] Après consultation et analyse, les métadonnées relatives aux communications permettent de dresser un profil descriptif de la vie d'un individu, incluant entre autres des informations sur son état de santé, ses opinions politiques et religieuses, ses relations sociales et ses centres d'intérêts. Ces données sont tout aussi complètes, si ce n'est plus, que le seul contenu des communications.[5] Malgré ce risque élevé d'intrusion dans la vie privée des personnes et l'effet d'intimidation qu'il peut avoir sur les associations politiques ou autres, les instruments législatifs et réglementaires accordent souvent aux métadonnées une protection moindre. Ils ne limitent pas suffisamment la façon dont les agences gouvernementales peuvent manipuler ces informations, notamment pour les explorer, les partager et les conserver.

Pour que les États respectent réellement leurs obligations en matière de droits de l'homme au plan international dans le domaine de la surveillance des communications, ils doivent se conformer aux principes présentés ci-dessous. Ces principes s'appliquent à la surveillance exercée au sein d'un État ou la surveillance extraterritoriale. Ils sont mis en œuvre quel que soit l'objectif de la surveillance : application de la loi, sécurité nationale ou toute autre fin réglementaire. Ils concernent également l'obligation qui incombe à l'État de respecter les droits de chaque individu et de protéger ces droits contre d'éventuels abus commis par des acteurs non étatiques, et en particulier des entreprises privées.[6] Le secteur privé assume une responsabilité équivalente en termes de respect des droits de l'homme, car il joue un rôle déterminant dans la conception, le développement et la diffusion des technologies, dans la mise à disposition des services de communication et, le cas échéant, dans la coopération avec les activités de surveillance des États. Néanmoins, le champ d'application des présents principes est limité aux obligations des États.

Des technologies et Des Définitions en Pleine Évolution

Dans un contexte moderne, le concept de "surveillance des communications" désigne le contrôle, l'interception, la collecte, l'analyse, l'utilisation, la préservation, la conservation, la modification ou la consultation d'informations qui contiennent les communications passées, présentes ou futures d'une personne, ainsi que de toutes les informations qui sont relatives à ces communications. Les "communications" désignent toute activité, interaction ou transaction transmise de façon électronique, telle que le contenu des communications, l'identité des parties impliquées, les données de localisation (adresses IP, par exemple), les horaires et la durée des communications, ainsi que les identifiants des appareils utilisés.

Le caractère intrusif de la surveillance des communications est traditionnellement évalué sur la base de catégories artificielles et formelles. Les cadres légaux existants font la distinction entre le "contenu" et les "données hors contenu", les "informations sur l'abonné" et les "métadonnées", les données stockées et celles en transit, les données conservées dans leur emplacement d'origine et

celles transmises à un prestataire de services tiers.[7] Pourtant, ces distinctions ne sont plus appropriées pour mesurer le niveau d'intrusion entraîné par la surveillance des communications dans la vie privée et les relations sociales des individus. Il est admis de longue date que le contenu des communications nécessite une protection légale importante dans la mesure où il peut révéler des informations sensibles. Toutefois, il est maintenant clair que d'autres informations issues des communications d'un individu, telles que les métadonnées et d'autres formes de données hors contenu, peuvent fournir plus de renseignements sur cette personne que le contenu lui-même. Elles doivent donc bénéficier d'une protection équivalente. Aujourd'hui, qu'elles soient analysées séparément ou conjointement, ces informations peuvent permettre de déterminer l'identité d'un individu et d'en savoir plus sur son comportement, ses relations, son état de santé, son origine ethnique, sa couleur de peau, son orientation sexuelle, sa nationalité ou ses opinions. Elles peuvent également être utilisées pour établir une carte complète des déplacements et des interactions de cette personne dans le temps,[8] ou de toutes les personnes présentes à un endroit donné, par exemple dans le cadre d'une manifestation ou d'un rassemblement politique. Par conséquent, toutes les informations qui contiennent les communications d'une personne ou sont relatives à ces communications, et qui ne sont pas publiquement et facilement accessibles, doivent être considérées comme des "informations protégées". Elles doivent donc, à ce titre, bénéficier du plus haut niveau de protection au regard de la loi.

Pour évaluer le caractère intrusif de la surveillance des communications par l'État, il convient de prendre en considération non seulement le risque de divulgation des informations protégées, mais également les raisons pour lesquelles l'État recherche ces informations. Si la surveillance des communications a pour conséquence de révéler des informations protégées susceptibles d'exposer une personne à des enquêtes, des discriminations ou des violations des droits de l'homme, elle constitue à la fois une violation sérieuse du droit au respect de la vie privée et une atteinte à la jouissance d'autres droits fondamentaux tels que la liberté d'expression, d'association et d'engagement politique. En effet, ces droits ne sont effectifs que si les personnes ont la possibilité de communiquer librement, sans subir l'effet d'intimidation qu'engendre la surveillance gouvernementale. Il est donc nécessaire de rechercher, pour chaque cas particulier, tant la nature des informations collectées que l'usage auquel elles sont destinées.

Lors de l'adoption d'une nouvelle technique de surveillance des communications ou de l'extension du champ d'action d'une technique existante, l'État doit vérifier préalablement si les informations susceptibles d'être obtenues entrent dans le cadre des "informations protégées". Il est ensuite tenu de se soumettre à un examen par le pouvoir judiciaire ou à un mécanisme de supervision démocratique. Pour déterminer si les informations obtenues par le biais de la surveillance des communications doivent être considérées comme des "informations protégées", il est judicieux de prendre en compte non seulement la nature de la surveillance, mais aussi sa portée et sa durée. Une surveillance généralisée ou systématique peut entraîner la divulgation d'informations privées au-delà des données collectées individuellement. Elle est donc susceptible de conférer à la surveillance des informations non protégées un caractère intrusif nécessitant une protection renforcée.[9]

Pour déterminer si l'État peut ou non entreprendre une surveillance des communications faisant intervenir des informations protégées, il convient de se conformer aux principes ci-dessous.

Principes

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

Portée Légitime: La surveillance des communications par des autorités gouvernementales ne doit être autorisée par la loi que pour poursuivre un objectif légitime lié à la défense d'un intérêt juridique fondamental pour une société démocratique. Aucune mesure de surveillance ne doit donner lieu à une discrimination basée sur l'origine, la couleur de peau, le sexe, la langue, la religion, les opinions politiques ou autres, la nationalité, l'appartenance à un groupe social, la richesse, la naissance ou toute autre situation sociale.

Nécessité: Les lois permettant la surveillance des communications par l'État doivent limiter cette dernière aux éléments strictement et manifestement nécessaires pour atteindre un objectif légitime. Cette surveillance ne doit être utilisée que si elle constitue l'unique moyen d'atteindre un but légitime donné, ou, dans le cas où d'autres moyens existent, si elle représente celui qui est le moins susceptible de porter atteinte aux droits de l'homme. La charge de la preuve à cet égard incombe à l'État, pour les procédures judiciaires et législatives.

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

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

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

1. Il existe une forte probabilité pour qu'une infraction pénale grave ait été ou soit commise;
2. Il est possible d'obtenir la preuve d'une telle infraction en accédant à l'information protégée recherchée;
3. Les techniques d'investigation moins intrusives ont toutes été utilisées;
4. Les informations recueillies se limiteront à ce qui est raisonnablement pertinent au regard de l'infraction concernée, et toute information superflue sera rapidement détruite ou restituée;
5. Les informations sont consultées uniquement par l'autorité spécifiée et utilisées exclusivement aux fins pour lesquelles l'autorisation a été accordée.

Si l'État cherche à accéder à des informations protégées par le biais de la surveillance des communications à des fins non susceptibles d'exposer une personne à des poursuites pénales, des enquêtes, des discriminations ou des violations des droits de l'homme, il doit démontrer les points suivants à une autorité indépendante, impartiale et compétente:

1. D'autres techniques d'investigation moins intrusives ont été envisagées.;
2. Les informations recueillies se limiteront à ce qui est raisonnablement pertinent, et toute information superflue sera promptement détruite ou restituée à la personne concernée;
3. Les informations sont consultées uniquement par l'autorité spécifiée et utilisées exclusivement aux fins pour lesquelles l'autorisation a été accordée.

Autorité judiciaire compétente: Les décisions relatives à la surveillance des communications doivent être prises par une autorité judiciaire compétente, impartiale et indépendante. Cette autorité doit être:

1. distincte des autorités chargées de la surveillance des communications;
2. au fait des enjeux relatifs aux technologies de la communication et aux droits de l'homme, et compétente pour rendre des décisions judiciaires dans ces domaines;
3. disposer de ressources suffisantes pour exercer les fonctions qui lui sont assignées.

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

Notification des Utilisateurs: Les personnes concernées doivent être informées de toute décision autorisant la surveillance de leurs communications, dans un délai et des conditions leur permettant de faire appel de la décision. Elles doivent par ailleurs avoir accès aux documents présentés à l'appui de la demande d'autorisation. Les retards dans la notification ne se justifient que dans les cas suivants:

1. La notification porterait gravement atteinte à l'objet pour lequel la surveillance est autorisée, ou il existe un risque imminent de danger pour la vie des personnes;
2. L'autorisation permettant de retarder la notification est accordée par l'autorité judiciaire compétente en même temps que l'autorisation de surveillance;
3. La personne concernée est informée dès que le risque est levé ou dans un délai raisonnable (la plus courte de ces deux périodes étant retenue), et au plus tard lorsque la surveillance des communications prend fin. C'est à l'État qu'il incombe d'informer les personnes concernées, mais dans le cas où cette obligation ne serait pas remplie, les fournisseurs de services de communication sont libres d'informer les personnes de la

surveillance de leurs communications, que ce soit de leur propre initiative ou en réponse à une demande.

Transparence: Les États doivent faire preuve de transparence quant à l'utilisation et à la portée de leurs pouvoirs et techniques de surveillance des communications. Ils doivent publier au minimum les informations globales relatives au nombre de demandes approuvées et rejetées, une ventilation des demandes par fournisseur de services, par type d'enquête et par objectif. Les États doivent fournir aux individus des informations suffisantes pour leur permettre de comprendre pleinement la portée, la nature et l'application des lois autorisant la surveillance des communications. Ils doivent permettre aux fournisseurs de service de communiquer les procédures qu'ils appliquent en ce qui concerne la surveillance des communications par l'État, de respecter ces procédures et de publier des informations détaillées sur cette surveillance.

Contrôle Public: Les États doivent établir des mécanismes de contrôle indépendants pour garantir la transparence et la responsabilisation en matière de surveillance des communications.[11]Les instances de contrôle doivent avoir les pouvoirs suivants : accéder à toutes les informations potentiellement utiles concernant les actions de l'État, y compris, le cas échéant, à des informations secrètes ou confidentielles ; évaluer si l'État fait un usage légitime de ses prérogatives ; déterminer si l'État a publié de façon transparente et précise les informations relatives à l'utilisation et à la portée de ses pouvoirs et techniques de surveillance ; publier des rapports réguliers et toute autre information pertinente concernant la surveillance des communications. Ces mécanismes de contrôle indépendants doivent être mis en place en complément de tout contrôle interne déjà assuré par un autre organe du gouvernement.

Intégrité des Communications et Systèmes: Afin d'assurer l'intégrité, la sécurité et la confidentialité des systèmes de communication, et compte tenu du fait que toute atteinte à la sécurité pour des raisons d'État compromet presque toujours la sécurité en général, les États ne doivent pas contraindre les fournisseurs de services, ou les vendeurs de matériels et de logiciels, à inclure des fonctions de surveillance dans leurs systèmes, ou à recueillir et conserver certaines informations exclusivement dans le but de permettre une surveillance par l'État. La collecte et le stockage des données a priori ne doivent jamais être demandés aux fournisseurs de services. Les individus ayant le droit de s'exprimer de façon anonyme, les États doivent s'abstenir d'imposer l'identification des utilisateurs comme condition préalable pour l'accès à un service.[12]

Garanties Dans le Cadre de la Coopération Internationale: En réponse à l'évolution des flux d'informations ainsi que des technologies et services de communication, les États peuvent avoir besoin de demander l'assistance d'un fournisseur de services étranger. Les traités d'entraide juridique et les autres accords conclus entre les États doivent garantir que, lorsque plusieurs droits nationaux peuvent s'appliquer à la surveillance des communications, ce sont les dispositions établissant le plus haut niveau de protection pour les individus qui prévalent. Lorsque les États demandent de l'aide pour l'application du droit, le principe de double incrimination doit être appliqué. Les États ne doivent pas utiliser les processus d'entraide juridique ou les requêtes internationales portant sur des informations protégées dans le but de contourner les restrictions nationales relatives à la surveillance des communications. Les règles d'entraide juridique et autres accords doivent être clairement documentés, rendus publics et conformes au droit à une procédure équitable.

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

Signataires

1. Support for Information Technology Center - SITC

   (Egypt)

2. 7iber

   (Jordan)

3. Access

   (International)

4. Acción EsLaRed

   (Venezuela)

5. ActiveWatch - - Media Monitoring Agency

   (Romania)

6. Adil Soz - International Foundation for Protection of Freedom of Speech

   (Kazakhstan)

7. Africa Platform for Social Protection - APSP

   (Africa)

8. AGEIA Densi

   (Argentina)

9. AGEIA DENSI Colombia

(Colombia)

10. Agenda Social y Política para las y los Jóvenes 2011-2021.México.

    (México)

11. Agentura.ru

    (Russia)

12. AgoraVox

    (France)

13. Aktion Freiheit statt Angst

    (Germany)

14. ALCONSUMIDOR A.C.

    (Mexico)

15. Alfa-Redi

    (Latin America and Caribbean)

16. All India Peoples Science Network

    (India)

17. Alternatif Bilişim Derneği (Alternatif Bilişim) - Turkey

    (Turkey)

18. Alternative Law Forum

    (India)

19. Amnesty International USA

    (USA)

20. Arab Digital Expression Foundation

    (Egypt)

21. Arte Fora do Museu

    (Brasil)

22. Article 19

    (International)

23. Articultores

    (Argentina)

24. ASL19

    (Iran)

25. Asociación aLabs

    (Spain)

26. Asociación Civil por la Igualdad y la Justicia - ACIJ

    (Argentina)

27. Asociación Colombiana de Usuarios de Internet

    (Colombia)

28. Asociación de Abogados de Buenos Aires

    (Argentina)

29. Asociación de Internautas Spain

    (Spain)

30. Asociación para una Ciudadanía Participativa - ACI-Participa

    (Honduras)

31. Asociación Paraguaya De Derecho Informático Y Tecnológico - APADIT

    (Paraguay)

32. Asociación por los Derechos Civiles - ADC

(Argentina)

33. Aspiration

(United States)

34. Associação Brasileira de Centros de inclusão Digital – ABCID

(Brasil)

35. Associação Coolpolitics

(Portugal)

36. Associació Pangea Coordinadora Comunicació per a la Cooperació

(Spain)

37. Association for Freedom of Thought and Expression – AFTE

(Egypt)

38. Association for Progressive Communications - APC

(International)

39. Association for Proper Internet Governance

(Switzerland)

40. Association for Technology and Internet - APTI

(Romania)

41. Association of Caribbean Media Workers - ACM

(Trinidad and Tobago)

42. Association of Community Internet Center – APWKomitel

(Indonesia)

43. Australia Privacy Foundation - APF

(Australia)

44. Bahrain Center for Human Rights

    (Bahrain)

45. Bangladesh NGOs Network for Radio and Communication – BNNRC

    (Bangladesh)

46. BC Freedom of Information & Privacy Association (BC FIPA)

    (Canada)

47. Benetech

    (International)

48. Berlin Forum on Global Politics - BFoGP

    (Germany)

49. Big Brother Watch

    (United Kingdom)

50. Bits of Freedom

    (Netherlands)

51. Bolo Bhi

    (Pakistan)

52. Brasilian Institute for Consumer Defense - IDEC

    (Brasil)

53. British Columbia Civil Liberties Association - BCCLA

    (Canada)

54. Bytes for All

    (Pakistan)

55. Cairo Institute for Human Rights Studies

(Egypt)

56. Canadian Association of University Teachers (Association Canadienne des Professeures et Professeurs D'université)

    (Canada)

57. Canadian Friends Service Committee

    (Canada)

58. Casa de Derechos de Quilmes

    (Argentina)

59. Center for Democracy & Technology - CDT

    (United States)

60. Center for Digital Democracy

    (United States)

61. Center for Internet & Society India

    (India)

62. Center for Media Freedom & Responsibility - CMF

    (Philippines)

63. Center for Media Research - Nepal

    (Nepal)

64. Center for Media Studies and Peacebuilding

    (Liberia)

65. Center of Media Justice

    (United States)

66. Centre for Community Informatics Research, Development and Training

    (Canada)

67. Centre for Law and Policy Research India

    (India)

68. Centro de Estudios en Libertad de Expresión y Acceso a la Información - CELE

    (Argentina)

69. Centro de formação profissional Alzira de Aleluia

    (Brasil)

70. Centro de Tecnologia e Sociedade (CTS) da FGV

    (Brasil)

71. Centrum Cyfrowe Projekt: Polska

    (Poland)

72. CESAR - Recife Center for Advanced Studies and Systems

    (Brazil)

73. Chinese Association for Human Rights

    (Taiwan)

74. Citizen Lab

    (Canada)

75. Citizens Network Watchdog Poland

    (Poland)

76. Civil Initiative on Internet Policy

    (Kyrgyzstan)

77. Civil Society Information Society Advisory Council - CSISAC

    (International)

78. Clínica de Nuevas Tecnologías, Propiedad Intelectual y Sociedad de la Escuela

(Puerto Rico)

79. ClubComputer.at

(Austria)

80. Collaboration on International ICT Policy in total East and South Africa - CIPESA

(Uganda / East and Southern Africa)

81. Colnodo

(Colombia)

82. Comisión Colombiana de Juristas

(Colombia)

83. Comité Cerezo México

(Mexico)

84. Compliance Campaign

(Denmark)

85. Computer Professionals' Union in the Philippines - CPU

(Philippines)

86. Consumer Korea

(South Korea)

87. Consumers International

(International)

88. ContingenteMx

(Mexico)

89. Cooperativa Autogestionaria Sulá Batsú R.L.

(Costa Rica)

90. Cyber Arabs

(Middle East)

91. datapanik.org

(Belgium)

92. DAWN Network

(International)

93. Defending Dissent Foundation

(United States)

94. DeJusticia

(Colombia)

95. Delhi Science Forum

(India)

96. Digital Courage

(Germany)

97. Digital Enlightenment Forum

(Belgium)

98. Digital Rights Foundation

(Pakistan)

99. Digitterra

(International)

100. DiploFoundation

(Malta)

101. e-belarus.ORG

(Belarus)

102. E-demokracija.si

(Slovenia)

103. East European Development Institute

(Ukraine)

104. Egyptian Initiative for Personal Rights

(Egypt)

105. Electronic Frontier Finland - EFFI

(Finland)

106. Electronic Frontier Foundation - EFF

(International)

107. Electronic Frontiers Australia - EFA

(Australia)

108. Electronic Frontiers Italy - ALCEI

(Italy)

109. Electronic Privacy Information Center - EPIC

(United States)

110. Espacio Público

(Venezuela)

111. European Digital Rights - EDRI

(Europe)

112. European Information Society Institute - EISi

(Slovakia)

113. Fantsuam Foundation

(Nigeria)

114. Fight for the Future

(United States)

115. Foro Ciudadano de Participación por la Justicia y los Derechos Humanos - FOCO

(Argentina)

116. Foro de Periodismo Argentino - FOPEA

(Argentina)

117. Foundation for Community Educational Media - FCEM

(Thailand)

118. Foundation for Information Policy Research – FIPR

(United Kingdom)

119. Foundation for Media Alternatives - FMA

(Philippines / Asia Pacific)

120. Free Network Foundation

(United States)

121. Free Press

(United States)

122. Free Press Unlimited

(Netherlands)

123. Free Software Foundation Europe

(Europe)

124. Free Software Movement of India

(India)

125. Freedom Against Censorship Thailand (FACT)

(Thailand)

126. Freedom of the Press Foundation

(United States)

127. Fundación AccesArte

(El Salvador)

128. Fundación Ambio

(Costa Rica)

129. Fundación Andina para la Observación y el Estudio de Medios

(Ecuador)

130. Fundación Karisma

(Colombia)

131. Fundación para la Libertad de Prensa - FLIP

(Colombia)

132. Fundación Redes y Desarrollo - FUNREDES

(Dominican Republic)

133. Fundación Vía Libre

(Argentina)

134. German Working Group on Data Retention

(Germany)

135. Global Partners & Associates

(United Kingdom)

136. Global Voices Advocacy

(International)

137. Grupo de Software Libre de Cúcuta

(Colombia)

138. Guerrilla Translation

(Spain)

139. Gulf Center for Human Rights

(Arab Gulf region)

140. Hackerspace Rancho Electrónico

(Mexico)

141. Helsinki Foundation for Human Rights, Warsaw - HFHR

(Poland)

142. Hermes Center for Transparency and Digital Human Rights

(Italy)

143. Hiperderecho

(Peru)

144. Hong Kong Journalists Association

(Hong Kong SAR)

145. Human Rights Data Analysis Group

(International)

146. Human Rights Watch - HRW

(International)

147. HURIDOCS

(Switzerland)

148. ICT Consumers Association of Kenya - ICAK

(Kenya)

149. ICTWatch - Indonesian ICT Partnership

(Indonesia)

150. Independent Journalism Center from Moldova

(Republic of Moldova)

151. Index on Censorship

(United Kingdom)

152. Information Technology Law

(Belarus)

153. Initiative for Freedom of Expression

(Turkey)

154. Initiative für Netzfreiheit

(Austria)

155. Institute des Technologies de l'Information et de la Communication Pour le Developpement - INTIC4DEV

(Togo)

156. Institute for Reporters' Freedom and Safety

(Azerbaijan)

157. Institute for War and Peace Reporting - IWPR

(United Kingdom)

158. Instituto Baiano de Direito Processual Penal - IBADPP

(Brasil)

159. Instituto Bem Estar Brasil

(Brasil)

160. Instituto Brasileiro de Direito Da Informática

(Brasil)

161. Instituto Centroamericano de Estudios para la Democracia Social - DEMOS

(Guatemala)

162. Instituto NUPEF

(Brasil)

163. International Civil Liberties Monitoring Group

(Canada)

164. International Commission of Jurist - Kenya Section

(Kenya)

165. International Media Support - IMS

(International)

166. International Modern Media Institute

(Iceland)

167. Internet Governance Project, Syracuse University School of Information Studies

(United States)

168. Internet Protection Lab

(Netherlands)

169. Internet Society German Chapter e.V. (ISOC.DE e.V.)

(Germany)

170. Internet Society Palestine

(Palestine)

171. Internet Society Trinidad and Tobago Chapter

(Trinidad and Tobago)

172. InternetNZ

(New Zealand)

173. Internews

(United States)

174. Interzone Inc

(International)

175. IP Justice

(United States)

176. Iraqi Network for Social Media

(Iraq)

177. Iriarte & Asociados

(Peru)

178. ISOC Board of Trustees

(International)

179. ISOC Congo Chapter

(Congo)

180. IT for Change

(India)

181. Iuridicum Remedium, o.s.

(Czech Republic)

182. Jonction

(Mauritania, Senegal, Tanzania)

183. Jordan Open Source Association

(Jordan)

184. Journaliste en danger - JED

(Congo)

185. Kenya ICT Action Network - KICTANet

(Kenya)

186. Kenyan Ethical and Legal Issues Network

(Kenya)

187. Korean Progressive Network - JINBONET

(Korea)

188. La Quadrature du Net

(France)

189. Labdoo México

(Mexico)

190. Lakome.com

(Morrocco)

191. Latin American Network of Surveillance, Technology and Society Studies – LAVITS

(Latin America and Caribbean)

192. Liberty

(United Kingdom)

193. Liga Uruguaya de Defensa del Consumidor

(Uruguay)

194. Liga voor Mensenrechten vzw

(Belgium)

195. Massachusetts Pirate Party

(USA / Massachusetts)

196. May First / People Link

(International)

197. Media Action Grassroots Network - MAG-Net

(United States)

198. Media Development Centre

(Macedonia)

199. Media Rights Agenda - MRA

(Lagos, Nigeria)

200. Metamorphosis Foundation

(Macedonia)

201. MOGiS e.V. - A Voice for Victims

(Germany)

202. Movimento Mega

(Brasil)

203. National Coalition Against Censorship - NCAC

(United States)

204. National Union of Somali Journalists (NUSOJ)

(Somalia)

205. Nawaat

(Tunisia)

206. New York Chapter of the Internet Society

(United States)

207. Norwegian P.E.N

(Norway)

208. Observatorio Latinoamericano Para la Libertad de Expresión - OLA

(Latin America and Caribbean)

209. Oneworld: Platform for Southeast Europe – OWPSEE

(Western Balkans)

210. Ontario Humanist Society

(Ontario, Canada)

211. Open Internet Tools Project - Open ITP

(United States)

212. Open Knowledge Foundation

(United Kingdom)

213. Open Media and Information Companies Initiative – Open MIC

(United States)

214. Open Net Korea

(South Korea)

215. Open Rights Group

(United Kingdom)

216. Openmedia.ca

(Canada)

217. Pacific Freedom Forum

(Pacific Region)

218. Pakistan Press Foundation - PPF

(Pakistan)

219. Palestinian Center for Development & Media Freedoms - MADA

(Palestine)

220. Panoptykon Foundation

(Poland)

221. Paradigm Initiative Nigeria - PIN

(Nigeria / Africa)

222. Partners for Democratic Change Serbia

(Serbia)

223. PEN Canada

(Canada)

224. PEN International

(International)

225. People Who

(International)

226. Pirata España

(Spain)

227. Pirate Party of Russia

(Russia)

228. Privacy & Access Council of Canada

(Canada)

229. Privacy Activism

(United States)

230. Privacy First Foundation

(Netherlands)

231. Privacy International

(International)

232. Protege QV

(Cameroon)

233. Public Association "Journalists"

(Kyrgyzstan)

234. RedPaTodos

(Colombia)

235. Reporters Without Borders - RSF

(International)

236. Russian Pirate Youth Project

(Russia)

237. Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic - CIPPIC

(Canada)

238. Seattle Privacy Coalition

(United States)

239. SHARE Conference | SHARE Defense

(The Balkans)

240. Social Media Exchange

(Lebanon)

241. Society for Knowledge Commons

(India)

242. Software Freedom Law Centre

(India)

243. SonTusDatos.org

(Mexico)

244. South East European Network for Professionalization of Media - SEENPM

(South East Europe)

245. Southeast Asian Press Alliance

(South East Asia)

246. Statewatch

(United Kingdom)

247. Sulá Batsú

(Costa Rica)

248. Surveillance Studies Centre

(Canada)

249. Surveillance Studies Network

(International)

250. Swathanthra Malayalam Computing

(India)

251. TagMeNot
252. Taiwan Association for Human Rights

(Taiwan)

253. Tech To The People

(Estonia)

254. TechLiberty

(New Zealand)

255. TEDIC

(Paraguay)

256. Thai Netizen Network

(Thailand)

257. The Communisphere Project

(United States)

258. The Mother and Child Health and Education Trust

(Hong Kong)

259. The New Renaissance Network

(Sweden)

260. The Open Source Shoppe

(India)

261. The Pacific Islands News Association - PINA

(Pacific Islands)

262. ThoughtWorks

(International)

263. TransMediar-Pimentalab [at] Universidade Federal de São Paulo

(Brasil)

264. Uganda Harm Reduction Network(UHRN)

(Uganda)

265. University of Campinas - Research Group CTeMe (Knowledge, Technology and Market)

(Brasil)

266. University of São Paulo's Research Group on Access to Information Policies (GPoPAI-USP)

(Brasil)

267. Ushahidi

(International)

268. VECAM

(France)

269. VIBE!AT

(Austria)

270. Voices for Interactive Choice and Empowerment

(Bangladesh)

271. West African Journalists Association

(Mali)

272. WITNESS

(International)

273. Wlan Slovenija

(Slovenia)

274. Zwiebelfreunde e.V.

(Germany)

---

[1]Article 12 de la Déclaration universelle des droits de l'homme, article 14 de la Convention des Nations Unies sur les travailleurs migrants, article 16 de la Convention des Nations Unies sur la protection des droits de l'enfant, Pacte international relatif aux droits civils et politiques, article 17 du Pacte international relatif aux droits civils et politiques, conventions régionales dont l'article 10 de la Charte africaine des droits et du bien-être de l'enfant, article 11 de la Convention américaine des droits de l'homme, article 4 de la Déclaration de principe sur la liberté d'expression en Afrique, article 5 de la Déclaration américaine des droits et devoirs de l'homme, article 21 de la Charte arabe des droits de l'homme et article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, Principes de Johannesburg relatifs à la sécurité nationale, à la liberté d'expression et à l'accès à l'information, Principes de Camden sur la liberté d'expression et l'égalité.

[2]Article 29 de la Déclaration universelle des droits de l'homme ; observation générale n° 27 adoptée par le Comité des droits de l'homme à l'article 40, paragraphe 4, du Pacte international relatif aux droits civils et politiques, CCPR/C/21/Rev.1/Add.9, du 2 novembre 1999. Voir également le document "Report of the special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism" de Martin Scheinin, 2009, A/HRC/17/34.

[3]Les métadonnées relatives aux communications peuvent contenir des informations sur notre identité (données sur l'abonné et sur l'appareil utilisé), nos interactions (origines et destinations des communications, en particulier celles indiquant les sites consultés, les livres ou autres documents lus, les personnes contactées, les amis, la famille, les connaissances, les recherches effectuées et les ressources utilisées) et notre localisation (lieux et dates, proximité avec d'autres personnes). En résumé, elles conservent des traces de presque tous les actes accomplis dans le cadre de la vie moderne, et sont le reflet de nos humeurs, nos centres d'intérêts, nos projets et nos pensées les plus intimes.

[4]Par exemple, rien qu'au Royaume-Uni, près de 500 000 requêtes concernant les métadonnées relatives aux communications sont soumises chaque année, sous un régime d'auto-autorisation qui permet aux organismes chargés d'appliquer la loi d'autoriser leurs propres demandes d'accès aux informations détenues par les fournisseurs de services. Parallèlement, les données fournies par les rapports Transparence des informations de Google montrent qu'aux États-Unis, le nombre de requêtes concernant les données relatives aux utilisateurs est passé de 8 888 en 2010 à 12 271 en 2011. En Corée, près de 6 millions de requêtes concernant les informations relatives aux abonnés et aux internautes qui publient des messages, et quelque 30 millions de requêtes portant sur d'autres formes de métadonnées de communications ont été soumises chaque année en 2011 et 2012. Presque toutes ont été acceptées et exécutées. Les données de 2012 sont accessibles à l'adresse suivante:http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586

[5]Se reporter, par exemple, à une étude du travail de Sandy Pentland, "Reality Mining", dans la revue technologique du MIT (2008) disponible à l'adresse suivante:http://www2.technologyreview.com/article/409598/tr10-reality-mining/ Consulter également l'étude "Questioning lawful access to traffic data" réalisée par Alberto Escudero-Pascual et Gus Hosein, Communications of the ACM, volume 47, numéro 3, mars 2004, pages 77 à 82.

[6]Compte rendu du Rapporteur spécial des Nations Unies sur la promotion et la protection de la liberté d'opinion et d'expression, Frank La Rue, 3 juin 2013, disponible à l'adresse suivante: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

[7]"Les gens divulguent les numéros qu'ils appellent ou auxquels ils envoient des SMS à leurs opérateurs mobiles, les URL qu'ils consultent et les adresses e-mail avec lesquelles ils correspondent à leurs fournisseurs de services Internet, ainsi que les livres, les articles et les médicaments qu'ils achètent à leurs boutiques en ligne… On ne peut pas considérer que toutes ces informations, volontairement divulguées à certaines personnes dans un but spécifique, sont, de ce seul fait, exclues de la protection du 4e amendement de la Constitution." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., opinion concordante).

[8]"La surveillance à court terme des déplacements d'une personne sur la voie publique est compatible avec la protection de la vie privée", mais "l'utilisation de systèmes de surveillance GPS à plus long terme dans les enquêtes sur la plupart des infractions empiète sur le respect de la vie privée." United States v. Jones, 56 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J., opinion concordante).

[9]"La surveillance prolongée permet d'obtenir des informations qu'une surveillance à court terme ne révèle pas (telles que les actions réalisées à plusieurs reprises par un individu, celles qu'il n'effectue pas ou celles qu'il exécute en même temps). Ce type de donnée permet d'en savoir plus sur une personne comparativement à un déplacement considéré isolément. Des visites répétées à l'église ou chez un bookmaker, la fréquentation d'une salle de gym ou d'un bar, tout comme le fait de ne pas se rendre dans ces endroits pendant un mois, en disent plus long qu'une visite isolée. La séquence des déplacements d'une personne peut s'avérer encore plus révélatrice ; une seule consultation à un cabinet de gynécologie n'a pas grande signification, mais si ce rendez-vous est suivi quelques semaines plus tard d'une visite dans un magasin pour bébés, une toute autre version peut être donnée à l'histoire.* Toute personne parfaitement informée des déplacements d'un individu pourrait en déduire si ce dernier est un fervent pratiquant, un buveur invétéré, un habitué des clubs de sport, un mari infidèle, un patient en ambulatoire qui suit un traitement médical, ou bien encore un proche de tel ou tel individu ou un sympathisant d'un groupe politique. Il pourrait obtenir toutes ces informations, et pas seulement l'une d'entre elles." U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.)p. 562; U.S. v. Jones, 565 U.S. __, (2012), Alito, J., opinion concordante." De plus, lorsqu'elle est systématiquement collectée et stockée dans des fichiers détenus par les autorités, une information publique peut relever de la vie privée. Cela est encore plus vrai quand ces informations concernent le passé lointain d'une personne. De l'avis de la Cour, une telle information, lorsqu'elle est systématiquement collectée et stockée dans un fichier détenu par des agents de l'État, relève de la "vie privée" au sens de l'article 8 (1) de la Convention." (Rotaru v. Romania, [2000] ECHR 28341/95, paragraphes 43-44.

[10]Le terme "procédure équitable" peut être utilisé de manière interchangeable avec "équité procédurale" et "justice naturelle". Il est clairement défini dans l'article 6(1) de la Convention européenne des droits de l'homme et l'article 8 de la Convention américaine relative aux droits de l'homme.

[11]Le commissaire britannique à l'interception des communications est un exemple qui illustre ce type de mécanisme de contrôle indépendant. L'ICO publie un rapport comprenant des données agrégées, mais ne fournit pas de données suffisantes permettant d'examiner les types de demandes, l'étendue de chaque demande d'accès, leur objectif et l'examen dont elles font l'objet. Se reporter à la page http://www.iocco-uk.info/sections.asp?sectionID=2&type=top.

[12]Compte rendu du Rapporteur spécial des Nations Unies sur la promotion et la protection de la liberté d'opinion et d'expression, Frank La Rue, 16 mai 2011, A/HRC/17/27, paragraphe 84.