Biblioteca del Congreso Nacional de Chile

Análisis de la legislación, las políticas y las prácticas nacionales sobre ciberseguridad, y revisión de legislación comparada sobre inteligencia artificial (IA)

Serie Informes Nº 22-23, 24-10-2023

por Víctor Soto Martínez

Resumen

El presente informe se refiere a varios temas. En primer lugar, al tratamiento de la ciberseguridad en nuestro país, para lo cual se divide en cuatro partes: i) marco normativo del cibercrimen en Chile; ii) mociones parlamentarias que se están tramitando en el Congreso para mejorar la legislación; iii) revisión general del proyecto de Ley Marco sobre la Ciberseguridad; y iv) revisión general de la política nacional en la materia. En este último caso se analiza también qué se ha aseverado sobre ella desde un enfoque de género. En segundo lugar, se refiere a la legislación comparada relativa a la regulación de la inteligencia artificial (IA) y los proyectos de ley que se están discutiendo en Chile sobre esta materia.

Departamento de Estudios, Extensión y Publicaciones - Biblioteca del Congreso Nacional
eMail: vsoto@bcn.cl, Anexo: 1877

TABLA DE CONTENIDOS

Antecedentes

Con motivo de la participación del Presidente de la Cámara de Diputadas y Diputados en la Comisión de Asuntos Políticos de la Asamblea Parlamentaria Euro-Latinoamericana (*EuroLat*), a fines de octubre de 2023, se ha solicitado un informe que abarque una serie de materias relativas a la ciberseguridad y la inteligencia artificial.

Por cierto, un abordaje integral de esta materia requeriría de un enfoque disciplinario más específico, pero consideramos que bien se puede abordar preliminarmente desde una óptica jurídica. Así, el presente informe se refiere en términos generales a la legislación y las políticas actuales que se están implementando en Chile para enfrentar las diversas amenazas que se ciernen sobre la seguridad digital del Estado. Para ello, el trabajo se dividirá en cinco partes: 1) marco normativo del cibercrimen en Chile; 2) mociones de parlamentarios que se están tramitando en el Congreso sobre el tema; 3) revisión general del proyecto de Ley Marco sobre la Ciberseguridad; 4) revisión general de la política nacional en la materia; y 5) revisión general de la legislación comparada en materia de inteligencia artificial (en adelante, también, IA)[1]. En este último punto se incorporará la perspectiva de género, para destacar algunas de las materias vinculadas con la ciberseguridad, donde –en la actualidad- las mujeres son particularmente vulnerables.

1. Marco normativo sobre cibercrimen y ciberseguridad en Chile

Antes que nada corresponde determinar si existe alguna definición oficial de la ciberseguridad en nuestro país. Lamentablemente no contamos con una definición a nivel legal –como veremos en el punto 3, esto podría cambiar cuando se apruebe la Ley Marco sobre Ciberseguridad-, pero sí podemos guiarnos por lo que señala la actual Política Nacional sobre la materia. De acuerdo con dicho documento, la ciberseguridad es ”una condición caracterizada por un mínimo de riesgos para el ciberespacio, entendido como el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren. En este conjunto (…) los atributos claves a proteger son la confidencialidad, integridad y disponibilidad de la información”[2]. Esta definición tiene la virtud de poner el foco principal en la información y, por ende, en los datos de las personas que utilizan y acceden a los sistemas informáticos.

[1] Cabe señalar que esta es una actualización y complemento de la minuta 05-23, del presente año. Lo nuevo es la quinta sección, referida a la inteligencia artificial.

[2] Véase: GOBIERNO DE CHILE. *Política Nacional de Ciberseguridad (2017-2022)*, p. 16. Puede consultarse en línea:

https://biblioteca.digital.gob.cl/bitstream/handle/123456789/738/Pol%C3%ADtica%20Nacional%20de%20Ciberseguridad.pdf?sequence=1 [consultado el 10-11-2022]

Con esta idea en mente, podemos pasar a revisar el marco normativo de la ciberseguridad en Chile.

1.1. Convenio de Budapest

En primer lugar, cabe señalar que nuestro país suscribió hace algunos años el *Convenio sobre la Ciberdelincuencia del Consejo de Europa*, conocido como el "Convenio de Budapest", que entró en vigor el 1 de julio de 2004 y que, a la fecha de suscripción por parte de Chile (2016), había sido ratificado por cuarenta y siete Estados. Este convenio fue ratificado por el Congreso y publicado, finalmente, en el Diario Oficial el 28 de agosto de 2017.

El principal objetivo del convenio es el desarrollo de una política criminal común frente al ciberdelito por parte de los diversos países suscriptores, mediante tres vías principales: a) la homologación de la legislación penal sustantiva; b) el mejoramiento de las capacidades nacionales para la investigación de este tipo de delitos, según el derecho procesal de cada país; y c) el establecimiento de un sistema rápido y eficaz de cooperación internacional.

1.2. Ley N° 19.223 (recientemente derogada)

Sin perjuicio de lo anterior, hasta 2022, Chile contaba con una legislación sobre la materia que, si bien en su momento fue considerada como pionera en América Latina, se encontraba bastante desactualizada, sobre todo a la luz de lo dispuesto en el Convenio de Budapest. Se trata específicamente de la ley N° 19.223, que tipifica figuras penales relativas a la informática.

En particular, dicha ley tipificaba originalmente las siguientes conductas:

a) la destrucción o inutilización maliciosa de un sistema de tratamiento de información, sus partes o componentes, así como el impedimento, obstaculización o modificación de su funcionamiento;

b) la interceptación, interferencia o acceso a un sistema de tratamiento de la información realizada con el ánimo de apoderarse, usar o conocer indebidamente la información en él contenida;

c) la alteración, daño o destrucción de los datos contenidos en un sistema de tratamiento de información; y

d) la revelación o difusión maliciosa de los datos contenidos en un sistema de información.

Esta desactualización llevó a que el legislador optara por derogar la anterior normativa, introduciendo las modificaciones necesarias para adaptarla al Convenio de Budapest, como veremos a continuación.

1.3. Ley N° 21.459

Esta ley deroga la ley N° 19.223, con el objeto de establecer una regulación especial que contenga de manera integral las nuevas formas delictivas surgidas a partir del desarrollo de la informática. Así, como indicaba su mensaje, "se pretende llenar los vacíos o dificultades que ha tenido nuestro ordenamiento penal en la persecución de ciertas conductas que, incluso, no eran concebibles a la época de dictación de la ley N° 19.223".

En particular, se introducen las siguientes modificaciones sustantivas:

a) Se modifica el tratamiento que se entrega actualmente al **sabotaje y espionaje informático**, adecuándolos a las figuras penales reconocidas en el Convenio de Budapest, a saber: acceso ilícito a todo o parte de un sistema informático, ataque a la integridad del sistema y de los datos informáticos (arts. 2, 4 y 5 del mentado Convenio). Esto se encuentra recogido a grandes rasgos en los artículos 1 y 2 de la ley, sobre ataque a la integridad de un sistema informático y acceso ilícito, respectivamente.

b) Se agrega el delito de **interceptación ilícita**, para quien indebidamente intercepte, interrumpa o interfiera las transmisiones no públicas entre sistemas informáticos, así como la **captación ilícita** de datos transportados mediante emisiones electromagnéticas de sistemas informáticos, en concordancia con el art. 3 del Convenio de Budapest. Esto se encuentra recogido en el artículo 3 de la ley.

c) Se incorpora el delito de **falsificación informática**, que comprende la indebida introducción, alteración, daño o supresión de datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos (en concordancia del art. 7 del Convenio de Budapest). Esto se encuentra en el art. 5.

d) Se añade, en el artículo 6, el delito de **receptación de datos informáticos** respecto de quien "conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos" obtenidos a partir de un ataque ilícito (art. 2), interceptación ilícita (art. 3) o falsificación informática (art. 5).

e) Se incorpora, también, el delito de **fraude informático** (art. 7) respecto de quien manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, siempre que esto: (a) cause perjuicio a otro y (b) se haga con la finalidad de obtener un beneficio económico para sí o para un tercero. Aquí se aprecia una diferencia importante con el Convenio de Budapest, introducida durante el segundo trámite constitucional, ya que, por un lado, se omite

en la definición el carácter indebido e ilegítimo de la acción y, por otro, se añade al perjuicio la finalidad de obtener un beneficio económico, lo que en el art. 8 del referido convenio, sólo configura *una* de las hipótesis de este delito. Además, se considera autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero del artículo, facilita los medios con que se comete el delito.

f) Se tipifica el llamado **abuso de los dispositivos**, es decir, a quien entregare u obtuviere para su utilización, importare, difundiere o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o acceso, o datos informáticos similares, que permitan acceder a todo o parte de un sistema informático, creados o adaptados principalmente para la perpetración de los delitos establecidos en los artículos 1 a 4 (ataque a la integridad del sistema, acceso ilícito, interceptación ilícita y ataque a la integridad de los datos informáticos). Esto está en conformidad con el art. 6 del Convenio de Budapest y se traduce en el actual art. 8. Asimismo, se explicita que este delito se aplica también a propósito del delito de uso fraudulento de tarjetas de pago y transacciones electrónicas, tipificado en el art. 7 de la ley N° 20.009 (cuestión introducida durante la tramitación legislativa).

Además, se agregan circunstancias modificatorias de responsabilidad penal, ya sea para atenuar o agravar la misma (arts. 9 y 10 respectivamente).

Por otra parte, se modifican algunas normas procesales, con el objeto de mejorar la persecución e investigación de estos delitos, también en la línea del Convenio de Budapest. En particular, los cambios más relevantes son:

i) Se concede **legitimación activa** al Ministerio del Interior y Seguridad Pública, delegados presidenciales regionales y delegados presidenciales provinciales cuando las conductas afecten servicios de utilidad pública (art. 11).

ii) Se permite el uso de **técnicas especiales de investigación** (como agentes encubiertos, informantes, entregas vigiladas y controladas e interceptación de comunicaciones) cuando existan sospechas fundadas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en esta ley, previa autorización judicial, por cierto (art. 12).

iii) Se fija una regla especial de **comiso**, relacionada con los instrumentos del delito informático, los efectos y demás utilidades que se hubieran originado, o una suma de dinero equivalente (art. 13).

Cabe mencionar, además, que durante la tramitación se agregó un nuevo artículo 16, titulado "investigación académica", donde se establece que no será considerado ilegítimo el acceso a un sistema informático que no provoque daño o perturbación y tenga la finalidad de investigar o detectar sus vulnerabilidades, siempre y cuando quien lo realice reporte inmediatamente sus hallazgos a la autoridad

competente y, de ser posible, al responsable del sistema informático. Con este artículo se subsana "uno de los puntos en discusión durante el trámite del proyecto, sobre la legitimidad de las actividades de búsqueda de vulnerabilidades del "hacking ético", siempre que se dé cuenta de los hallazgos inmediatamente"[3].

2. Mociones parlamentarias en el Congreso para mejorar nuestra legislación

	N° Boletín	Fecha de Ingreso	Cámara de Origen	Etapa	Nivel de urgencia	Fundamento
1	9998-07	15 de abril de 2015	Cámara de Diputados	Primer trámite constitu-cional	Sin urgencia	Para solucionar el desfase de la legislación respecto del avance tecnológico se incorpora un nuevo artículo a la ley N°19.223, calificando como delito informático la producción, venta, distribución, exhibición, por cualquier medio web de material pornográfico en cuya elaboración hayan sido utilizados menores de edad, aunque el material tuviere su origen en el extranjero o fuere desconocido, y la facilitación de dichas conductas

[3] ROBERTS, Raimundo. "Proyecto de ley sobre delitos informáticos (N° de Boletín 12192-25). Estado del proyecto de ley al 1 de diciembre de 2020", SUP 129249, Biblioteca del Congreso Nacional, 2020, p. 6.

2	10145-07	18 de junio de 2015	Cámara de Diputados	Primer trámite constitu-cional	Sin urgencia	Ante el desfase de la ley N° 19.223 con el desarrollo tecnológico de los últimos años, el proyecto aborda las normas penales materiales que tipifican y sancionan las acciones que atentan contra los derechos de las personas en materia informática, y también en algunas normas de carácter procesal penal, con el fin de facilitar y hacer más eficiente la investigación y sanción de dichos delitos.
3	10979-07	16 de noviembre de 2016	Senado	Primer trámite constitu-cional	Sin urgencia	Se busca tipificar el daño informático, entendido como "todo acto deliberado e ilegitimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto produzca daños graves".

4	11214-07	3 de mayo de 2017	Senado	Primer trámite constitu-cional	Sin urgencia	La tipificación del delito de usurpación de nombre es anacrónica y no se encuentra actualizada a las nuevas maneras de relaciones interpersonales establecidas por la computación a través de Internet y las redes sociales.
5	11801-07	7 de junio de 2018	Cámara de Diputados	Primer trámite constitu-cional	Sin urgencia	A partir del caso de Katherine Winter[4], se busca incorporar a la ley N° 19.223 el delito de hostigamiento u acoso reiterado por redes sociales.
6	13928-07	1 de diciembre de 2020	Cámara de Diputados	Primer trámite constitu-cional	Sin urgencia	Proyecto de ley que proscribe, tipifica y sanciona la violencia digital en sus diversas formas y otorga protección a las víctimas de ella

3. Proyecto de Ley Marco sobre Ciberseguridad[5]

[4] Adolescente que se suicidó el año 2018 por el hostigamiento que sufrió en redes sociales.

[5] Al mes de abril de 2023 se encuentra en su primer trámite constitucional, en el Senado, lo están trabajando las Comisiones de Defensa Nacional y de Seguridad Pública, unidas, y se encuentra con un nivel de urgencia de discusión inmediata.

El día 15 de marzo de 2022 se ingresó el proyecto de **Ley Marco sobre Ciberseguridad** (Boletín N° 14.847-06). Este proyecto plantea tres objetivos generales:

i) definir la institucionalidad, los principios y la normativa que regirán las acciones de ciberseguridad de los órganos de la Administración del Estado y la relación entre éstos y los particulares;

ii) establecer los requisitos mínimos para la prevención, contención, resolución y respuesta frente a los incidentes de ciberseguridad que se generen;

iii) establecer las atribuciones y obligaciones tanto de los órganos del Estado como de las instituciones privadas que posean infraestructura crítica de la información, estableciendo mecanismos de control y un sistema de infracciones y sanciones.

Cabe mencionar que el proyecto se encuentra actualmente en su **segundo trámite constitucional**, luego de haber sido aprobado por el Senado. Está siendo revisado actualmente por la Comisión de Seguridad Ciudadana de la Cámara de Diputados. El Ejecutivo ha presentado diversos paquetes de indicaciones (en julio, en septiembre y en octubre del presente año) y ha decretado la urgencia suma del proyecto.

Profundizando un poco, podemos señalar que este proyecto de ley se centra en la creación de una institucionalidad robusta para enfrentar el problema de la ciberseguridad. Actualmente, el país cuenta con diversos equipos de respuesta frente a incidentes de ciberseguridad en los órganos públicos, incluido un *Equipo de Respuesta ante Incidentes de Seguridad Informática*, dependiente de la Subsecretaría del Interior, del Ministerio del Interior, creado el año 2018 y que se encuentra regulado en la Resolución Exenta N° 5.006, de 2019[6]. Sin embargo, no existe aún un sistema ni una institucionalidad permanente y de alcance general que permita enfrentar el problema de manera coordinada. En este sentido, se propone la creación de una **Agencia Nacional de Ciberseguridad**, órgano técnico y descentralizado, que contribuirá a la configuración de una política nacional en la materia (política que, a su vez, pasaría a formar parte integral del conjunto de políticas a ser definidas por los diversos gobiernos y no un esfuerzo aislado de cada gobierno). También se prevé la institucionalización de los equipos de respuesta tanto a nivel nacional como sectorial (entre los equipos de respuesta sectoriales, por ejemplo, se define uno de gobierno y uno de defensa).

Ahora bien, en cuanto al articulado más específico, el proyecto establece una serie de definiciones que, de seguro, serán útiles para la elaboración y el seguimiento de la política. Sin embargo, también se han identificado en este punto ciertos espacios de mejora[7].

[6] Véase: https://www.csirt.gob.cl/media/2019/09/RES.-EXENTA-N-5006-CREACION-DE-DIVISION-Y-UNIDAD.pdf [consultado el 25-06-2021]

[7] Véase: SOTO, Víctor. "Descripción del proyecto que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (Boletín N° 14.847-06)", Serie Minutas Nº 81-22, 2022. Disponible en el sitio de Asesorías Parlamentarias de la BCN:

En cuanto a las atribuciones de la Agencia es importante advertir que tendrá diversos niveles de atribuciones normativas. Por un lado, podrá dictar normas técnicas de carácter general y definir estándares mínimos de ciberseguridad. Estos últimos no obstan a la dictación, por parte de los órganos sectoriales, de estándares particulares para sus regulados, pero sí establecen el mínimo común que deberán considerar esos estándares (art. 7). Por otro lado, la Agencia también podrá dictar instrucciones que tendrán validez respecto de los órganos públicos y de aquellos privados con infraestructura crítica de la información que *no se encuentren sometidos a la regulación o fiscalización de un regulador o fiscalizador sectorial* (art. 9, b). Lo mismo ocurre respecto de su atribución de fiscalizar y sancionar el cumplimiento de la ley, sus reglamentos y su normativa técnica (art. 9, m).

4. Política nacional sobre ciberseguridad

4.1. Elementos de continuidad en la política pública (entre M. Bachelet, S. Piñera y G. Boric)

El año 2015 se creó el **Comité Interministerial sobre Ciberseguridad** (mediante decreto supremo N° 533, de 2015, del Ministerio del Interior), órgano que tiene como principales funciones asesorar del Presidente de la República en el análisis y definición de la política nacional de ciberseguridad (art. 2, a) del decreto citado) y analizar la legislación vigente aplicable en materia de ciberespacio, proponiendo las modificaciones constitucionales, legales y reglamentarias que sean necesarias (art. 2, d) del decreto), entre otras.

A partir del trabajo realizado por dicho comité, el año 2017 se dio a conocer la *Política Nacional de Ciberseguridad 2017-2022*, con medidas a corto plazo (2017-2018) y objetivos a largo plazo (2022). Estos objetivos a largo plazo son, a grandes rasgos, los siguientes:

1. Que el país cuente con una infraestructura de la información robusta y resiliente (es decir, con la capacidad de mantener una continuidad operacional a pesar de las fallas), preparada para resistir y recuperar de incidentes de ciberseguridad.

2. Que el Estado vele por los derechos de las personas en el ciberespacio, lo que implica la prevención de ilícitos y el establecimiento de prioridades en la implementación de medidas sancionatorias, entre otras medidas.

---

https://www.bcn.cl/asesoriasparlamentarias/detalle_documento.html?id=81100 [consultado el 16-01-2023]

3. Desarrollar una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de las tecnologías digitales.

4. Establecer relaciones de cooperación en ciberseguridad con otros actores y participar activamente en foros y discusiones internacionales.

5. Promover el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos.

Un aspecto que debemos destacar es que la *Política* aporta una definición bastante exhaustiva de la ciberseguridad –véase el punto 1 de este trabajo- y que se caracteriza por su énfasis en los derechos humanos (como queda claro con los objetivos 2 y 3). En suma, se trata de objetivos generales, relacionados con la seguridad de las instituciones públicas, con bastante énfasis en la prevención y en el desarrollo de políticas de formación y sensibilización en el tema de la ciberseguridad. Sin embargo, no se incorporan medidas directas para mejorar la legislación penal (aunque el problema sí se menciona, a propósito del establecimiento de prioridades en la implementación de medidas sancionatorias[8]).

Buscando cierta continuidad con la política nacional establecida por el gobierno de Michelle Bachelet, el gobierno de Sebastián Piñera desarrolló una *Estrategia Gubernamental sobre Ciberseguridad 2018-2022*[9]. Entre las medidas concretas propuestas figura la tipificación de nuevos delitos informáticos en consonancia con la Convención de Budapest y la mejora procesal de la prueba del delito. Asimismo, se comprometió el envío del proyecto de ley marco de ciberseguridad, ya revisado, que actualmente está siendo discutida por el Congreso Nacional.

El gobierno del Presidente Gabriel Boric ha mencionado la lucha contra el cibercrimen como una arista a ser considerada dentro de su *Plan Nacional contra el Crimen Organizado,* cuya mayor novedad a este respecto es que tendrá una coordinación regional a través de Consejos Regionales creados para tal efecto, cuya principal tarea será articular territorialmente el seguimiento de las acciones comprometidas en las diversas áreas del Plan y la Política Nacional que se diseñe, entre las cuales se cuenta, por cierto, la lucha contra el cibercrimen[10]. También se puede destacar, durante el mes de octubre de 2022, la inauguración del Edificio de la

[8] Gobierno de Chile, Política Nacional de Ciberseguridad, p. 19. Puede consultarse en línea: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

[9] Se delinea básicamente a partir del instructivo presidencial N° 008, de 2018, sobre ciberseguridad. La estrategia puede consultarse en línea: https://mba.americaeconomia.com/sites/mba.americaeconomia.com/files/s3e4-jorgeatton-confyn2018.pdf

[10] GOBIERNO DE CHILE, *Plan Nacional de Seguridad Pública y Prevención del Delito (2022–2026),* 2022, p. 58. Disponible en: https://drive.google.com/file/d/1Gq0b4_Rr4_12fyEAabJZedqIvRfk32ZY/view [consultado el 24-08-2022]

Jefatura del Cibercrimen de la Policía de Investigaciones (PDI) y, desde septiembre de dicho año, el trabajo de actualización de la Política Nacional de Ciberseguridad, para el período 2023-2028, llevado a cabo por el Comité Interministerial sobre Ciberseguridad.

4.2. Enfoque de género en la política de ciberseguridad

Siguiendo a Álvarez y Vera, una mirada de la ciberseguridad centrada en los derechos humanos "no solo apunta a proteger a los atributos de la información, sino también a asegurar que el ciberespacio sea un ambiente fértil para el desarrollo de las personas, permitiendo a la humanidad alcanzar nuevos estándares de libertad y dignidad"[11]. A partir de ello, Paloma Herrera sostiene que "[la] promoción de la igualdad entre hombres y mujeres en el pleno disfrute y goce de los derechos fundamentales es primordial para cumplir con este propósito, por lo que la concientización en esta materia es trascendental"[12]. Por lo tanto, podemos decir que la ciberseguridad no se agota en una definición de la infraestructura crítica de la información o en una enumeración de ciberdelitos, sino que debe apuntar más allá, lo que incluye la generación de un marco de convivencia respetuoso en el ciberespacio.

A partir de este marco general, hay –al menos- dos ámbitos de la política de ciberseguridad que debieran ser pensados desde un enfoque de género. En primer lugar, la implementación de medidas para **disminuir la brecha de género a nivel digital**, ya sea en el uso de dispositivos conectados a internet o la falta de capacitación técnica y profesional de las mujeres en áreas relacionadas con la ciberseguridad[13]. En efecto, en América Latina no sólo existe una brecha respecto de la cantidad de profesionales relacionados con el rubro de la ciberseguridad, sino que además se presenta una enorme desproporción entre hombres y mujeres, tal como han indicado el Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA) en su *Reporte de Ciberseguridad 2020*: "Uno de los factores que limita el progreso de nuestra región en materia de ciberseguridad es la ausencia de talento humano calificado. La brecha de profesionales en ciberseguridad se estima en 600.000 personas en la región. El problema se agrava cuando se analiza desde la perspectiva de género, ya que menos de un cuarto de los profesionales son mujeres"[14]. Para enfrentar esto se ha propuesto incorporar en el currículum educativo

[11] ÁLVAREZ, Daniel y VERA, Francisco. "Ciberseguridad y derechos humanos en América Latina". En: DEL CAMPO, Agustina (compiladora). *Hacia una internet libre de censura II: Perspectivas en América Latina*, Universidad de Palermo, Buenos Aires, 2017, p. 53.

[12] HERRERA, Paloma. "El enfoque de género en la Política Nacional de Ciberseguridad de Chile", *Revista Chilena de Derecho y Tecnología*, vol. 9, N° 1, 2020, p. 12.

[13] Ibíd., p. 9.

[14] BANCO INTERAMERICANO DE DESARROLLO (BID) y ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA). *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe*, 2020, p. 11. Disponible en: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe [consultado el 17-01-2023]

la educación en temas relacionados con las tecnologías de la información y la comunicación (TIC) y específicamente con la ciberseguridad desde una edad temprana, con tal de homogeneizar los conocimientos en el uso de las nuevas tecnologías y, también, identificar a los futuros cibertalentos[15]. Por otro lado, si bien en Chile no se han desarrollado aún programas nacionales que giren en torno al género y ciberseguridad, el ya mencionado *Comité Interministerial sobre Ciberseguridad* "ha promovido actividades como el *OEA Cyberwomen Challenge*, que invita a mujeres con interés en temas de TIC a poner sus habilidades a prueba en la resolución de incidentes y protección de infraestructura crítica en materia de ciberseguridad originada por la baja participación femenina en trabajos relacionados con esta área"[16].

En segundo lugar, es preciso considerar en el ámbito legal cómo **se acrecientan ciertos riesgos presentes en el ciberespacio en contra de las mujeres**[17]. En efecto, el último *Índice anual de civismo digital*, de Microsoft, señaló que, si bien la falta de civismo digital es una cuestión transversal –y que para las generaciones más jóvenes se ha convertido en una especie de "nueva normalidad"- la situación es aún más crítica respecto de las mujeres (así, durante 2021, el 57% de las mujeres sufrieron actividades riesgosas en Internet, frente a un 43% de los hombres)[18]. Dentro de las actividades que tienden a ser sufridas más por mujeres, tenemos la pornografía no consentida. Ésta "involucra la captación o divulgación de material gráfico y audiovisual de tono erótico o explícitamente sexual, sin el consentimiento de alguna de las personas retratadas y sin propósito legítimo"[19]. De acuerdo con Paloma Herrera, "[las] mujeres son las principales víctimas de estas prácticas, y quienes cometen este tipo de actos habitualmente son hombres. Dado lo anterior, la pornografía no consentida es reconocida como un tipo de violencia de género"[20].

Siguiendo esta línea, el informe «Violencia de género en internet en Chile» de la *Fundación Datos Protegidos* determinó, en una encuesta dirigida a mujeres y población LGBTIQ+, que el 88,1% de quienes respondieron declaró haber sufrido algún tipo de violencia a través de internet, el 66,1% señaló que sufrió acoso y hostigamiento en línea, el 13,6% señaló sufrir la difusión de imágenes íntimas sin su

[15] HERRERA, Paloma. Op. Cit., p. 17.

[16] Ibíd., p. 18.

[17] Ibíd., p. 9.

[18] MICROSOFT. *Civility, Safety & Interaction Online* (Sexta Edición), 2021. Disponible en: https://news.microsoft.com/es-xl/micitt-y-microsoft-presentan-nuevo-estudio-de-tendencias-de-civilidad-en-linea/ [consultado el 17-01-2023]

[19] HERRERA, Paloma. Op. Cit., p. 25.

[20] Ibíd.

consentimiento, y 10,2% de extorsión en la red[21]. En Chile no existe un tipo penal específico que se refiera a estas conductas, frente a lo cual en la Cámara de Diputadas y Diputados se han presentado diversas mociones que tratan el tema. Actualmente, el proyecto más abarcador en esta materia es el que proscribe, tipifica y sanciona la violencia digital en sus diversas formas y otorga protección a las víctimas de ella (boletín N° 13928-07), aprobado en general el mes de agosto del año 2022 por la Cámara (actualmente, sin embargo, sigue en primer trámite constitucional).

5. Legislación comparada sobre inteligencia artificial (IA)

Se podría aseverar que el desarrollo de la IA y su impacto en la realidad práctica –al igual que otras materias vinculadas, como la automatización, el uso de redes sociales, las plataformas digitales, el uso de los *bots* para influir en la opinión pública, etc.- han superado la velocidad de respuesta de los gobiernos y parlamentos a lo largo del mundo. Su carácter todavía experimental y dinámico, además, dificultan las definiciones; se trata de una materia todavía en expansión. Asimismo, sus potenciales beneficios para diversos mercados en ciernes, así como para los propios Estados, han obligado a estos últimos a ser cautos en sus avances regulatorios. Esto podría explicar el hecho de que, si bien últimamente se han aprobado múltiples normativas que incorporan alguna mención a la IA, existen escasas regulaciones sistemáticas de esta materia en el derecho comparado[22]. Con todo, revisaremos a vuelo de pájaro tres iniciativas relevantes sobre la materia[23].

5.1. Los casos de la Unión Europea, Estados Unidos y China

5.1.1. Unión Europea

El proyecto de reglamento más completo ha sido elaborado por la Unión Europea, encontrándose actualmente bastante avanzado en su tramitación.

[21] Ibíd., p. 26.

[22] De acuerdo con el informe "Artificial Intelligence Index Report 2023" del *Institute for Human-Centered AI*, de la Universidad de Stanford, entre 2016 y 2022, parlamentos y congresos de 127 países aprobaron al menos un proyecto de ley relacionado con la IA y en conjunto aprobaron un total de 123 proyectos de ley. Sin embargo, no se han observado muchas regulaciones integrales. Véase: WEIDENSLAUFER, Christine y ROBERTS Raimundo. "Regulación de la IA en la experiencia comparada: Unión Europea, Estados Unidos y China", Biblioteca del Congreso Nacional, 2023. Disponible en: https://www.bcn.cl/obtienearchivo?id=repositorio/10221/34470/2/BCN_regulacion_global_IA_2023_jul.pdf [consultado el 24-10-2023]

[23] Si se quiere un análisis más detallado sobre este punto, véase el trabajo ya citado de Christine Weidenslaufer y Raimundo Roberts.

¿Qué establece a grandes rasgos el proyecto? En primer lugar, sus normas siguen un enfoque basado en riesgos y establecen obligaciones para proveedores y usuarios dependiendo del nivel de riesgo que la IA pueda generar[24].

Los sistemas de IA se califican en:

i) *IA de riesgo inaceptable*. Aquí se establecen algunas conductas derechamente prohibidas, como implementar técnicas subliminales o deliberadamente manipuladoras que resulten en daño físico o psicológico; explotar las vulnerabilidades de personas con discapacidad o niños, resultando en daño físico/psicológico; o utilizar la IA para calificar a las personas en función de su comportamiento social, su estatus socioeconómico o sus características personales, entre otras.

ii) *IA de alto riesgo*. Para ser calificado como de "alto riesgo" el sistema debe cumplir dos condiciones: (1) ser usado como un componente de seguridad de un producto regulado (por ejemplo, dispositivos médicos o maquinaria) sujeto a la evaluación de terceros en virtud de la legislación sectorial, y (2) el producto del que el sistema de IA es componente de seguridad, o el propio sistema de IA como producto, debe someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio. De acuerdo con esto, serían sistemas de alto riesgo la gestión y operación de infraestructura crítica; la educación y la formación profesional; el empleo y la gestión de trabajadores, el acceso al autoempleo; el acceso y disfrute de servicios privados esenciales y de servicios y prestaciones públicas; el cumplimiento de la ley (policía), entre otros[25].

iii) *IA de riesgo bajo o mínimo*. Los sistemas que no se encuentran en las situaciones anteriores.

Dependiendo del nivel de riesgo del producto, los proveedores tendrán distintos tipos de obligaciones, entre las que se cuentan: establecer e implementar un sistema de gestión de la calidad en su organización; elaborar y mantener al día la documentación técnica; someterse a una evaluación de la conformidad y eventualmente a una reevaluación del sistema; realizar un seguimiento posterior a la comercialización y tomar medidas correctivas cuando corresponda, entre otras.

Cabe mencionar que también se incorporan medidas de apoyo a la innovación como el establecimiento de "espacios controlados de pruebas para la IA" o *regulatory sandboxes*[26] por parte de las autoridades competentes de uno o varios Estados

[24] WEIDENSLAUFER, Christine y ROBERTS Raimundo. Op. Cit., p. 11 y ss.

[25] Ibid.

[26] Esto se deriva de un "enfoque de caja de arena" o *sandbox approach* en la regulación, consistente en remover regulaciones que puedan generar barreras a la innovación. Es decir, se trata de una *desregulación acotada*, de ahí la imagen de una caja de arena, donde los niños juegan libremente, pero sin salirse de sus márgenes.

miembros o por el Supervisor Europeo de Protección de Datos (arts. 53 y 54)[27].

Otro punto relevante de la regulación son las definiciones que aporta. Además, estas nos pueden ayudar a determinar cuáles son los focos de este proyecto y de la Unión Europea al respecto. Así, la definición de IA busca "ser lo más tecnológicamente neutra posible y resistir al paso del tiempo lo mejor posible, habida cuenta de la rápida evolución tecnológica y del mercado en relación con la IA" (*Exposición de motivos*, 5.2). En el actual estado de la discusión, para el Parlamento Europeo un "sistema de IA" sería un "software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el *anexo I* y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa"[28]. El *anexo I*, a su vez, establece las siguientes técnicas y estrategias:

"a) Estrategias de aprendizaje automático [machine learning], incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo [deep learning].

b) Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico).

c) Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización"[29].

Cabe mencionar que el último hito relevante en la tramitación de este proyecto es del 14 de junio de 2023, fecha en que el Parlamento Europeo aprobó diversas modificaciones al proyecto, incluyendo ajustes en las definiciones, la inclusión de nuevos sistemas de IA de alto riesgo, y nuevas prohibiciones, en base a la protección de los derechos fundamentales (así, por ejemplo, se aprobó una norma que prohíbe los sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público que permitirían un control masivo y los sistemas de identificación biométrica remota "en diferido", con la única excepción de las fuerzas de seguridad para la persecución de delitos graves y sólo previa autorización judicial, entre otros)[30]. Se espera que antes de fin de año concluyan las negociaciones y deliberaciones entre

[27] Ibid.

[28] Véase: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF [consultado el 24-10-2023]

[29] Véase: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_2&format=PDF [consultado el 24-10-2023]

[30] REAL INSTITUTO ELCANO, «Novedades en la tramitación del próximo Reglamento europeo de inteligencia artificial», en: https://www.realinstitutoelcano.org/analisis/novedades-en-la-tramitacion-del-proximo-reglamento-europeo-de-inteligencia-artificial/ [consultado el 24-10-2023].

el Parlamento Europeo, el Consejo Europeo y la Comisión Europea, a fin de cerrar el texto definitivo y aprobarlo dentro de 2023[31].

5.1.2. Estados Unidos

El año 2020 se promulgó la *National Artificial Intelligence Initiative Act* (2020). Esta ley tiene el objeto de proveer un programa coordinado para todo el gobierno federal para acelerar la investigación y aplicación de la IA. Los valores principales que mueven este esfuerzo legislativo son la prosperidad económica y la seguridad nacional. Es decir, no tiene un foco regulatorio sino que de fomento de las actividades asociadas a la IA. Asimismo, busca garantizar el liderazgo continuo de EE.UU. en la investigación y desarrollo de estos sistemas, preparar la fuerza laboral presente y futura de ese país para la integración de sistemas de IA en todos los sectores de la economía y la sociedad, y coordinar las actividades de IA en todas las agencias federales[32].

La ley contiene incluso una estrategia, denominada *Iniciativa Nacional de IA* (NAIIA), que proporciona un marco general para fortalecer y coordinar las actividades de investigación, desarrollo, demostración y educación de IA en todos los departamentos y agencias de EE.UU., en cooperación con la academia, la industria, las organizaciones sin fines de lucro y la sociedad civil[33].

En cuanto a su aporte a las definiciones de IA, según esta ley un sistema de IA sería un "sistema basado en una máquina que puede, para un conjunto determinado de objetivos definidos por el ser humano, realizar predicciones, recomendaciones o decisiones que influyan en entornos reales o virtuales. Los sistemas de inteligencia artificial utilizan inputs de máquinas y humanos para: a) percibir entornos reales y virtuales; (b) abstraer tales percepciones en modelos a través de análisis de forma automatizada; y (c) utilizar la inferencia de modelos para formular opciones de información o acción" (sec. 5002)[34].

5.1.3. China

China no cuenta con una regulación integral en la materia, pero una somera revisión a su estrategia sobre IA da cuenta de un enfoque similar al de Estados Unidos. Sus principales objetivos son económicos y vinculados con la seguridad nacional. Asimismo, se ha intentado desarrollar una serie de incentivos para el desarrollo de la investigación científica en IA, su utilización práctica y el desarrollo de una industria que tenga liderazgo a nivel mundial[35].

---

[31] Ibid.

[32] WEIDENSLAUFER, Christine y ROBERTS Raimundo. Op. Cit., p. 21.

[33] Ibid.

[34] https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210

[35] Véase: https://flia.org/notice-state-council-issuing-new-generation-artificial-intelligence-development-plan/ [consultado el 24-10-2023]

Con todo, se han publicado dos regulaciones sectoriales desde el año 2021, y se está tramitando actualmente una tercera. También se ha definido un órgano encargado de la regulación de este ámbito: la "Administración China del Ciberespacio" (CAC95).

Las normativas actualmente vigentes sobre IA en ese país son[36]:

(1) *Disposiciones sobre la administración de las recomendaciones de algoritmos del servicio de información de Internet* (2021). Regula los algoritmos de recomendación de los servicios de información, los cuales son definidos en su art. 2 como "suministro de información a los usuarios mediante el uso de tecnologías de algoritmos tales como generación y síntesis, envío personalizado, clasificación y selección, recuperación y filtrado, programación y toma de decisiones".

(2) *Disposiciones sobre la administración de servicios de información de Internet de síntesis profunda* (2022). Regula la información generada por sistemas de IA. Prohíbe las que contengan o sean noticias falsas o videos *deep fake*, y exige etiquetar estos contenidos como material elaborado por IA.

5.2. Los proyectos de ley que se discuten en Chile

Aunque Chile aún no cuenta con leyes que se refieran a la IA, se trata de un tema que ha preocupado a nuestros parlamentarios desde hace varios años. Así, el año 2019, la Comisión de Desafíos del Futuro, del Senado, organizó una serie de mesas de trabajo que decantaron en una propuesta de estrategia de IA para Chile. Sobre la base de este trabajo preliminar, una comisión experta nombrada por el presidente Sebastián Piñera elaboró la actual *Política Nacional de Inteligencia Artificial* (2021).

En cuanto a los proyectos de ley que regulan materias específicas o sectoriales sobre la IA, cabe mencionar el boletín 15.935-07, que modifica el Código Penal para sancionar el mal uso de la inteligencia artificial (ingresado el 15 de mayo de 2023) y el boletín 16.021-07, que modifica el Código Penal, para incorporar, como circunstancia agravante de la responsabilidad, el uso de inteligencia artificial en la comisión de un delito (ingresado el 13 de junio de 2023).

Por otro lado, el boletín 15.869-19, que regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas, en sus distintos ámbitos de aplicación (ingresado el 24 de abril de 2023), abarca una cantidad mayor de temas, pudiendo calificarse como el más completo hasta la fecha. Cabe mencionar que este proyecto se basa principalmente en el proyecto de reglamento de la Unión Europea, ya revisado, particularmente en lo relativo a su definición de sistema de IA como "el *software* que se desarrolla empleando una o varias de las siguientes técnicas: a) Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el

[36] Todo este párrafo ha sido tomado del trabajo de WEIDENSLAUFER, Christine y ROBERTS Raimundo ya citado, p. 28.

aprendizaje profundo; b) Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico); c) Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización" (art. 2, N° 1 del proyecto).

El proyecto desarrolla, asimismo, una regulación en base al riesgo –replicando los niveles diferenciados de riesgo establecidos en la regulación europea- y crea una Comisión Nacional de Inteligencia Artificial, cuyo principal foco sería regulatorio.

Actualmente la Comisión de Desafíos del Futuro, del Senado, se encuentra organizando una serie de mesas de trabajo con científicos e investigadores nacionales, que idealmente generarán las bases para un proyecto de ley integral sobre la materia de aquí al término del año.

Conclusiones

La ciberseguridad y, dentro de este ámbito, la defensa contra los ciberdelitos, es un tema central para la seguridad del país y de los ciudadanos, sobre todo a la luz de los avances tecnológicos de las últimas dos décadas. Por eso mismo, los últimos gobiernos han realizado un esfuerzo para contar con una política nacional y una estrategia gubernamental en esta materia.

Uno de los puntos centrales de estas iniciativas es la adecuación de la legislación sobre delitos informáticos con los avances tecnológicos y los estándares internacionales. De ahí que, durante el gobierno de Michelle Bachelet, Chile haya suscrito el Convenio de Budapest, que es uno de los instrumentos más avanzados sobre delitos informáticos en el contexto internacional. Asimismo, esto se reflejó en la estrategia del gobierno de Sebastián Piñera, que consideró varias iniciativas legales para realizar dicha adecuación normativa, en particular la ley N° 21.459, que derogó la ley N° 19.223, estableció nuevos delitos informáticos y modificó los tipos penales ya consagrados y el proyecto de Ley Marco sobre Ciberseguridad, actualmente en tramitación.

Cabe señalar que también existen varias mociones parlamentarias en tramitación que buscan adecuar y actualizar nuestra normativa, donde destacan aquellas vinculadas con la violencia de género en el ciberespacio. Todos estos esfuerzos son relevantes y deberían ser estudiados y profundizados, ya que, de concretarse, permitirían al país elevar sus estándares en materia de ciberseguridad.

Con todo, es importante que el enfoque de la ciberseguridad sea consistente con los principios generales que guían el actuar del Estado, en particular, los derechos fundamentales de las personas y que esto se convierta en una mirada transversal a las diversas instituciones y órganos que manejan datos personales o que tienen alguna relación con la ciberseguridad. Por ejemplo, si bien la Ley Marco ya indicada

establece importantes definiciones sobre ciberseguridad, en ningún caso agota lo que debiera entenderse por ella. Así, se puede sostener que el elemento central en la ciberseguridad- la protección de la integridad de los datos de las personas- requiere del sustento de un verdadero **ecosistema institucional**. Este ecosistema vendría dado por diversas líneas de acción, además del marco institucional ya mencionado. En primer lugar, por una adecuada definición de los ciberdelitos, lo que actualmente se resguarda mediante la ley N° 21.459. En segundo lugar, por la ley de protección de datos personales que actualmente se discute en el Congreso[37].

Es preciso recordar que el resguardo de los derechos fundamentales no se da simplemente a través de medidas punitivas, que operan siempre a posteriori, sino con protocolos que pongan a resguardo los datos que los ciudadanos comparten con los organismos gubernamentales. En otras palabras, para prevenirnos de posibles ataques, es necesario enfatizar también el **control público sobre el uso de los datos de las personas**, e implementar este control como un imperativo de todos los órganos públicos. Es decir, es preciso contar con una mirada integradora, transversal y no parcializada del problema.

En este sentido, queda claro que la ciberseguridad no se limita a su aspecto penal, procesal o de defensa nacional. Se necesita aquí, como en otras materias derivadas de la transformación tecnológica de la sociedad, enraizar el problema en una comprensión de los principios básicos que guían el actuar del Estado y poner en el centro de la política a las personas. De ahí también que el **enfoque de género**, al que dedicamos un apartado específico en este trabajo, sea un aspecto trascendental de una política nacional en la materia.

Por otra parte, se ha incluido aquí también una revisión general de las leyes que regulan la inteligencia artificial (IA) en el derecho comparado, así como los proyectos que actualmente se discuten en Chile sobre la materia. Este punto es importante porque da cuenta del creciente interés de los parlamentos por regular una materia que se desarrolla cada día, generando, por un lado, grandes beneficios tanto para los mercados como para las personas, y por otro, una serie de riesgos que pueden terminar perjudicándolas (y debilitando las bases democráticas de los Estados). Es imperativo, por tanto, que los parlamentos comiencen a regular el avance de la IA, poniendo como **foco principal los derechos fundamentales** de todas las personas y el fortalecimiento de la democracia. Un ejemplo señero en esta materia es el reglamento que se discute actualmente en la **Unión Europea**.

[37] Chile ya cuenta con una ley de protección de datos personales (ley N° 19-628), pero ella se ha considerado insuficiente para resguardar muchas de las situaciones que se viven a partir de la digitalización del país. Para hacer frente a esta situación, se discute en el Congreso el proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín N° 11.144-07), actualmente en segundo trámite constitucional, en la Cámara de Diputados.