Boletín N° 11.037-07

Proyecto de reforma constitucional, iniciado en moción de los Honorables Senadores señores Ossandón y Girardi, que incorpora un numeral nuevo en el artículo 19 de la Carta Fundamental, para consagrar el derecho al acceso a internet y la especial protección a la vida privada en ambientes digitales.

Antecedentes e ideas matrices

El desarrollo de Internet ha generado no solo grandes progresos para el ser humano, sino que también nuevos desafíos que subyacen en esos avances.

Uno de ellos, y de los más relevantes en el último tiempo, es el triángulo que forman las permanentes necesidades de conectividad, con el ejercicio de la libertad de expresión y la custodia de la privacidad de las personas en sus actividades en línea.

La Internet moderna ha superado el modelo lineal de intercambio de información, en el cual un usuario requería los datos desde un proveedor en cualquier parte del mundo. El nuevo modelo genera múltiples interacciones, convirtiendo al usuario en un generador de contenidos y, en tal esquema, la persona -o al menos su personalidad en línea- es la pieza central de interés para algunas líneas de negocios, así como para los Estados.

Tal es el caso de la publicidad en línea, que a través del conocimiento de los hábitos de navegación o de consumo de información de una persona, puede entregar publicidad segmentada de acuerdo a dichos parámetros[1], siendo más eficiente para el anunciante; pero al mismo tiempo, es una ventana de discusión respecto del derecho que asiste al usuario para la conservación del anonimato o privacidad.

Lo indudable de toda esta discusión, es que Internet se ha convertido en la fuente más importante de datos sobre las personas que jamás haya existido en la historia, ya sea a través de información directa y personal que pueda ser almacenada sobre los usuarios, así como los metadatos generados por las actividades realiza y servicios que consume la persona en la red; y, obviamente, los contenidos que los propios usuarios disponibilizan en Internet.

La visión de los organismos internacionales

El 1 de julio de 2016, el Consejo de Derechos Humanos, en el marco de la Asamblea General de las Naciones Unidas, dictó la resolución 32/13, siendo apoyado por más de 70 Estados, para la promoción, protección y disfrute de los derechos humanos en Internet.

Dicho acto de Naciones Unidas tiene una gran relevancia en el reconocimiento del ejercicio de los derechos humanos en ambientes digitales: los derechos de las personas deben ser protegidos también cuando su ejercicio se realiza en Internet, “en particular la libertad de expresión, que es aplicable sin consideración de fronteras y

por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos”[2].

El reconocimiento no nace por mero capricho de los Estados, sino que más bien se ha motivado por una serie de hechos de gran relevancia internacional respecto del uso de tecnologías de la información y también se ha inspirado en los atentados que los Estados han cometido en contra de la libertad de expresión y privacidad en el ambiente digital[3].

Uno de los casos de mayor relevancia fue el de “La Primavera Árabe”, en el cual Egipto sufrió un bloqueo completo de servicios de Internet[4], y un bloqueo parcial de los sistemas de telefonía celular con motivo de las protestas civiles que se desarrollaban en el país.

El régimen de Hosni Mubarak ordenó a las cuatro compañías de telecomunicaciones egipcias - Link Egypt, Vodafone/Raya, Telecom Egypt y Etisalat Misr - que “cortaran” la conexión del país con el resto del mundo y dispusieran del envío de mensajes de propaganda pro-régimen, poniendo en efecto un sistema de censura para evitar el conocimiento público de las graves protestas y hechos de violencia que acontecían en el país dejando, de paso, sin acceso a la red a más de 16 millones de usuarios.

Asimismo, las compañías de telecomunicaciones fueron forzadas a facilitar información para la identificación de los disidentes[5], profundizando aún más la crisis de derechos humanos desatada en el país.

El ejemplo egipcio daría lugar a otros episodios liderados por gobiernos, siempre fundamentados en razones políticas de dudosa procedencia.

Tal fue el caso de Turquía[6] quienes, tras una enmienda a su ley de telecomunicaciones, permitieron la denegación de contenidos en Internet por razones como “la seguridad nacional”, “ofensas a los valores sociales”, “perturbación del orden público”, “injurias al presidente”, etc. Cabe destacar que dichas denegaciones forzosas eran permitidas sin la necesidad de una orden judicial que así lo dispusiera, estando la autoridad administrativa facultada para hacerlo de forma totalmente discrecional.

Esto llevó a que durante 2014 el gobierno turco diera un golpe sin precedentes a la libertad de expresión en Internet, prohibiendo el acceso a algunas redes sociales[7] por la negativa de cumplir ciertas sentencias judiciales, pero evidentemente orientado a silenciar las crecientes críticas a la gestión del presidente Erdogan y los casos de corrupción conocidos en dicho país. El malestar público y las protestas contra el accionar del gobierno fueron masivos y se convirtió en un caso icónico de vulneración de los derechos humanos en Internet.

Actualmente, las autoridades turcas han denegado a sus ciudadanos el servicio de más de 115.000 sitios y servicios de contenido en Internet, con un porcentaje muy menor de resoluciones judiciales ordenando dichos bloqueos, y con un 93% de bloqueos cursados por la autoridad administrativa de telecomunicaciones (TIB)[8], que representa el brazo del gobierno en estas materias.

Privacidad y la vigilancia del Estado

En 2013, el caso del ex contratista de seguridad de la NSA (National Security Agency) Edward Snowden y las filtraciones de información de las agencias de inteligencia de los Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda, detonó uno de los episodios más importantes de la historia moderna respecto del manejo de datos personales de la ciudadanía.

En particular, la revelación del programa de seguridad de los Estados Unidos llamado PRISM[9], mostró al mundo las capacidades de los Estados para comprometer la privacidad de los ciudadanos a través de la vigilancia masiva de las telecomunicaciones.

A través del programa PRISM, las agencias de inteligencia de los Estados Unidos recolectaban datos desde la red pública, obligando a una serie de proveedores de contenido como Google, Yahoo, Microsoft o Facebook, y a proveedores de infraestructura y servicio de telecomunicaciones, como Verizon y otros, a entregar información sobre el tráfico de sus clientes.

Esta información consistía, principalmente, en registros de llamados, conversaciones por mensajería de texto, tráfico de Internet, horarios de entrada y salida de los usuarios en algunos servicios, correos electrónicos, historiales de búsqueda, registros de conversaciones en aplicaciones, llamadas por VoIP, ubicación geográfica de teléfonos celulares con registros históricos y, en general, todo tipo de datos generados por la presencia o actividad en línea de las personas.

Esta recolección indiscriminada de datos puso en efecto un programa de vigilancia masiva sin precedentes en la historia, permitiendo a los Estados vulnerar toda protección a la vida privada que hubiese estado en rigor hasta ese minuto, “y que ya no son explicables ni justificables con la lucha contra el terrorismo”[10].

En Chile, durante 2015 se dio a conocer la existencia de un software contratado por la Policía de Investigaciones a la empresa italiana Hacking Team. Dicho software era llamado originalmente “Galileo”, pero en nuestro país adoptó el nombre de “Phantom”[11].

El objetivo de “Phantom” es la vigilancia masiva de computadores y teléfonos celulares[12], principalmente -y en la voz del propio encargado de la intermediación entre la Policía de Investigaciones y la empresa- la Policía querría utilizar el sistema para “obtener acceso a información que no obtendrán a través de una orden judicial”[13].

De acuerdo a lo que se conoce del sistema, “Phantom” (Galileo) posee capacidades para “registrar llamadas (también conversaciones por Skype), espiar mensajes (tanto SMS como por aplicaciones de mensajería instantánea), copiar documentos y fotos, realizar capturas de pantalla con el intervalo deseado, obtener la ubicación del sujeto cada X minutos, acceder a los contactos, calendario y webs visitadas por el sospechoso, registrar todas las teclas pulsadas, clics de ratón y contraseñas introducidas por el usuario y, por supuesto, acceder a la cámara del dispositivo en cuestión”[14].

Si bien nuestro régimen jurídico cuenta con la exigencia de control y órdenes judiciales para poder realizar diligencias intrusivas, como la interceptación de telecomunicaciones o la recolección de datos personales para fines de persecución penal, las vías de hecho han demostrado que no siempre ésta salvaguarda funciona de la forma esperada cuando se trata de ambientes digitales.

Para entender lo anterior, hay que estudiar el caso del abogado chileno Rodrigo Ferrari, quien fuera acusado por un empresario de una supuesta usurpación de identidad por el uso de una cuenta en la red social Twitter[15].

De acuerdo a los relatos de Ferrari, la policía y fiscalía chilena habría hecho uso de sus facultades para obtener desde diversas fuentes, como el proveedor de acceso a Internet y el proveedor de contenidos, los datos que lo identificaban, incluyendo su RUT, domicilio, nombre, correo electrónico, la dirección IP con las cuales fueron creadas o administradas las cuentas de redes sociales, etc.

En voz del propio afectado, el método utilizado fue ilegal al carecer de una orden judicial, sin embargo consiguieron de todas formas los datos solicitados, para posteriormente hacer públicas las acusaciones en su contra: “La Fiscalía se basó en un acuerdo policial entre Chile y Estados Unidos para la persecución de delitos como pornografía infantil o lavado de dinero, donde sí se puede pedir información. Siempre me llamó la atención haber encontrado en mi carpeta de investigación unos papeles de otra causa paralela, en la que efectivamente la Fiscalía pedía a Twitter información sobre determinados usuarios, en el marco de una investigación sobre redes en internet.
Creo, y esto es especulación mía, que aprovecharon una solicitud de esa investigación para meter la solicitud de mis datos personales.”[16].

Finalmente, el abogado sería absuelto de los cargos tras esta irregular investigación, sin embargo la extralimitación de la fiscalía y la policía ya había causado daño al hacerse público el caso, afectando no solo la honra del querellado, sino también normas esenciales del debido proceso y las salvaguardas para la protección de la intimidad. El requerimiento de una orden judicial, si bien es la piedra angular para hilvanar el debido proceso, puede en algunos casos no ser suficiente para resguardar a los ciudadanos en los desafíos que importan las nuevas tecnologías de la información.

La inquietud de la policía chilena pone sobre la mesa la necesidad de revisar los mecanismos de protección constitucional y legal con los que contamos para defender a la ciudadanía, en este caso, del apetito del Estado para inmiscuirse en su vida privada.

Casos como los anteriores han llevado a que la Organización de Naciones Unidas resolviera nombrar un Relator Especial en el derecho de privacidad[17], cuyo encargo durará tres años, y que ya cuenta con una visión preliminar respecto al estado del derecho a la vida privada en lo que corre del año 2016.

Algunas de las aproximaciones del Relator Especial señalan que "El contraterrorismo y el crimen organizado, así como otras ofensas socialmente sensibles como la pedofilia, son los principales objetivos de tales legislaciones [que autorizan la vigilancia masiva]. En estos debates se han entregado evidencias contradictorias, que a menudo sugieren que las medidas intrusivas en la privacidad y, especialmente, la vigilancia masiva no da lugar a una mayor seguridad, y dichas fallas de inteligencia deben ser abordadas por otros medios."[18].

Agrega además: "el Relator Especial sostiene firmemente la opinión que el cyberespacio arriesga ser arruinado por la cyber-guerra y la cyber-vigilancia; y que los gobiernos y otras partes interesadas deberían trabajar hacia la cyber-paz. En este sentido, al menos, la protección de la privacidad también es parte del movimiento de cyber-paz. De esta forma, el cyberespacio puede realmente convertirse en un espacio digital donde el ciudadano puede esperar tanto privacidad como seguridad, un espacio pacífico que no será constantemente puesto en riesgo por las actividades de algunos de los Estados, más allá de las amenazas que plantean el terrorismo y el crimen organizado.".[19]

Respecto de las necesidades que surgen para enfrentar el cambio de paradigma entre el ejercicio de los derechos humanos como los hemos conocido hasta hoy, y su ejercicio en ambientes digitales, el Relator sostiene que "El impacto de las nuevas tecnologías también significa que tendremos que revisar las distinciones entre privacidad individual y colectiva, así como las expectativas de privacidad en espacios públicos como privados, siempre en el contexto de dignidad y el desarrollo libre y sin obstáculos de la personalidad."[20]

La interpelación de la ONU

La resolución 32/13 del Consejo de Derechos Humanos de la ONU, sobre la promoción, protección y disfrute de los derechos humanos en Internet, reconoce a la Internet como "fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas"[21], e interpela a los Estados miembros a tomar medidas para la protección de los Derechos Humanos en ambientes digitales.

Asimismo, la resolución "Exhorta a todos los Estados a abordar las preocupaciones relativas a la seguridad en Internet de conformidad con sus obligaciones internacionales en materia de derechos humanos, para garantizar la protección de la

libertad de expresión, la libertad de asociación, la privacidad y otros derechos humanos en Internet, entre otras cosas mediante instituciones nacionales democráticas y transparentes basadas en el estado de derecho, de forma tal que se asegure la libertad y la seguridad en la red para que pueda seguir siendo un motor enérgico del desarrollo económico, social y cultural."[22].

De esta forma, el proyecto en estudio recoge el llamado de Naciones Unidas para abordar las problemáticas mencionadas, especialmente aquellas relacionadas con el ejercicio de la libertad de Expresión y la protección de la vida privada.

Para la protección de tales derechos, el proyecto propone agregar un nuevo ordinal al artículo 19 de la Constitución, y modificar el artículo 20 para incorporar nuevos derechos susceptibles de ser custodiados por el recurso de protección.

Estructura

La incorporación de un nuevo ordinal al artículo 19 de la Constitución tiene por objeto consagrar cinco conceptos que constituyen las ideas matrices del proyecto.

1. La consagración del acceso a Internet como derecho garantizado a todas las personas. Tal propuesta no obliga al Estado a efectivamente "conectar" a los ciudadanos con la red, sin embargo, fija un objetivo de promoción y protección del derecho del que deben gozar todas las personas para acceder a la red, sin distinciones, o perturbación por parte de terceros. En otras palabras, no se consagra un derecho-prestación, como es la naturaleza de los derechos económicos y sociales.

   Así lo han entendido los organismos supranacionales que han analizado la relevancia de Internet como un sistema que permite a millones de personas "acceder, compartir, intercambiar y disfrutar de bienes culturales de manera global, instantánea y a relativo bajo costo"[23].

   Esta obligación de promoción y protección se concreta a través de políticas públicas inclusivas orientadas a disminuir la brecha digital, entendida como "la separación entre quienes tienen acceso efectivo a las tecnologías digitales y de la información, en particular a Internet, y quienes tienen un acceso muy limitado o carecen de él"[24] y también la brecha digital entre géneros[25]; garantías legales para el respeto de la neutralidad de la red[26] (con las que Chile ya cuenta[27]), acceso universal a infraestructura y a la tecnología necesaria para hacer uso de ella, etc.

2. La protección de la libertad de expresión ejercida en Internet. Si bien el ordinal 12º del artículo 19 de la Constitución consagra el derecho a la libertad de expresión de forma general y aplicable a cualquier medio, y siendo éste además objeto del recurso de protección del artículo 20, la adición propuesta en el inciso segundo hace referencia solo a una pormenorización de lo ya señalado en el ordinal 12º, pero aplicado al ejercicio del derecho en Internet y

cumpliendo la función de incorporar las conclusiones del Consejo de Derechos Humanos referentes a que la libertad de expresión se ejerce sin consideración de fronteras y por cualquier procedimiento que se elija.

El proyecto no propone someter este ejercicio a la vigilancia del recurso de protección por ya encontrarse cubierto en el ordinal 12º, sin embargo, puede formar parte del debate parlamentario al respecto.

3. El inciso tercero propuesto para el ordinal 27º consagra la prohibición constitucional a la que estarán sujetos los órganos del Estado, respecto del control de las comunicaciones electrónicas, o el ejercicio de actividades de vigilancia a través de la recolección masiva e indiscriminada de datos de las personas, utilizando medios como la interceptación de comunicaciones en la red pública, poniendo en efecto, de esta forma, una especial protección a la vida privada cuando tal derecho se ejerce en ambientes digitales.

   Aquella incorporación obedece a la necesidad de evitar los espacios de abuso del Estado en la utilización de los datos personales y las facilidades que ofrecen las tecnologías de la información para su tratamiento, tal y como pudimos apreciar en los casos de las agencias de los Estados Unidos o las compras que pretendía realizar la policía chilena.

   Cabe señalar que, para efectos del proyecto, el concepto de “datos” abarca no solo a los que hacen identificable a la persona o la información específica contenida en las comunicaciones, sino que también los metadatos que genera el uso de cada servicio de comunicaciones, tales como los horarios en los que una persona se comunica, la duración y el destino de la comunicación o, en general, todo dato que pueda utilizarse para obtener o identificar otro dato[28].

   La consideración de los metadatos no es superficial. De acuerdo al Tribunal de Justicia de la Unión Europea, “Estos datos, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan.”[29]

4. De la misma forma, el proyecto se hace cargo del uso de la interceptación de comunicaciones para el ejercicio de la persecución penal. Para tales efectos, la propuesta reconoce la facultad de los tribunales de justicia de autorizar excepcionalmente la interceptación de comunicaciones circunscrita a una persona determinada, siempre y cuando se cumplan los requisitos objetivos que señala el inciso, de esta forma, reproduciendo la lógica y los elementos ya fijados por el artículo 222 del Código Procesal Penal.

5. Finalmente, el mandato constitucional de dictar una ley que aborde el tratamiento de los datos personales, en el marco de las garantías a la privacidad de las personas y al derecho de autodeterminación informativa.

   El derecho a la autodeterminación informativa ha sido copiosamente desarrollado por la doctrina. Ella ha señalado que "es un típico corolario de la sociedad moderna, en la cual las informaciones pueden dañar de la misma manera que la violencia física; sin embargo, el elemento caracterizador de este derecho es la autonomía del consentimiento, la posibilidad de autorizar,

---

[1] Aunque no es central al estudio planteado por este proyecto, Cfr. https://es.wikipedia.org/wiki/Segmentaci%C3%B3n_por_comportamiento

[2] Consejo de Derechos Humanos, Organización de Naciones Unidas, "Resolución 32/13. Promoción, protección y disfrute de los derechos humanos en Internet", A/HRC/RES/32/13, p. 3, 1 de julio de 2016, disponible en http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/RES/32/13&Lang=S

[3] The Verge. "UN condemns internet access disruption as a human rights violation". 4 de julio de 2016. Disponible en http://www.theverge.com/2016/7/4/12092740/un-resolution-condemns-disrupting-internet-access

[4] ONG Access Now, "Five years later: the internet shutdown that rocked Egypt", 21 de enero de 2016, disponible en https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/

[5] Democracy Now!, "Digital Darkness: U.S., U.K. Companies Help Egyptian Regime Shut Down Telecommunications and Identify Dissident Voices", 1 de febrero de 2011, disponible en https://www.democracynow.org/2011/2/1/digital_darkness_us_uk_companies_help

[6] El País, "Qué pasa con internet en Turquía", 5 de mayo de 2015, disponible en http://verne.elpais.com/verne/2015/05/04/articulo/1430732296_453069.html

[7] El País, "Golpe de Erdogan contra las redes sociales", 21 de marzo de 2014, disponible en http://internacional.elpais.com/internacional/2014/03/21/actualidad/1395387818_481360.html

[8] Estadísticas no oficiales, disponibles en https://engelliweb.com/istatistikler/

[9] Cfr. https://es.wikipedia.org/wiki/PRISM; https://hipertextual.com/2013/06/que-es-prism-claves

[10] Biblioteca del Congreso Nacional. "Vigilancia indiscriminada y derechos ciudadanos", 7 de julio de 2015, disponible en http://www.bcn.cl/observatorio/europa/noticias/vigilancia-indiscriminada-y-derechos-ciudadanos

[11] Ciper Chile. "Los correos que alertaron sobre la compra del poderoso programa espía de la PDI". 10 de julio de 2015, disponible en http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi/

[12] Pérez de Acha, Gisela. "Hacking Team: Malware para la vigilancia en América Latina". ONG Derechos Digitales, marzo de 2016. Disponible en https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

[13] La descripción fue hecha pública a través de correos electrónicos entre la PDI y la empresa, filtrados y publicados el 8 de julio de 2015 en Wikileaks. El correo en cuestión corresponde a un intercambio del 12 de junio de 2015. Cfr. Wikileaks, disponible en https://wikileaks.org/hackingteam/emails/emailid/1030224

[14] Cfr. http://www.malavida.com/es/noticias/asi-funciona-galileo-rcs-el-software-de-espionaje-de-hacking-team-005448#gref; así como https://www.4armed.com/blog/galileo-rcs-running-espionage-operation/ ; o también https://www.derechosdigitales.org/9880/el-auge-del-software-de-vigilancia-en-america-latina/

[15] The Clinic. "Rodrigo Ferrari, acusado por Andrónico Luksic de suplantarlo en Twitter: 'Los investigadores violaron todos mis derechos de privacidad'", 22 de septiembre de 2016. Disponible en http://www.theclinic.cl/2016/09/22/554806/

[16] Ibid.

[17] Se trata del profesor Joe Cannataci. Cfr.
http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

[18] Organización de Naciones Unidas, Oficina del Alto Comisionado de Derechos Humanos."Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci - Advance unedited version. A/HRC/31/64", 8 de marzo de 2016, p 6. Disponible en http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session31/Documents/A-HRC-31-64.doc

[19] Ibid.

[20] Ibid p. 11.

[21] Consejo de Derechos Humanos, Organización de Naciones Unidas. Ob. Cit., p. 3.

bloquear, oponerse, ratificar, de quedarse indiferente respecto a las circulaciones de voces, 'rectius' informaciones, acerca de la persona misma.".[30]

También existen amplios desarrollos jurisprudenciales, como el del Tribunal Constitucional de Perú, en que señala: "Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen.

En este orden de ideas, el derecho a la autodeterminación informativa protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera "sensibles" y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos."[31]

---

[22] Ibid, p. 4.

[23] Naciones Unidas. Asamblea General. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. A/HRC/17/27". 16 de mayo de 2011. Párr. 19 y 22. Disponible en: http://ap.ohchr.org/documents/dpage_s.aspx?m=85

[24] Ibid. Párr 60 y 61.

[25] Organización de los Estados Americanos. Asamblea General. Declaración de Santo Domingo. Gobernabilidad y Desarrollo en la Sociedad del Conocimiento. AG/DEC. 46 (XXXVI-O/06). Aprobada en la cuarta sesión plenaria, celebrada el 6 de junio de 2006. Párr. 13. Disponible en http://www.oas.org/dil/esp/AGRES-06S.doc

[26] Relator Especial de las Naciones Unidas (ONU) sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión, y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). "Declaración conjunta sobre libertad de expresión e Internet". 1 de junio de 2011, Punto 5, literal a. Disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2

[27] Cfr. Ley 20.453 disponible en https://www.leychile.cl/Navegar?idNorma=1016570

[28] Cfr. Electronic Frontier Foundation. "Por qué la metadata importa: Los peligros y la naturaleza reveladora de Retención de Datos". Disponible en https://www.eff.org/es/node/81907; Mayer, Jonathan y otros. "Evaluating the privacy properties of telephone metadata", 27 de abril de 2016. Universidad de Stanford. Disponible en http://www.pnas.org/content/113/20/5536.full; Sobre esto último, Stanford News. "Stanford computer scientists show telephone metadata can reveal surprisingly sensitive personal information". 16 de mayo de 2016. Disponible en http://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/

[29] Tribunal de Justicia de la Unión Europea. Digital Rights Ireland vs. Minister of Communications, Marine and Natural Resources y otros. Casos Conjuntos, C-293/12 y C-594/12, 8 de abril de 2014, párr. 27. Disponible en http://curia.europa.eu/juris/document/document.jsf?doclang=ES&text=&pageIndex=0&part=1&mode=DOC&docid=150642&occ=first&dir=&cid=99319%20(judgment,%20advisory%20opinions,%20resolutions,%20dissenting%20opinions)

[30] P. Ej. v., Adinolfi, Giulio. "Autodeterminación informativa, consideraciones acerca de un principio general y un derecho fundamental". 2007. p. 7. Disponible en http://www.scielo.org.mx/pdf/cconst/n17/n17a1.pdf

[31] Tribunal Constitucional del Perú. Expediente Nº 4739-2007-PHD/TC, considerandos 3 y 4. 15 de octubre de 2007. Disponible en http://www.tc.gob.pe/jurisprudencia/2008/04739-2007-HD.html

Asimismo, algunos países han legislado en base a este principio. Tal es el caso de México[32], Perú[33] o Colombia[34], quienes cuentan con legislación moderna respecto de la materia en estudio.

Si bien Chile cuenta con la ley 19.628 sobre protección de la vida privada, esta data del año 1999, se estructura con lógicas que obedecen a una realidad ampliamente superada por la tecnología y, al respecto, podemos encontrar múltiples proyectos de ley que modifican en mayor o menor extensión dicho cuerpo, evidenciando la necesidad e interés de promover nuevas reglas que se ajusten con la realidad que vive la sociedad actualmente.

Será misión del legislador fijar un marco regulatorio acorde a los desafíos actuales y futuros que plantea la tecnología, mientras que el proyecto propone establecer como piedra angular de tal proceso, el derecho a la autodeterminación informativa de las personas.

En un número adicional, el proyecto incorpora los incisos tercero y cuarto propuestos a la lista de los derechos custodiados por el recurso de protección del artículo 20.

POR TANTO,

Vengo en presentar a discusión el siguiente

PROYECTO DE REFORMA CONSTITUCIONAL

ARTÍCULO ÚNICO

Modifícase la Constitución Política de la República de la siguiente forma:

1. Agrégase al artículo 19 el siguiente ordinal 27º, nuevo:

"27º.- El derecho al acceso a Internet y la especial protección de la vida privada en ambientes digitales. En consecuencia, el Estado promoverá el acceso libre e igualitario a la red pública y no podrá suspender ni entorpecer la capacidad de cualquier persona de acceder y utilizar los contenidos ofrecidos a través de ésta.

Ninguna persona podrá impedir u obstaculizar la divulgación de información en línea.

---

[32] Cfr. "Ley Federal de protección de datos personales en posesión de los particulares". 5 de julio de 2010. Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[33] Cfr. "Ley 29.733 de protección de datos personales". 3 de julio de 2011. Disponible en http://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf

[34] Cfr. "Ley Estatutaria 1581 de 2012". 17 de octubre de 2012. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

El Estado no ejercerá control sobre las comunicaciones electrónicas, así como tampoco dará tratamiento ni recolectará masiva o indiscriminadamente datos de las personas, sean éstas nacionales o extranjeras, que puedan ser obtenidos mediante interceptación de la red pública o de otro medio de comunicación.

Sólo un tribunal de justicia, a petición del Ministerio Público, podrá autorizar la interceptación de comunicaciones para la recolección de datos de una persona determinada, siempre que existieren fundadas sospechas, basadas en hechos determinados, de comisión o participación en un hecho punible sancionado con pena de crimen, y en cuanto tal interceptación sea proporcional e imprescindible para la investigación.

La ley determinará la forma legítima en la que podrá darse tratamiento a los datos personales, procurando garantizar la privacidad y el derecho a la autodeterminación informativa de las personas".

2. Modifícase el artículo 20, reemplazando la voz "y 25º" por la expresión "25º, y 27º incisos tercero y cuarto".