https://es.necessaryandproportionate.org/text

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones

Traducción por Comisión Colombiana de Juristas, Access, Fundación Karisma, Fundación Vía Libre.

Versión Final 10 de Julio de 2013

A medida que avanzan las tecnologías que facilitan la vigilancia estatal de las comunicaciones, los Estados están fracasando en garantizar que las leyes y regulaciones relacionadas con la vigilancia de las comunicaciones estén de acuerdo con el derecho internacional de los derechos humanos y protejan adecuadamente los derechos a la privacidad y a la libertad de expresión. Este documento intenta explicar cómo se aplica el derecho internacional de los derechos humanos en el actual entorno digital, particularmente a la luz del aumento de las tecnologías y técnicas de vigilancia de las comunicaciones, y los cambios en ellas. Estos principios pueden proporcionar a los grupos de la sociedad civil, a la industria y a los Estados un marco para evaluar si las leyes y prácticas de vigilancia, actuales o propuestas, son consistentes con los derechos humanos.

Estos principios son el resultado de una consulta global con grupos de la sociedad civil, con la industria y con expertos internacionales en legislación sobre vigilancia de las comunicaciones, políticas públicas y tecnología.

Preámbulo

La privacidad es un derecho humano fundamental y es primordial para el mantenimiento de sociedades democráticas. Es esencial a la dignidad humana y refuerza otros derechos, tales como la libertad de expresión y de información, y la libertad de asociación, y se encuentra reconocido por el derecho internacional de los derechos humanos.[1]

Las actividades que restringen el derecho a la privacidad, incluida la vigilancia de las comunicaciones, solo pueden justificarse cuando son prescritas por ley, necesarias para alcanzar un objetivo legítimo y proporcionales al fin perseguido[2].

Antes de la adopción pública de Internet, principios jurídicos bien definidos y dificultades logísticas inherentes al monitoreo de las comunicaciones crearon límites a la vigilancia de las comunicaciones por parte del Estado. En décadas recientes, esas dificultades logísticas en la vigilancia han disminuido y la aplicación de principios jurídicos en los nuevos contextos tecnológicos se ha vuelto poco clara. La explosión del contenido digital en las comunicaciones y

de la información acerca de ellas, o "metadatos de comunicaciones" (información sobre las comunicaciones o el uso de dispositivos electrónicos de una persona), el costo cada vez menor de almacenamiento y minería de grandes cantidades de datos y el suministro de contenido personal a través de terceros proveedores de servicios, hacen posible la vigilancia estatal a una escala sin precedentes.[3]

Mientras tanto, las concepciones de la legislación vigente en materia de derechos humanos no se han mantenido a tono con las modernas y cambiantes capacidades estatales de vigilancia de comunicaciones, la aptitud del Estado para combinar y organizar la información obtenida mediante distintas técnicas de vigilancia, o la creciente susceptibilidad de la información a la que se puede acceder.

La frecuencia con la que los Estados procuran acceder tanto al contenido de las comunicaciones cuanto a sus metadatos aumenta drásticamente, sin controles adecuados.[4]

Acceder a los metadatos de las comunicaciones y analizarlos permite crear perfiles de la vida de las personas, incluyendo estado de salud, opiniones políticas y religiosas, asociaciones, interacciones e intereses, revelando tanto o más detalle que el que podría apreciarse a partir del contenido de las comunicaciones. [5].Los instrumentos legislativos y de políticas públicas a menudo otorgan a los metadatos de comunicaciones un menor nivel de protección, y no imponen restricciones suficientes sobre cómo puedan ser posteriormente utilizados por los organismos del Estado --incluyendo la forma en que son minados, compartidos y conservados-- a pesar del vasto potencial de intromisión en la vida de las personas y el efecto amedrentador sobre las asociaciones políticas y de otros tipos.

Para satisfacer sus obligaciones internacionales de derechos humanos en lo relativo a la vigilancia de las comunicaciones, los Estados deben cumplir con los principios que se presentan más abajo. Estos se aplican tanto a la vigilancia realizada dentro de las fronteras del Estado cuanto extraterritorialmente. Los principios deben ponerse en práctica con independencia de la finalidad de la vigilancia, sea esta el cumplimiento de la ley, la seguridad nacional o cualquier otro propósito normativo, y se aplican no solamente en relación con la obligación del Estado de respetar y garantizar los derechos individuales, sino también respecto de la obligación de proteger los derechos de las personas ante abusos por parte de actores no estatales, incluidas las personas jurídicas.[6]

El sector privado carga con la misma responsabilidad de respetar los derechos humanos, en particular considerando el rol clave que cumple en diseñar, desarrollar y difundir tecnologías, activar y suministrar comunicaciones y, cuando se le requiere, cooperar con las actividades de vigilanciadel Estado. Sin embargo, el alcance de los presentes Principios se limita a las obligaciones del Estado.

Cambio de tecnología y definiciones

«Vigilancia de comunicaciones» en el entorno moderno comprende monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas. «Comunicaciones» abarca las actividades, interacciones y transacciones transmitidas por medios

electrónicos, tales como el contenido, la identidad de las partes, información de rastreo de ubicación incluyendo direcciones IP, momento y duración de las comunicaciones, e identificadores de los equipos utilizados.

Tradicionalmente, el carácter invasivo de la vigilancia de las comunicaciones ha sido evaluado sobre la base de categorías artificiales y formalistas. Los marcos legales existentes distinguen entre "contenido" o "no contenido", "información del suscriptor" o "metadatos", datos almacenados o datos en tránsito, datos que se tienen en el hogar o en la posesión de un tercero proveedor de servicios.[7]

Sin embargo, estas distinciones ya no son apropiadas para medir el grado de intromisión que la vigilancia de las comunicaciones realiza en la vida privada y las relaciones de las personas. Aunque desde hace tiempo se ha acordado que el contenido de la comunicación merece una protección significativa en la ley debido a su capacidad de revelar información sensible, ahora está claro que existe otra información que surge de las comunicaciones, y datos que no son contenido, que puede revelar incluso más acerca de una persona que el contenido en sí, y por lo tanto merece una protección equivalente. Hoy en día, cada uno de estos tipos de información, por sí sola o analizada colectivamente, puede revelar la identidad de una persona, su comportamiento, sus asociaciones, sus condiciones físicas o estado de salud, su raza, color, orientación sexual, origen nacional o puntos de vista, o puede permitir el mapeo de la ubicación de la persona, sus movimientos e interacciones en el tiempo[8], o puede hacer esto respecto de todas las personas en una ubicación determinada, incluyendo una manifestación pública u otro acontecimiento político. Como resultado, toda la información que incluye, refleja, surge de o es sobre las comunicaciones de una persona y que no está disponible ni es de fácil acceso para el público general, debería ser considerada como "información protegida", y por lo tanto se le debería dar la más alta protección de la ley.

Al evaluar el carácter invasivo de la vigilancia de las comunicaciones por el Estado, es necesario considerar la potencialidad de la vigilancia de revelar información protegida, así como la finalidad para la que el Estado procura la información. La vigilancia de las comunicaciones que posiblemente de lugar a revelar información protegida que pueda poner a una persona en riesgo de ser investigada, de sufrir discriminación o de violación de sus derechos humanos, constituirá una infracción grave a su derecho a la privacidad, y también afectará negativamente el disfrute de otros derechos fundamentales, incluyendo las libertades de expresión, de asociación y de participación política. Ello es así porque estos derechos requierenque las personas sean capaces de comunicarse libres del efecto amedrentador de la vigilancia gubernamental. Será pues necesario en cada caso específico determinar tanto el carácter como los posibles usos de la información que se procura.

Al adoptar una nueva técnica de vigilancia de las comunicaciones o ampliar el alcance de una existente, el Estado debe determinar, antes de buscarla, si la información que podría ser adquirida cae en el ámbito de la "información protegida", y debería someterse a escrutinio judicial u otro mecanismo de control democrático. La forma de la vigilancia, así como su alcance y duración, son factores relevantes para determinar si la información obtenida a través de la vigilancia de las comunicaciones alcanza el nivel de "información protegida". Puesto que el monitoreo generalizado o sistemático tiene la capacidad de revelar información privada que excede en

mucho la suma de valor informativo de los elementos individuales recogidos, puede elevar la vigilancia de información no protegida a un nivel invasivo que exija una mayor protección.[9]

Determinar si el Estado puede llevar a cabo vigilancia de comunicaciones que interfiera con información protegida debe ser compatible con los siguientes principios:

Los Principios

Legalidad: Cualquier limitación al derecho a la privacidad debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un nivel de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Dado el ritmo de los cambios tecnológicos, las leyes que limitan el derecho a la privacidad deben ser objeto de revisión periódica por medio de un proceso legislativo o reglamentario de carácter participativo.

Objetivo Legítimo: Las leyes sólo deberían permitir la vigilancia de las comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

Necesidad: Las leyes que permiten la vigilancia de las comunicaciones por el Estado deben limitar dicha vigilancia a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La vigilancia de las comunicaciones sólo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado.

Idoneidad: Cualquier caso de vigilancia de las comunicaciones autorizado mediante ley debe ser apropiado para cumplir el objetivo legítimo específico identificado.

Proporcionalidad: La vigilancia de las comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos a la privacidad y la libertad de opinión y de expresión, amenazando los cimientos de una sociedad democrática. Las decisiones sobre la vigilancia de las comunicaciones deben tomarse sopesando el beneficio que se persigue contra el daño que se causaría a los derechos de las personas y contra otros intereses en conflicto, y debería incluir un examen de la sensibilidad de la información y de la gravedad de la infracción al derecho a la privacidad.

En concreto, esto requiere que si un Estado busca acceder o usar información protegida obtenida a través de vigilancia de las comunicaciones en el marco de una investigación penal, debe establecer ante una autoridad judicial competente, independiente e imparcial que:

1. existe un alto grado de probabilidad de que un grave delito ha sido cometido o será cometido;
2. la evidencia sobre tal delito sería obtenida al acceder a la información protegida que se busca;
3. otras técnicas de investigación que son menos invasivas y están disponibles ya han sido agotadas;
4. la información a la que se accede se limitará a la razonablemente relevante para el presunto delito y cualquier exceso en la información recopilada será destruido o devuelto sin demora, y
5. solo tendrá acceso a la información la autoridad especificada y se utilizará solo para el propósito para el cual se le dio autorización.

Si el Estado busca el acceso a la información protegida a través de la vigilancia de las comunicaciones para un propósito que no pone a una persona en riesgo de persecución penal, investigación, discriminación o violación de derechos humanos, el Estado debe establecer ante una autoridad independiente, imparcial y competente que:

1. otras técnicas de investigación que son menos invasivas y están disponibles han sido consideradas;
2. la información a la que se accede se limitará a la que sea razonable y relevante y cualquier exceso de información recopilada será destruido o devuelto a la persona afectada sin demora, y
3. a la información solo tendrá acceso la autoridad especificada y se utilizará solo para el propósito para el cual se le dio autorización.

Autoridad Judicial Competente: Las decisiones relacionadas con la vigilancia de las comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente. La autoridad debe (1) estar separada de las autoridades encargadas de la vigilancia de las comunicaciones, (2) ser experta en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la vigilancia de las comunicaciones, las tecnologías utilizadas y los derechos humanos, y (3) tener los recursos adecuados en el ejercicio de las funciones que se le asignen.

Debido proceso: El debido proceso exige que los Estados respeten y garanticen los derechos humanos de las personas asegurando que los procedimientos legales que rigen cualquier interferencia con los derechos humanos estén enumerados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público general. Específicamente, al decidir sobre sus derechos, toda persona tiene derecho a una audiencia pública y justa dentro de un plazo razonable por un tribunal independiente, competente e imparcial establecido por ley,[10]

salvo en casos de emergencia donde exista un riesgo inminente de peligro para la vida humana. En tales casos, debe buscarse una autorización con efecto retroactivo dentro de un plazo razonable y factible. El mero riesgo de fuga o de destrucción de pruebas no se considerará suficiente para justificar la autorización con efecto retroactivo.

Notificación del usuario: Las personas deberían ser notificados de una decisión que autoriza la vigilancia de las comunicaciones con el tiempo e información suficientes para permitirles apelar

la decisión, y deberían tener acceso a los materiales presentados en apoyo de la solicitud de autorización. El retraso en la notificación sólo se justifica en las siguientes circunstancias:

1. La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana; o
2. La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia; y
3. La persona afectada es notificada tan pronto como el riesgo desaparece o dentro de un período de tiempo razonable y factible, según lo que ocurra primero, y en todo caso en el momento en que la vigilancia de las comunicaciones se ha completado. La obligación de notificar recae en el Estado, pero en el caso de que el Estado no haya dado aviso, los proveedores de servicios de comunicaciones estarán en libertad de notificar a las personas de la vigilancia de las comunicaciones, sea de manera voluntaria o bajo pedido.

Transparencia: Los estados deberían ser transparentes sobre el uso y el alcance de las técnicas y los poderes de la vigilancia de las comunicaciones. Deberían publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, según el tipo de investigación y sus propósitos. Los Estados deberían proporcionar a las personas la información suficiente para que puedan comprender plenamente el alcance, la naturaleza y la aplicación de las leyes que permiten la vigilancia de las comunicaciones. Los Estados deberían permitir que los proveedores de servicios publiquen los procedimientos que ellos aplican cuando se trata de la vigilancia de las comunicaciones por el Estado, adherir a esos procedimientos y publicar los registros de vigilancia de las comunicaciones del Estado.

Supervisión pública: Los estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones[11]

Los mecanismos de supervisión deberían tener la autoridad para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado, incluyendo, cuando sea el caso, el acceso a información secreta o clasificada, para valorar si el Estado está haciendo un uso legítimo de sus funciones legales, para evaluar si el Estado ha sido transparente y ha publicado información precisa sobre el uso y el alcance de las técnicas y poderes de vigilancia de las comunicaciones; y para publicar periódicamente informes y otra información relevante para la vigilancia de las comunicaciones. Deberían establecerse mecanismos de supervisión independientes adicionales a cualquier supervisión ya proporcionada a través de otra rama del poder.

Integridad de las comunicaciones y sistemas: Con el fin de garantizar la integridad, la seguridad y la privacidad de los sistemas de comunicaciones, y en reconocimiento del hecho de que poner en peligro la seguridad del Estado casi siempre pone en peligro la seguridad en términos generales, los Estados no deberían obligar a los proveedores de servicios o proveedores de hardware o software a construir la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de vigilancia del Estado. La retención o la recopilación de datos a priori nunca debe ser exigida a los proveedores de servicios. Las personas tienen el derecho a expresarse anónimamente, por lo que los Estados

deberían abstenerse de obligar a la identificación de los usuarios como condición previa para la prestación de servicios[12]

Garantías para la cooperación internacional: En respuesta a los cambios en los flujos de información y en las tecnologías y servicios de comunicaciones, los Estados pueden necesitar buscar la asistencia de un proveedor de servicios extranjero. En consecuencia, los tratados de asistencia jurídica mutua (MLAT) y otros acuerdos celebrados entre Estados deben asegurarse de que, cuando la legislación de más de un Estado pudiera aplicarse a la vigilancia de las comunicaciones, la que se adopte sea la norma disponible con el mayor nivel de protección para las personas. Cuando los Estados buscan asistencia para efectos hacer cumplir su legislación interna, debería ser aplicado el principio de la doble incriminación. Los Estados no pueden utilizar los procesos de asistencia judicial recíproca y las solicitudes extranjeras de información protegida para evitar las restricciones de derecho interno relativas a la vigilancia de las comunicaciones. Los procesos de asistencia jurídica mutua y otros acuerdos deben estar claramente documentados, a disposición del público y sujetos a las garantías de imparcialidad procesal.

Garantías contra el acceso ilegítimo: Los Estados deberían promulgar leyes que penalicen la vigilancia ilegal de las comunicaciones por parte de agentes públicos o privados. La ley debería proveer sanciones penales y civiles suficientes y significativas, proteger a los denunciantes (whistle blowers) y prever mecanismos de resarcimiento a las personas afectadas. Las leyes deberían estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como prueba en cualquier procedimiento, al igual que cualquier evidencia derivada de dicha información. Los Estados también deben promulgar leyes que establezcan que, después de que el material obtenido a través de la vigilancia de las comunicaciones ha sido utilizado para el propósito para el cual fue dada la información, el material debe ser destruido o devuelto a la persona.

Firmantes

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]Declaración Universal de Derechos Humanos, Artículo 12, Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares, Artículo 14, Convención sobre los Derechos del Niño de Naciones Unidas, Artículo 16, Pacto Internacional de Derechos Civiles y Políticos Artículo 17; convenciones regionales incluido Artículo 10 Del Capítulo Africano Carta sobre los Derechos y el Bienestar del Niño, Artículo 11 de la Convención Americana de Derechos Humanos, Artículo 4 de los principios de la Unión Africana sobre la Libertad de Expresión, Artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre, Artículo 21 de la Carta Árabe de Derechos Humanos, y Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; Principios de Johannesburgo sobre la Seguridad Nacional, Expresión y Acceso a la Información, Principios de Camden para la Libertad de Expresión y la Igualdad Libre.

[2]Declaración Universal de Derechos Humanos, Artículo 29; Comentarios Generales No. 27, Adoptado por el Comité de Derechos Humanos bajo el Artículo 40, Parágrafo 4 del Pacto Internacional de Derechos Civiles y Políticos, CCPR/C/21/Rev.1/Add.9, Noviembre 2, 1999; Ver también Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[3]Los metadatos de las comunicaciones pueden incluir información acerca de nuestras identidades (información del abonado, información del dispositivo), las interacciones (origen y destino de las comunicaciones, especialmente las que muestran los sitios web visitados, los libros y otros materiales de lectura, las personas interactuaron con los amigos, familia, conocidos, búsquedas realizadas, los recursos utilizados) y ubicación (lugares y tiempos, proximidades a otros), en suma, los metadatos proporciona una ventana a casi todas las acciones en la vida moderna, nuestros estados mentales, los intereses, las intenciones y los pensamientos más íntimos.

[4]Por ejemplo, solamente en el Reino Unido existe aproximadamente 500.000 solicitudes de acceso a los metadatos de las comunicaciones todos los años, actualmente bajo un régimen de auto-autorización, los servicios policiales puedan autorizar la solicitud de acceso a la información en poder de los proveedores de servicios. Mientras tanto, los datos proporcionados por los informes de transparencia de Google muestran que las solicitudes de datos de los usuarios de los EE.UU. aumentaron solamente de 8.888 en 2010 a 12.271 en 2011. En Corea, cada año había alrededor de 6 millones de solicitudes de abonados de información y alrededor de 30 millones de solicitudes de otras formas de metadatos de comunicaciones en el período 2011-2012, casi de todo lo cual se entregó y se ejecuta. Los datos del año 2012 están disponibles en http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586

[5]Ver la revisión del trabajo de Sandy Petland, 'Reality Mining', en MIT's Technology Review, 2008, disponible en http://www2.technologyreview.com/article/409598/tr10-reality-mining/ y ver también Alberto Escudero-Pascual y Gus Hosein, 'Questioning lawful access to traffic data', Communications of the ACM, Vólumen 47 Issue 3, Marzo 2004, páginas 77 - 82.

[6]Reporte del Relator de Naciones Unidas sobre la Promoción y Protección de la Libertad de Opinión y Expresión, Frank La Rue, 16 de Mayo 2011, disponible en http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

[7]"People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[8] "People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[9]"Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.* A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." 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., concurring. "Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past…In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for the purposes of Article 8(1) of the Convention." (Rotaru v. Romania, [2000] ECHR 28341/95, paras. 43-44.

[10] El término "debido proceso" puede utilizarse de manera intercambiable con "justicia procesal" y "justicia natural" y está bien articulado en el Convenio Europeo de Derechos Humanos del artículo 6(1) y el artículo 8 de la Convención Americana sobre Derechos Humanos.

[11] El Comisionado de Interceptación de Comunicaciones del Reino Unido es un ejemplo de un mecanismo de supervisión independiente de ese tipo. El ICO publica un informe que incluye algunos datos agregados pero no proporciona datos suficientes para examinar los tipos de solicitudes, la extensión de cada petición de acceso, el propósito de las solicitudes, y el escrutinio que se aplica a ellos. Ver http://www.iocco-uk.info/sections.asp?sectionID=2&type=top.

[12] Informe del Relator Especial de Naciones Unidas sobre la protección y promoción del derecho a la libertad de opinión y expresión, Frank La Rue, 16 Mayo 2011, A/HRC/17/27, para 84.