REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 9 NÚM. 1 (2020) • PÁGS. 5-32 • DOI 10.5354/0719-2584.2020.51577
RECIBIDO:16/11/2018 • APROBADO: 4/5/2020 • PUBLICADO: 30/6/2020

DOCTRINA

El enfoque de género en la Política Nacional de Ciberseguridad de Chile

The gender focus in Chile's National Cyber Security Policy

Paloma Herrera Carpintero
Universidad de Chile

RESUMEN La Política Nacional de Ciberseguridad de Chile señala que, en materia de derechos fundamentales, se debe emplear un enfoque de género para asegurar la igualdad de las personas en el ciberespacio. El presente artículo tiene por objeto analizar lo que se debe entender por enfoque de género en el marco de esta Política Nacional de Ciberseguridad, junto con la importancia de disminuir la brecha de género a través de la capacitación y manejo de tecnologías por parte de las mujeres. La reflexión se centra en describir los principales peligros y transgresiones que sufren las mujeres en el ciberespacio, en específico, en materia de privacidad y datos personales, para efectos de manifestar que solo en la medida en que todos los sectores de la sociedad estén conscientes de esta desigualdad, podremos lograr un ciberespacio libre, abierto, seguro, resiliente e igualitario.

PALABRAS CLAVE Ciberseguridad, género, derechos fundamentales, privacidad, datos personales.

ABSTRACT Chile's National Cybersecurity Policy indicates that in the matter of fundamental rights, a gender focus must be used to ensure the equality of all people in cyberspace. This article aims to analyze what should be understood by gender focus in the context of the National Cybersecurity Policy and the importance of reducing the gender gap in women's training and technology management. The analysis will focus on describing the main dangers and transgressions suffered by women in cyberspace, specifically in terms of privacy and data protection, to express that only to the extent that all sectors of society are aware of this inequality, we can achieve an open, safe, resilient and egalitarian cyberspace.

KEYWORDS Cybersecurity, gender, fundamental rights, privacy, data protection.

Introducción

El creciente desarrollo económico y social de los Estados se debe en gran parte a la globalización y a la constante evolución y desarrollo de las tecnologías de la información y comunicación (TIC). El uso de drones en la agricultura ha permitido la identificación en forma temprana de plagas y sequías que perjudican a los cultivos,[1] mientras que el análisis y tratamiento de datos mediante *big data*[2] ha permitido que las empresas mejoren sus procesos y rentabilidad. Sobre esto último, conocido fue el caso de la multinacional Walmart en Estados Unidos, que gracias al análisis de los patrones de compra de sus clientes pudo predecir el volumen de aprovisionamiento que requeriría para hacer frente al huracán Katrina y satisfacer la excesiva demanda de productos por parte de los consumidores.[3]

Las fronteras físicas hace tiempo dejaron de ser obstáculos para que las personas se desarrollen en diversos ámbitos de su vida gracias a la comunicación, el acceso y la difusión del conocimiento que se produce en el ciberespacio. Sin embargo, esta tecnoglobalización también tiene consecuencias negativas, ya que ofrece un escenario propicio para actividades que atentan contra la seguridad de los Estados y sus nacionales (Castro Valdebenito y Monteverde Sánchez, 2018).

De acuerdo con el Foro Económico Mundial,[4] los incidentes de seguridad y ciberataques están entre los principales riesgos globales que se vislumbran en los próximos diez años, en específico, aquellos ataques a infraestructura crítica (como banca, salud, transporte, entre otros) y al robo de información (por ejemplo, *phishing*), cuyas consecuencias es posible advertir en el ámbito económico, político y social. En el caso de Chile, han sido mediáticos los ataques informáticos que han sufrido entidades gubernamentales, bancarias y de salud, casos que han puesto el tema de la ciberseguridad en el debate público.[5]

1. Julie Turkewitz, «Farmers flying drones may soon be given clearence», *The New York Times*, 15 de mayo de 2015, disponible en https://nyti.ms/3g6LfrC.

2. «Analytics: El uso del *big data* en el mundo real», IBM Institute for Business Value, 2012, disponible en https://bit.ly/3e4mE4U.

3. Ryan Scot, «How hurricane Katrina changed corporate social responsibility forever», *Huffpost*, 6 de diciembre de 2017, disponible en https://bit.ly/2TnbQql.

4. «The global risks report», World Economic Forum, 2020, p. 7, disponible en https://bit.ly/3e256pR. El Foro Económico Mundial, mejor conocido como Foro de Davos, es una fundación sin fines de lucro ubicada en Ginebra, Suiza, que involucra a los principales líderes políticos, empresariales y culturales, entre otros, para debatir sobre las agendas mundiales, regionales e industriales. Para más información, véase «Our mission», World Economic Forum, disponible en https://bit.ly/2XbmoKo.

5. Para más información sobre los incidentes de seguridad contra infraestructura crítica de Chile, véase «Informe de estabilidad financiera», Banco Central de Chile, 2018, pp. 17-18, disponible en https://bit.ly/2W5kLxb; y «Escenario de amenazas en la industria de salud y ciencias de la vida», Deloitte Threat Intelligence & Analytics, 2019, disponible en https://bit.ly/2W5liiF.

El ciberespacio debe ser comprendido como un ámbito de información digital que va más allá de internet[6] y que incluye las interacciones humanas que allí se producen (Álvarez Valenzuela y Vera Hott, 2017: 40). Por lo tanto, es un ámbito más por el cual las personas proyectan su libertad y desarrollo personal. Ejemplo de esto es lo acontecido por la pandemia del covid-19,[7] durante la cual el aislamiento obligó a las personas a depender aún más de las TIC para aminorar los impactos económicos y sociales producidos por la enfermedad. Estos cambios y sucesos nos llevan a reconsiderar y replantear la noción de derechos humanos, con el fin de que sean respetados, cumplidos y protegidos también en el ciberespacio.

Entenderemos la ciberseguridad, desde nuestra óptica de análisis, no solo como un fenómeno que se manifiesta y percibe en el conjunto de acciones que se desarrollan, coordinan e implementan para la gestión y minimización de riesgos en el ciberespacio, con el objetivo de proteger los atributos de la información (confidencialidad, integridad y disponibilidad). También la consideraremos desde una perspectiva garantista, ya que debe propiciar y asegurar el respeto y promoción de los derechos humanos en el ciberespacio (Álvarez Valenzuela y Vera Hott, 2017: 53). Para conseguirlo, es primordial contar con la cooperación y coordinación de los sectores público y privado, la sociedad civil y la ciudadanía en general para armonizar las directrices, principios y medidas que se deban implementar en el ciberespacio con miras a lograr un efectivo respeto de los derechos fundamentales, como la privacidad, la libertad de expresión y el debido proceso, por nombrar algunos (Viollier, 2017b: 9).

En este contexto, a principios de 2017, Chile lanzó su Política Nacional de Ciberseguridad con el objetivo de mejorar los estándares de seguridad en el ciberespacio y, de esta forma, asegurar el pleno goce de los derechos fundamentales de todas las personas en igualdad de condiciones. La Política declara cuatro objetivos generales: i) resguardar la seguridad de las personas en el ciberespacio; ii) proteger la seguridad del país; iii) promover la colaboración y coordinación entre instituciones; y iv) gestión de riesgos del ciberespacio.[8]

Desde el lanzamiento de la Política, según el ranking The Inclusive Internet Index

6. Álvarez Valenzuela y Vera Hott (2017) señalan a modo de ejemplo el caso de Stuxnet, programa malicioso que atacó una central nuclear que no estaba conectada a ninguna red computacional como internet. Para más información del caso, véase «El virus que tomó control de mil máquinas y le ordenó autodestruirse», *BBC*, 11 de octubre de 2015, disponible en https://bbc.in/3aJgzZj.

7. María Paz Canales, «Tecnología contra la pandemia: Derechos fundamentales mucho más que daño colateral», Derechos Digitales, 2 de abril de 2020, disponible en https://bit.ly/2KNif9U. Asimismo, se sugiere consultar el compilado elaborado por la iniciativa Data2X, «COVID-19 Resources: Gender Data, Gendar and data: Gender data is a critical input for a gender-sensitive response to Covid-19», marzo de 2020, disponible en https://bit.ly/2VWZPd8.

8. «Política Nacional de Ciberseguridad», Gobierno de Chile, 2017, p.12, disponible en https://bit.ly/2Rgcipj.

de 2020,[9] Chile es uno de los países con más avances respecto del promedio mundial en el uso de internet, con el decimotercer lugar de 100 a nivel global, y el primer lugar a nivel latinoamericano. A su vez, en materia de ciberseguridad, el ranking National Cyber Security Index[10] posicionó al país en el lugar 37 de 152 a nivel mundial, mientras que a nivel latinoamericano compartió el primer lugar con Paraguay.

Sin embargo, una de las grandes preocupaciones a nivel mundial en materia de ciberseguridad es la falta de talento y de profesionales especializados. El informe Cybersecurity Work Force de 2019[11] señaló que la fuerza laboral global de técnicos y profesionales necesita crecer 145%; además, señaló que los profesionales de ciberseguridad tienen el doble de probabilidad de ser hombres, por lo que existe un grupo demográfico que no está siendo considerado en la generación de nuevos talentos y su reclutamiento.

Las mujeres, por razones históricas y culturales, son discriminadas por el hecho de ser tales (Durack, 1997), sesgo que también se ha manifestado en el diseño e implementación de la tecnología, la cual no ha sido ni es neutral. Esto ha quedado de manifiesto a través de la feminización por defecto de los asistentes virtuales, como Siri, Alexa o Cortana. En este sentido, la Organización de las Naciones Unidas para la Educación elaboró un informe en 2019, titulado *I'd blush if I could: Closing gender divides in digital skills through education*, que aborda el caso del asistente virtual Siri señalando que, cuando se le insultaba, esta tecnología respondía de forma sumisa y servil (West, Kraut y Chew, 2019: 107), lo cual deja en evidencia que el estereotipo de género sí está presente en el atributo de las tecnologías, que en algunos casos puede ser catalogada como una forma de violencia de género.[12]

Sobre la violencia de género, la Convención Belén do Pará[13] ha manifestado que la

9. El informe fue encomendado por Facebook y elaborado por *The Economist* Intelligence Unit. Su objetivo es permitir que el uso de internet refleje resultados positivos en el desarrollo económico y social. Para más información, véase «Chile», The Inclusive Internet Index, disponible en https://bit.ly/3bS1OVx.

10. Desarrollado por la e-Governance Academy, organización sin fines de lucro que surge de una iniciativa en conjunto del Gobierno de Estonia, el Open Society Institute y el Programa de las Naciones Unidas para el Desarrollo. El reporte está disponible en https://ncsi.ega.ee/compare/.

11. Informe elaborado por el Consorcio internacional de Certificación de Seguridad de Sistemas de Información, más conocido como (ISC)², disponible en https://bit.ly/2Wfln3H.

12. Unesco ha señalado que la utilización de los estereotipos de género es dañina cuando produce violaciones de los derechos y las libertades fundamentales. Para más información, véase «Los estereotipos de género y su utilización», Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos, disponible en https://bit.ly/3f5NQ4k.

13. La Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer fue adoptada en Belém do Pará, Brasil, en 1994, y formalizó la violencia contra las mujeres como una violación de sus derechos humanos. Fue publicada y promulgada en Chile en 1998 mediante Decreto 1.640 del Ministerio de Relaciones Exteriores, disponible en https://bit.ly/3d2Dtwj.

violencia contra la mujer es, por una parte, una ofensa a la dignidad humana y, por otra, una manifestación de las relaciones de poder históricamente desiguales entre hombres y mujeres. Esta discriminación y desigualdad también se ha visto proyectada en el ámbito digital (Peña, 2017). Si bien ha disminuido la denominada «primera brecha digital», caracterizada por el acceso a internet, la segunda brecha, referente a incorporar a las mujeres a la sociedad de la información, ha sido más difícil de superar (Castaño, 2008). En consecuencia, si ya la participación de las mujeres es relativamente baja en temas de TIC, en ciberseguridad es escasa.

Ante este escenario, concluimos que mientras no se asegure la participación efectiva de todos los sectores de la sociedad y no se establezcan las medidas necesarias para solucionar la falta de talento en el sector de ciberseguridad, no podremos cimentar las bases democráticas para contar con un ciberespacio libre, abierto, seguro, resiliente e igualitario.

Para efectos de concientizar en la correlación entre género y ciberseguridad, el presente artículo describirá, en primer lugar, la importancia del enfoque de género que se debe considerar en el respeto y promoción de los derechos humanos, de acuerdo con lo expresado en la Política Nacional de Ciberseguridad, para luego explicar qué se entiende por enfoque de género a nivel internacional. En segundo lugar, se reflexionará sobre 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. En tercer lugar, se describirá desde el ámbito normativo cómo se acrecientan ciertos riesgos presentes en el ciberespacio en contra de las mujeres. Respecto de este punto, se analizará: i) la vigilancia focalizada, descontrolada y abusiva; ii) el tratamiento abusivo e indiscriminado de datos en el contexto de *big data* y iii) la pornografía no consentida. Por último, se manifiesta en la conclusión la imperiosa necesidad de establecer parámetros y medidas que expliciten en qué consiste el enfoque de género expresado, pero no explicado, en la Política; cómo la concientización de la brecha de género digital es primordial para prevenir y combatir las amenazas que se presentan en el ciberespacio; e instar a que desde el ámbito normativo se construya una legislación que vele de manera efectiva por los derechos fundamentales de las personas.

La Política Nacional de Ciberseguridad de Chile

El Decreto Supremo 533, que crea el Comité Interministerial sobre Ciberseguridad (CICS), del 17 de julio de 2015, dispuso que esta entidad fuese la encargada de proponer la Política Nacional de Ciberseguridad y asesorar en la coordinación de acciones, planes y programas de los distintos actores institucionales.[14] El Decreto define

14. El Decreto Supremo 533 señala en su artículo 3 quiénes conforman el comité permanente, que

en su artículo 1 bis la ciberseguridad como «aquella condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como también el conjunto de políticas y técnicas destinadas a lograr dicha condición».

Desde el ámbito del conjunto de políticas y técnicas que se deben implementar para lograr un ciberespacio seguro y resiliente, la ciberseguridad es un desafío global y multisectorial. Es global, debido a que las ciberamenazas y todo lo que se relaciona con el ciberespacio rompe fronteras. Es multisectorial, porque la prevención y respuesta a los incidentes de seguridad en el ciberespacio requieren la coordinación y colaboración de todos los sectores que convergen en la sociedad (Dammert y Núñez, 2019).

La Política Nacional de Ciberseguridad de 2017 es la encargada de entregar las principales orientaciones y lineamientos de acción de aplicación general para la implementación y evaluación en Chile de actividades que buscan minimizar los riesgos y amenazas en el ciberespacio. Asimismo, este instrumento contó con la participación[15] del sector público, el sector privado, el sector académico y la sociedad civil (Sancho Hirane, 2018) con un fuerte grado de transparencia e inclusividad en su elaboración (Viollier, 2017b: 11). Consideramos que estas acciones manifestaron la intención del Estado de conseguir una efectiva validación de este instrumento y manifiestan la ratificación del compromiso de transparencia, coordinación y colaboración que debe asumir la sociedad hacia la consecución de los objetivos plasmados en ella.

La Política se encarga de definir la ciberseguridad delimitando los atributos que se busca resguardar, además del objetivo que se persigue con las medidas a implementar para alcanzar estos fines. De esta forma, define a la ciberseguridad como «el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren, siendo la confidencialidad, integridad y disponibilidad de la información los atributos a proteger, los que a su vez generan un ciberespacio robusto y resiliente» (página 15).

El mensaje del Gobierno central plasmado en la Política es reiterativo al señalar, a grandes rasgos, que su principal objetivo es mejorar los estándares de seguridad digital para proteger a las personas y asegurarles el pleno ejercicio y goce de los derechos

---

debe considerar la integración permanente de un representante de las subsecretarías de Interior, Defensa, Relaciones Exteriores, Justicia, General de la Presidencia, Telecomunicaciones, Economía y Empresas de Menor Tamaño, Hacienda, Minería, Energía y la Dirección Nacional de la Agencia Nacional de Inteligencia.

15. En las sesiones públicas celebradas para la elaboración de la Política Nacional de Ciberseguridad, por nombrar algunos actores, participó el Poder Judicial, la Asociación Gremial de Desarrolladores de Software, el Centro de Estudios en Derecho Informático, la Fiscalía de Chile, la ONG Derechos Digitales y la Cámara de Comercio de Santiago, entre otros. Asimismo, el borrador de la Política fue sometido a consulta pública en febrero y marzo del año 2016. Para más información, véase «Participación», Ciberseguridad, Gobierno de Chile, disponible en https://bit.ly/2ziS9cq.

fundamentales (página 9). La percepción de la ciberseguridad desde un enfoque de 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» (Álvarez Valenzuela y Vera Hott, 2017: 54). 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.

En materia de ciberseguridad, consideramos que una de las principales medidas que se deben adoptar e implementar para la concientización consiste en desarrollar campañas informativas dirigidas a la ciudadanía sobre los riesgos de un uso inadecuado del ciberespacio, debido a que las mayores amenazas que se generan contra los derechos humanos por el uso indebido de las TIC son contra la privacidad y protección de datos personales de las personas (Leiva, 2015: 166).

Frente a estos peligros y preocupaciones, la Política estableció un mandato estatal de velar por el respeto y promoción de los derechos fundamentales en el ciberespacio (página 12). También señala que, en materia de derecho fundamentales, se empleará «un enfoque de género, que permita hacer visible y enfrentar desigualdades que enfrentan los diversos grupos en el ciberespacio» (página 15).[16]

Lo anterior adquiere relevancia si se considera que al analizar las estrategias de ciberseguridad de los Estados latinoamericanos,[17] Chile ha sido el único que dispuso explícitamente la consideración de un enfoque de género en materia de ciberseguridad; en comparación, los demás países solo hicieron alusión a la consideración de una perspectiva general en materia de derechos humanos.[18] Si bien puede interpretarse que hacer alusión a la promoción, respeto y protección de los derechos humanos comprende de manera implícita la consideración de un enfoque de género, debemos señalar que ante el escenario actual, en el que las mujeres y niñas han sido las principales víctimas por discriminación y vulneración de sus derechos en el ciberespacio,

16. Es importante señalar que entre los grupos vulnerables en el ciberespacio, la Política menciona a niños, adolescentes, personas de la tercera edad, personas con discapacidad y minorías éticas, entre otros.

17. Trinidad y Tobago (2013), Panamá (2013), Jamaica (2015), Colombia (2011, 2016), Costa Rica (2017), Chile (2017), Paraguay (2017), México (2017), Argentina (2017), República Dominicana (2018), Guatemala (2018) y Brasil (2019).

18. De las políticas de ciberseguridad revisadas, solo Guatemala hace referencia en un pie de página sobre la equidad de género, en el que reconoce la «primacía de la persona humana, respeto al Estado de derecho, observancia de los derechos humanos, equidad de género, respeto a la diversidad cultural, fortalecimiento de la gobernanza local y ejercicio de los controles democráticos». Véase Gobierno de la República de Guatemala, «Estrategia de Seguridad Cibernética», p. 31, disponible en https://bit.ly/2KQ7Nyo.

se torna imperioso y trascendental concientizar, sensibilizar y rememorar a los actores de la sociedad sobre la importancia de considerar un enfoque de género en la protección y promoción de los derechos fundamentales de las personas, en equidad de condiciones.

El mandato estatal de la Política sobre instar al respeto y promoción de los derechos fundamentales en el ciberespacio guarda directa concordancia con lo señalado en la Carta de Derechos Humanos y Principios para Internet,[19] elaborada por el Foro para la Gobernanza de Internet de la Organización de las Naciones Unidas,[20] que dispone como principio fundamental la importancia de «aumentar la concientización acerca de la Carta a la luz de la creciente preocupación pública nacional e internacional respecto de la protección y el goce de los derechos humanos tanto *online* como *offline*» (página 1) y la importancia del respeto del derecho a la no discriminación en el acceso, uso y gobernanza en internet reconociendo la igualdad de género y señalando que se debe asegurar la «plena participación de las mujeres en todos los ámbitos relacionados con el desarrollo de internet para garantizar la igualdad de género» (página 14).

Para conseguir lo anterior, los Estados deben acelerar e intensificar sus esfuerzos para prevenir y eliminar cualquier violación, abusos, discriminación y violencia contra mujeres y niñas en los contextos digitales.[21] La mención explícita de un enfoque de género en materia de derechos fundamentales en el ámbito de la ciberseguridad pone de manifiesto la inequidad existente entre hombres y mujeres, en razón de una construcción social y patriarcal —como se expuso en nuestra introducción— y que se ve proyectada también en el ciberespacio.

Es necesario evidenciar que en la Política se omitió el establecimiento de parámetros explícitos respecto de lo que se debe entender por enfoque de género y cuáles son los principales indicadores y medidas que deben considerarse en el contexto de género y ciberseguridad. Si no contamos con el establecimiento de estos elementos,

19. «Carta de Derechos Humanos y Principios para Internet», Naciones Unidas, 2015, disponible en https://bit.ly/3g64UYD.

20. El Foro es convocado por el Secretario General de Naciones Unidas y tiene por objetivo reunir a los *stakeholders* para debatir sobre cuestiones de política pública relacionadas con internet, con el fin de informar e inspirar en la formulación de políticas tanto del sector público como privado. Para más información véase el sitio web oficial, disponible en https://bit.ly/3bYgGBS.

21. La Asamblea General de las Naciones Unidas se ha referido en varias oportunidades a la correlación de la desigualdad de género con la violencia de género en los entornos digitales. Se recomienda consultar las siguientes resoluciones: A/HRC/RES/38/5, «Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: Prevenir la violencia contra las mujeres y las niñas en los contextos digitales y responder a ese fenómeno», 5 de julio de 2018, disponible en https://bit.ly/3d9LnEc; y A/RES/73/148, «Intensificación de los esfuerzos para prevenir y eliminar todas las formas de violencia contra las mujeres y las niñas: El acoso sexual», 17 de diciembre de 2018, disponible en https://bit.ly/35rcl7W.

no podremos verificar si el estatuto de las mujeres en la sociedad efectivamente está mejorando.

En este sentido, una de las principales medidas a considerar para lograr un cambio sustancial es la generación de encuestas nacionales y periódicas por parte del Estado, que midan y analicen la brecha de género en el ciberespacio y cómo ésta impacta en el desarrollo económico y social de Chile. Sin embargo, estos informes son prácticamente inexistentes, por lo que no contamos con una perspectiva general que aborde esta temática. Su principal consecuencia es un desconocimiento generalizado de la realidad particular del país.

Desde el ámbito multilateral, el Comité de Expertas del Mecanismo de Seguimiento de la Convención Belém do Pará (MESECVI)[22] señaló explícitamente su preocupación por la falta de normativa en el país que contemple la obligación de hacer encuestas sobre manifestaciones de violencia contra las mujeres tanto en el ámbito privado como en el público, así como la inexistencia de informes, estudios o investigaciones que reflejen el impacto de las estrategias o campañas de divulgación para erradicar la violencia de género contra la mujer.[23]

De tal forma, para que se pueda cumplir de manera eficaz el postulado de la Política Nacional de Ciberseguridad referente a la perspectiva de género, es primordial partir con la generación de encuestas e informes que den cuenta de la relación de las mujeres en Chile con el ciberespacio y en específico con la ciberseguridad. Estimamos que, como mínimo, se debiese considerar un indicador laboral (estadísticas de mujeres que trabajan en ciberseguridad) y un indicador social (estudios de discriminación y violencia de género en línea) para instar al debate entre los distintos *stakeholders* en esta materia. Solo en la medida en que la sociedad comprenda que las mujeres enfrentan mayores riesgos en el ciberespacio se podrán desarrollar medidas que tengan por finalidad el respeto y promoción de los derechos humanos de las personas en igualdad de condiciones.[24]

22. El Mecanismo tiene por objetivo vigilar la implementación efectiva de la Convención a través de un proceso de evaluación y apoyo continuo e independiente, con un foro de intercambio y cooperación técnica entre los Estados parte en lo relacionado a la violencia de género. Para más información, véase «Qué es el MESECVI», Organización de los Estados Americanos, disponible en https://bit.ly/2Yni3pQ.

23. «Chile: Informe país. Tercera Ronda», Mecanismo de Seguimiento de la Convención Belém do Pará, 24 de agosto de 2017, p. 9, presentado en la decimocuarta reunión del comité de expertas de la OEA, disponible en https://bit.ly/35tkvfI.

24. Se sugiere consultar los «Apuntes para la discusión: Políticas de ciberseguridad desde un enfoque de derechos humanos», elaborado por GenderIt, el cual refundió las opiniones e intervenciones de Valeria Betancourt y Olga Paz en representación de la Asociación para el Progreso de las Comunicaciones durante el taller sobre investigación y políticas en ciberseguridad, organizado por el Canada Centre for Global Security Studies junto con Citizen Lab, que tuvo lugar en mayo de 2012 en Panamá, disponible en https://bit.ly/2VVunM7.

El enfoque de género

El sistema internacional de los derechos humanos se funda principalmente en dos principios rectores: la igualdad de derechos entre hombres y mujeres y la no discriminación entre ellos. En consecuencia, los Estados deben adoptar las medidas necesarias para garantizar a todos, en igualdad de condiciones, el pleno goce de los derechos humanos. Sin embargo, a lo largo de la historia y hasta nuestros días, las mujeres han sido discriminadas y privadas de participación en trascendentales instancias del acontecer social, por lo que se encuentran en una constante lucha por validarse ante la sociedad y lograr el efectivo respeto de sus derechos. Esto ha sido así desde hace mucho tiempo en el espacio físico, y puede intensificarse en el espacio digital.[25]

En este contexto, los organismos internacionales han demostrado preocupación por la discriminación y transgresión de los derechos de las mujeres. La Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW, por sus siglas en inglés), del año 1979,[26] señaló su inquietud por este tema y el gran impacto que produce en los derechos humanos manifestando en su considerando séptimo que

> la discriminación contra la mujer viola los principios de la igualdad de derechos y del respeto de la dignidad humana, que dificulta la participación de la mujer, en las mismas condiciones que el hombre, en la vida política, social, económica y cultural de su país, que constituye un obstáculo para el aumento del bienestar de la sociedad y de la familia y que entorpece el pleno desarrollo de las posibilidades de la mujer para prestar servicio a su país y a la humanidad.

Para aminorar esta discriminación, desde la década de los noventa la comunidad internacional de derechos humanos comenzó a hacer alusión al enfoque de género y la importancia de su transversalización.

La transversalización del enfoque de género es un término originado en la Cuarta Conferencia Mundial de la Mujer celebrada en Beijing en 1995, y hace referencia al deber que tienen los miembros de «adoptar las medidas que sean necesarias para eliminar todas las formas de discriminación contra las mujeres y las niñas, y suprimir todos los obstáculos a la igualdad de género y al adelanto y potenciación de papel de la mujer».[27] En general, la conferencia hace referencia a la importancia de la colaboración entre todos los sectores en la implementación de estrategias políticas y técnicas que propendan al logro de la igualdad sustantiva entre ambos géneros.

25. «El derecho a la vida privada en la era digital», International Network of Civil Liberties Organizations y otros, abril de 2018, p. 7, disponible en https://bit.ly/36nvKae.

26. La Convención fue publicada y promulgada en Chile en 1989 mediante el Decreto 789, del 9 de diciembre de 1989, del Ministerio de Relaciones Exteriores, disponible en https://bit.ly/2VXLFZm.

27. «Informe de la Cuarta Conferencia Mundial sobre la Mujer», Naciones Unidas, A/CONF.177/20/Rev.1, 1996, p. 4, disponible en https://bit.ly/3b1jyNo.

En concordancia con lo anterior, el enfoque de género fue definido en 1997 por el Consejo Económico y Social (ECOSOC) de Naciones Unidas,[28] en el siguiente tenor:

> El proceso de evaluación de las consecuencias para las mujeres y los hombres de cualquier actividad planificada, inclusive las leyes, políticas o programas, en todos los sectores y a todos los niveles. Es una estrategia destinada a hacer que las preocupaciones y experiencias de las mujeres, así como de los hombres, sean un elemento integrante de la elaboración, la aplicación, la supervisión y la evaluación de las políticas y los programas en todas las esferas políticas, económicas y sociales, a fin de que las mujeres y los hombres se beneficien por igual y se impida que se perpetúe la desigualdad. El objetivo final es lograr la igualdad [sustantiva] entre los géneros.[29]

ONU Mujeres[30] ha interpretado y complementado la definición anterior, al señalar la relación medio/fin existente entre los conceptos de *igualdad de género* y *perspectiva de género* en el ámbito de los derechos humanos. En este sentido, manifestó que la igualdad de género es el objetivo de desarrollo general y a largo plazo, mientras que la incorporación de una perspectiva de género es un conjunto de enfoques específicos y estratégicos, así como procesos técnicos e institucionales que se adoptan para alcanzar este objetivo.[31]

La no inclusión de las mujeres en las diversas aristas sociales nos afecta a todos por igual. El no contar con perspectivas de pensamiento, habilidades y talentos provenientes de todos los grupos sociales tiene como principal consecuencia la obstaculización del desarrollo sostenible y bienestar social, en especial en esta época en que la innovación y generación de nuevas tecnológicas ha sido trascendental para el mejoramiento en la calidad de vida de las personas.

Desde el ámbito de las TIC y en específico desde la ciberseguridad, la baja participación e inclusión de las mujeres en esta área se traduce en una falta de recursos humanos y de herramientas técnicas necesarias para enfrentar los desafíos y riesgos actuales en el espacio digital.[32] A nivel mundial, la ciberseguridad no ha logrado cum-

28. Para una mayor profundización sobre lo que se debe entender por perspectiva de género, véase «La incorporación de la perspectiva de género: Una visión general», Oficina de la Asesora Especial en Cuestiones de Género y Adelanto de la Mujer, 2002, disponible en https://bit.ly/2qEGJIa.

29. «Informe del Consejo Económico y Social correspondiente a 1997», Naciones Unidas, A/52/3/Rev.1, 1997, p. 24, disponible en https://bit.ly/2YxhycK.p.

30. ONU Mujeres es la organización de las Naciones Unidas dedicada a promover la igualdad de género y el empoderamiento de las mujeres. Como defensora mundial de mujeres y niñas, fue creada para acelerar el progreso que llevará a mejorar las condiciones de vida de las mujeres y para responder a las necesidades que enfrentan en el mundo. Para más información, véase «Sobre nosotros», ONU Mujeres, disponible en https://bit.ly/21V7KWy.

31. «Incorporación de la perspectiva de género», ONU Mujeres, disponible en https://bit.ly/2WiV2S5.

32. «Strategies for building and growing strong Cybersecurity Teams», (ISC)² Cybersecurity Workforce Study, 2019, disponible en https://bit.ly/3aRp8To.

plir con la demanda de profesionales con las habilidades necesarias para desempeñarse en este campo y las mujeres que deciden dedicarse a esta área deben enfrentarse a una industria marcada por la discriminación de género. Un informe elaborado a partir de entrevistas a mujeres que trabajan en ciberseguridad mostró que en sus entornos de trabajo era habitual escuchar discusiones sobre la supuesta incapacidad natural de las mujeres para programar o que algunos compañeros comentaban que se desalentaban de asistir a una charla en la materia si la oradora era una mujer.[33]

La brecha digital de género en el ámbito de la ciberseguridad

La Política Nacional de Ciberseguridad señala la importancia de «desarrollar una cultura digital consciente, competente, informada y responsable que incluya a todos los actores relevantes entendiendo que estamos frente a un esfuerzo colectivo en pro de un beneficio común y de largo plazo» (página 15). Sin embargo, la brecha de género existente en esta área —como hemos señalado— es un tema preocupante, dado que no se asegura la participación efectiva de todos los actores relevantes, como ocurre con el género femenino.[34]

Por brecha de género entendemos la diferencia entre las tasas masculinas y femeninas en la categoría de una variable. Cuanto menor sea la brecha, más cerca estaremos de la igualdad.

El Foro Económico Mundial (FEM), en su informe «The global gender gap report» de 2020, que tuvo por objeto medir la disminución global de la brecha de género, situó a Chile en el lugar 57 de 153 del ranking mundial. Si bien el informe señala que Chile ha disminuido progresivamente esta brecha, la desigualdad es persistente y se sigue proyectando en la participación de la mujer en el ámbito laboral y político.[35]

La Comisión Económica para América Latina y el Caribe (Cepal) define *brecha digital de género* como «aquellas diferencias entre hombres y mujeres en el acceso a equipos informáticos y en el uso de dispositivos electrónicos e internet».[36] El informe señala que a nivel latinoamericano, si bien las mujeres igualan a los hombres en el acceso a computadores y conexión de internet, en cuanto al uso de estas tecnologías existe una brecha digital en que el porcentaje de mujeres es menor al de los hombres.

33. Juan Manuel Harán, «El desafío de ser mujer en la industria de la ciberseguridad», *We Live Security*, 8 de marzo de 2019, disponible en https://bit.ly/2StHzG5.

34. Sobre este tema, se sugiere consultar el reporte de la Association for Progressive Communications: Deborah Brown y Allison Pytlak, «Why gender matters in international cyberseciruty», Women's international League for Peace and Freedom and the Association for Progresive Communications, 2020, disponible en https://bit.ly/3dfU3Jc.

35. «The global gender gap report», World Economic Forum, 2020, disponible en https://bit.ly/3d7f74H.

36. «La brecha digital de género: Reflejo de la desigualdad social», Comisión Económica para América Latina y el Caribe, 2013, p.1, disponible en https://bit.ly/3fcS9uG.

Esto demuestra falta de interés y desconocimiento generalizado en este aspecto por parte del grupo femenino, en gran medida por estereotipos negativos de género en torno a las TIC.

En Chile el escenario es similar. La Comisión Nacional de Investigación Científica y Tecnológica (Conicyt) estudió la brecha de género en el ámbito de las ciencias y tecnologías señalando que la baja incorporación de mujeres en estas áreas puede explicarse por factores del entorno, estereotipos, expectativas de docentes y familias, entre otros, los cuales se reflejan en distribuciones de tareas diferenciadas por género y en la misma autopercepción que tienen las mujeres de su participación en la sociedad (Conicyt, 2017: 5).

En el ámbito de la ciberseguridad, esta brecha digital de género es aún más preocupante al considerar que si ya existe una enorme escasez de personal con habilidades, incentivar y promocionar la participación de mujeres en esta área del conocimiento requiere de un esfuerzo social en conjunto mayor. La empresa de seguridad informática Kaspersky Lab, en su estudio sobre los motivos que impiden el acceso de las mujeres al campo de la ciberseguridad, llegó a la conclusión de que el bajo porcentaje de participación femenina se debe al desconocimiento y falta de interés en estas materias, originados principalmente en prejuicios sociales inculcados desde muy temprana edad.[37]

La educación en temas TIC y ciberseguridad es el principal mecanismo para lograr a la deconstrucción del machismo en este ámbito y el fin de las conductas abusivas contra las mujeres en el ciberespacio. Para tales efectos, consideramos que los planes de educación deben iniciarse a temprana edad, pues solo de esta forma las mujeres tendrán el empoderamiento, la flexibilidad y la habilidad de desarrollar un análisis crítico libre de prejuicios y discriminaciones basadas en el género. Además, como señala Leiva (2015: 163), el objeto de iniciar la educación a temprana edad pretende, por un lado, homogeneizar los conocimientos en el uso de las nuevas tecnologías, así como su uso responsable; y, por otro lado, identificar a los futuros cibertalentos.

La importancia de instar a las mujeres a optar por alguna carrera relacionada con las TIC forma parte de la solución a la crisis de habilidades en el campo de la ciberseguridad y se traduce también en una manera de asegurar la generación de talento disponible con las habilidades e ingenio necesarios para hacer frente a las amenazas y ataques que surgen en el ciberespacio, y que ponen en riesgo la seguridad de todos.

37. El estudio prevé que para el año 2020 la brecha en ciberseguridad llegaría a los 1,8 millones de personas, lo cual se ve exacerbado por la falta de participación femenina. «¿Qué dirección seguir?: Estudio sobre los motivos que impiden el acceso de las mujeres al campo de la ciberseguridad», Kaspersky Lab, 2017, disponible en https://bit.ly/2Woz945.

Muchas organizaciones[38] y países han entendido la relevancia de considerar la perspectiva de género en el respeto y promoción de los derechos fundamentales en el ciberespacio, por lo que han promovido el desarrollo y capacitación del género femenino en ciberseguridad. En España, el Instituto Nacional de Ciberseguridad (INCIBE) organiza desde 2017 el Foro Internacional de Género y Ciberseguridad,[39] que en colaboración con la Organización de los Estados Americanos (OEA) tiene por objetivo: i) promover el intercambio de información y el desarrollo de conocimientos de género y ciberseguridad, ii) analizar la situación actual y problemática de género tanto a nivel nacional como internacional en relación con el sector de la ciberseguridad, y iii) debatir sobre los principales problemas en relación con la violencia de género en el ámbito digital.

En Chile, si bien a la fecha no contamos con una declaración de principios específicos o implementación de programas nacionales que giren en torno al género y ciberseguridad, hemos de reconocer que ya se están ejecutado ciertas medidas desde el ámbito de la capacitación técnica. Así, con el objeto de instar a las mujeres a capacitarse en temas relacionados con la ciberseguridad, el Comité Interministerial sobre Ciberseguridad ha promovido actividades como el OEA Cyberwomen Challenge,[40] 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.

Una mayor participación e inclusión femenina impacta en diversas aristas de nuestra sociedad, lo cual también incide en la ciberseguridad. A modo de ejemplo, se ha demostrado que el género está directamente relacionado con el grado de preocupación que se tiene de la privacidad en línea, con la conclusión de que las mujeres demuestran más preocupación respecto de estos temas. Asimismo, se demostró una correlación significativa entre el cumplimiento de las políticas de seguridad internas de cada organización y la mayor preocupación que manifiestan las mujeres en su cumplimiento (Anwar y otros, 2017). En Chile, manifestación de lo anterior es el resultado del ranking publicado por Leading Lawyers 2019,[41] en el cual la categoría «Data protection» fue liderada por mujeres en el primer y segundo lugar.

38. En razón de la manifiesta desigualdad y discriminación de género que sufren las mujeres en el ciberespacio, han surgido agrupaciones que centran su accionar en visibilizar este problema. Por nombrar algunas: Ciberseguras (https://ciberseguras.org/nosotras/), GenderIt (https://www.genderit.org/about) y The Women's Rights Online (WRO) Network (https://webfoundation.org/wro-network-orgs/).

39. Para más información, véase el sitio web oficial del Foro Internacional de Género y Ciberseguridad, disponible en https://www.incibe.es/foro-genero-ciberseguridad.

40. «Ciberseguridad: Más de 100 mujeres compitieron en Chile en el OEA Cyberwomen Challenge», *TrendTIC*, 28 de junio de 2019, disponible en https://bit.ly/3bXCldv.

41. Para más información, consúltese «Ganadores Leading Lawyers 2019», Leading Lawyers Chile, disponible en https://bit.ly/2VWWDOF.

Para finalizar este apartado, si consideramos que la tecnología no es neutral debido a que presenta sesgos de género desde su desarrollo, validación y puesta a disposición, y lo extrapolamos al ámbito de nuestra Política Nacional de Ciberseguridad, podemos señalar que solo en la medida en que se asegure, promocione e incentive la participación social y técnica de las mujeres en el diseño de políticas públicas y en el desarrollo, ejecución e implementación de medidas técnicas y normativas en materias relacionadas con la ciberseguridad, podremos lograr un ciberespacio libre, abierto, seguro, resiliente e igualitario.

El derecho a la vida privada y a la protección de datos personales

La ciberseguridad involucra el establecimiento y gestión de medidas que promuevan la seguridad de las personas en el ciberespacio. Estimamos que esta seguridad se logra en la medida en que se garantice a las personas el pleno respeto y goce de sus derechos fundamentales en el ámbito digital. Si bien todos los derechos humanos deben ser reconocidos y respetados en el ciberespacio, existen ciertos derechos que son especialmente más afectados, como el derecho a la privacidad y el derecho a la protección de datos personales.

En este contexto, como los estereotipos y discriminaciones del mundo físico se manifiestan también en el mundo virtual, las mujeres sufren su transgresión en mayor porcentaje. Un estudio publicado por Microsoft, llamado «Índice anual de civismo digital»,[42] señaló que en Chile las mujeres tienen las tasas más altas de acoso en línea en comparación con la población masculina, mientras que la Alta Comisionada de las Naciones Unidas para los Derechos Humanos manifestó que «el acoso en línea y las campañas de troleo e intimidación han contaminado algunas secciones de internet y plantean amenazas muy reales fuera del mundo virtual, con efectos desproporcionados sobre las mujeres».[43]

Consideramos que un eficaz análisis y estudio del derecho a la vida privada y protección de datos personales[44] desde una perspectiva de género debe identificar

42. «Microsoft lanza Índice de Civismo Digital y desafía a la gente a ser más empática en línea», Microsoft News Center Latinoamérica, 7 de febrero de 2017, disponible en https://bit.ly/2Oy5rUd.

43. Michelle Bachelet, «Derechos humanos en la era digital: ¿Pueden marcar la diferencia?», ACNUDH, 17 de octubre de 2019, disponible en https://bit.ly/3dbzfTm.

44. La Constitución Política de la República, en su artículo 19 numeral 4, reconoce a todas las personas «el respeto y protección a la vida privada y a la honra de la persona y su familia, y, asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley». Mientras que el numeral 5 del mismo artículo dispone «la inviolabilidad del hogar y de toda forma de comunicación privada. El hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley».

y comprender las amenazas particulares a las cuales están predispuestas las mujeres en el ciberespacio. Al respecto, es tarea de toda la sociedad —partiendo por el Estado— transversalizar el enfoque de género, con el objetivo de establecer indicadores, medidas de prevención y de coerción en caso de vulneración, para cumplir con el mandato establecido en la Política.

Al analizar el ordenamiento jurídico de Chile, se vislumbra que la normativa sectorial contenida en la Ley 19.628,[45] sobre Protección de la Vida Privada, no contempla una autoridad administrativa con potestades de fiscalización y sanción por contravenciones a la ley, por lo cual se ha transformado en una ley que ha servido más para legitimar el tratamiento indiscriminado de datos personales que para proteger a las personas,[46] mientras que desde la perspectiva penal ciertas acciones no están tipificadas como delito o es imposible configurar el tipo penal en el ciberespacio.[47]

El Código Penal, en los artículos 161-A y 161-B, tipifica los delitos contra el respeto y protección a la vida privada y pública de las personas y su familia. El artículo 161-A sanciona, a grandes rasgos, a quienes difundan hechos de carácter privado por cualquier medio y cuya captura o reproducción hayan sido obtenidos sin consentimiento de la persona afectada. A su vez, el artículo 161-B regula la figura penal comúnmente conocida como chantaje, que contempla la pretensión de entrega de dinero, la realización de cualquier conducta jurídicamente no obligatoria o la ejecución de un acto o hecho constitutivo de delito, bajo la amenaza de dar a conocer material que da cuenta de la intimidad de alguien obtenido de la forma descrita en el artículo 161-A. Sin embargo, dichos artículos son considerados de confusa redacción e interpretación, ya que dejan sin regulación las intrusiones no autorizadas en la vida privada de alguien en lugares públicos, no es claro si es punible la comisión del delito por uno de los intervinientes del acto de carácter privado, ni tampoco regula la difusión no consentida de material íntimo o de carácter sexual que se obtuviera de manera consentida (Bascuñán, 2005; Díaz, 2007).

En el caso del género femenino, la falta de mecanismos eficaces de protección en temas relacionados con la privacidad y protección de datos personales, así como la falta de tipificación de ciertos delitos relacionados con las tecnologías, nos han generado las siguientes preocupaciones, que analizaremos de forma general.

45. Vale precisar que se está tramitando actualmente en el Congreso la actualización de la referida Ley mediante el «Proyecto de ley sobre protección de datos personales» (Boletín 11.092-07) y 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 11.144-07), disponibles en https://bit.ly/3aSRw69.

46. Para una profundización sobre la historia y estado de la Ley 19.628, veáse Viollier (2017a).

47. Para efectos de implementar el Convenio de Budapest, el Gobierno firmó el 25 de octubre de 2015 el proyecto de ley que busca frenar los delitos informáticos (Boletín 12.192-25) que «Establece normas sobre delitos informáticos, deroga Ley 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest», disponible en https://bit.ly/2QBeOnR.

Vigilancia focalizada, descontrolada y abusiva

El uso de estas tecnologías, como drones o globos, puede dar lugar a una «vigilancia indiscriminada, constante y permanente hacia ciertos grupos sociales o étnicos, quienes se ven compelidos a dejar de actuar naturalmente por sentirse observados y perseguidos».[48]

En Chile, mediáticos fueron los casos *Drones* y *Globos*.[49] En ambos, diversas autoridades de gobierno local justificaron la implementación de estas medidas bajo el argumento de protección de la seguridad nacional. Sin embargo, en nuestra opinión, terminó convirtiéndose en una política de vigilancia masiva, arbitraria y altamente intrusiva (Garrido y Becker Castellaro, 2017).

Cuando se discutió el uso de estas tecnologías a nivel de municipalidades, se señaló que serían funcionarias públicas las encargadas de efectuar las labores de televigilancia, pues cuando se implementó la misma medida en Argentina, descubrieron que los hombres la usaban para seguir mujeres.[50]

Hasta el día de hoy, los drones y globos son permitidos por el Estado en el ámbito de la seguridad ciudadana y son utilizados en la generalidad de los casos sin tener en consideración una perspectiva de derechos humanos, mucho menos un enfoque de género. Si bien este tema afecta a la ciudadanía en general, el uso de estas tecnologías puede vulnerar aún más a las mujeres. Estas prácticas autorizadas por las entidades públicas, la judicatura y la actual normativa no solo legitiman una vigilancia arbitraria, abusiva y excesiva, sino que incluso voyerista.

En este sentido, en 2011 una ONG norteamericana[51] advirtió que, sin las precauciones adecuadas, los drones podrían ser utilizados incluso para registrar la intimidad sexual de las parejas en sus hogares con finalidades voyeristas.[52] Lo que al presente ya está ocurriendo a nivel global, por lo que abunda material en internet sobre

48. «El derecho a la privacidad», comunicación conjunta de Derechos Digitales, Ciudadano Inteligente, Fundación Pro Acceso y Privacy International, julio de 2018, disponible en https://bit.ly/3giRlVB.

49. Para más información sobre el caso *Drones*, véase la sentencia de la Corte de Apelaciones de Santiago, rol 82289-15, 4 de marzo de 2016, disponible en https://bit.ly/2qNkobj; mientras que para el caso *Globos,* véase la sentencia de la Corte de Apelaciones de Santiago, rol 34360-17, 21 de agosto de 2017, disponible en https://bit.ly/2yaH4tH.

50. Pablo Palma, «Corte de Apelaciones de Santiago, sistema de drones para la vigilancia viola la protección de la vida privada», *Derecho Chile*, 16 de marzo de 2016, disponible en https://bit.ly/2qK5PW4.

51. La American Civil Liberties Union es una organización sin fines de lucro progresista. Para más información, véase su sitio web oficial, disponible en https://www.aclu.org/.

52. El informe señaló, para ilustrar la amenaza a la privacidad que significa el uso desproporcionado e ilegítimo de drones, que en 2004 un helicóptero policial con visión nocturna de Nueva York captó y grabó a una pareja teniendo relaciones sexuales en un balcón, con lo que excedió sus facultades y finalidades legales en su actuar. «Protecting privacy from aerial survillance: Recommendations for Government use of drone aircraft», American Civil Liberties Unión, 2011, p.12, disponible en https://bit.ly/2JIvjg3.

esta temática, en que las mujeres son ciertamente las más afectadas por motivos de la cosificación[53] sexual a la que se ven expuestas.

Estimamos que el uso abusivo e indiscriminado de estos mecanismos de televigilancia no es un tema que solo nos debe preocupar por su utilización constante y abusiva desde el ámbito estatal, sino que también es preocupante desde el ámbito privado. En efecto, debido al bajo costo económico y facilidad de acceso, cualquier particular puede adquirir un dron, sin que exista en Chile el suficiente resguardo legal o práctico que asegure un uso legal y ético de estos equipos.

Tratamiento abusivo e indiscriminado en el contexto de *big data*

Para efectos de desarrollar la presente investigación, entenderemos por *big data*[54] la habilidad de almacenar, tratar y analizar grandes bases de datos mediante la utilización de herramientas tecnológicas de *data mining*, con el objetivo de inferir información y correlacionarla en un determinado contexto.

Los beneficios que conlleva la utilización de *big data* por parte de los diversos sectores de la sociedad son innumerables. Sobre todo en el ámbito público, el *big data* ha tenido fuerte impacto en el diseño, implementación y evaluación de políticas públicas, ya sea para incentivar el uso del transporte público o resolver el acceso desigual a los servicios y seguridad ciudadana (Rodríguez, Palomino y Mondaca, 2017: 1).

Asimismo, el *big data* para la obtención y análisis de datos relativos al género es esencial para disminuir la desigualdad entre hombres y mujeres. Así lo ha manifestado Naciones Unidas al consagrar la igualdad de género como uno de los objetivos centrales de la Agenda de Desarrollo Sostenible.[55] En la misma línea, la iniciativa Data2x[56] ha señalado la importancia del *big data* para disminuir esta brecha al promover la obtención datos de género que sean de calidad para la elaboración de políticas que consideren la perspectiva de género, con el objetivo de poder fiscalizar si están mejorando el bienestar de mujeres y niñas en la sociedad.[57]

53. El *Diccionario de la lengua española* define *cosificar* como «reducir a la condición de cosa a una persona». En la práctica, se suele considerar como un término de connotación despectiva.

54. Si bien no existe una definición plenamente aceptada de *big data*, para una mayor profundización sobre este tema, véase De Mauro, Greco y Grimaldi (2016).

55. La Agenda 2030 para el Desarrollo Sostenible fue adoptada por Chile en 2015, en su calidad de Estado miembro de Naciones Unidas. Para más información, véase http://www.chileagenda2030.gob.cl/.

56. Data2x es una iniciativa de 2012 promovida por la Fundación de las Naciones Unidas, la Fundación William y Flora Hewlett y el Gobierno de Estados Unidos. Su objetivo es generar conciencia sobre la importancia de obtener datos de género y que éstos sean analizados considerando una perspectiva de género. Para más información, véase su sitio web oficial, disponible en https://data2x.org/.

57. «What is gender data?», Data2x, disponible en https://bit.ly/2TwV2gX. Asimismo, se sugiere revisar los siguientes documentos de esta iniciativa: Mayra Buvinic, Rebecca Furst-Nichols y Gayatri Koolwal, «Mapping gender data gaps», Data2x, marzo de 2014, disponible en https://bit.ly/2WoTNYV; y

Para la obtención de los beneficios del *big data* en materia de género, los actores que intervienen en su desarrollo, implementación y análisis deben considerar un enfoque de género en la ejecución de sus labores, ya que como hemos indicado, la tecnología no es neutral y está condicionada por los sesgos históricos y culturales de sus desarrolladores y demás intervinientes. A partir de estos antecedentes, el *big data* se puede transformar en un mecanismo abusivo y discriminatorio que puede vulnerar los derechos humanos de las personas y, en situaciones específicas, las garantías fundamentales de las mujeres por el solo hecho de ser tales. Como ejemplo, podemos mencionar que una investigación efectuada por la Universidad de Washington descubrió que en el buscador de imágenes de Google, al hacer referencia a la palabra «CEO», los resultados correspondían tan solo en 11% a mujeres, a pesar de que en 2015 el 27% de las personas que ostentaban estos cargos eran de género femenino, por lo que arrojan una imagen distorsionada de la realidad (Kay, Matuszek y Munson, 2015).[58]

Lo anterior refleja que la discriminación contra las mujeres también está presente en la implementación de los algoritmos en el contexto del *big data* al interior de una base de datos. En efecto, estos algoritmos son creados y formulados por seres humanos, quienes poseen todo tipo de valores, muchos de los cuales promueven abiertamente el racismo, el sexismo y la falta de meritocracia (Noble, 2018), por lo que contar con la participación de mujeres y de las minorías en áreas relacionadas con las tecnologías es primordial para el desarrollo, implementación y difusión de tecnologías que consideren el respeto y promoción de los derechos fundamentales de las personas a través de una perspectiva de género que busque efectivamente disminuir la brecha en materia de algoritmos e inteligencia artificial.

La recolección de grandes conjuntos y análisis de datos origina ciertas preocupaciones sobre la privacidad en su almacenamiento y tratamiento. En efecto, las tareas de garantizar la seguridad de los datos y proteger la privacidad se dificultan a medida que la información se multiplica y se comparte de manera cada vez más amplia alrededor del mundo. Esto tiene como consecuencia que información como diagnósticos médicos, o situaciones financieras o familiares, por ejemplo, esté expuesta en línea, lo que otorga la posibilidad de crear perfiles de una persona determinada y prever sus patrones de comportamiento.

En Chile, esto se ve agravado por motivos del tratamiento masivo de datos provenientes de fuentes accesibles al público. En efecto, la Ley 19.628 señala en su artículo

---

Bapu Vaitla y otros, «Big data and the well-being of women and girls: Applications on the social scientific frontier», Data2x, abril del 2017, disponible en https://bit.ly/3bYtvvS.

58. Para profundizar sobre la investigación, véase Toni Castillo, «Cuando busco "cocinar", Google Images me muestra mujeres: ¿Debería Google modificar los resultados?», *Xataka*, 5 de enero de 2018, disponible en https://bit.ly/3aZKsET.

4 que no será necesario requerir autorización para el tratamiento de datos personales cuando éstos provengan o se recolecten de fuentes accesibles al público y cuando dicho tratamiento sea realizado por las personas privadas para el uso exclusivo suyo. En este contexto, especial preocupación se ha generado en el ámbito del *big data*, pues las entidades pueden excusarse en la supuesta legitimidad que otorga la Ley para tratar grandes bases de datos en programas que, a partir de variables algorítmicas, pueden discriminar sobre factores como el género. En el caso de las mujeres, especial preocupación conlleva la mala utilización y discriminación que pueden cometer las entidades y su personal involucrado en el análisis de estos datos.

La información que puede ser procesada a través de *big data* es valiosa sobre todo para el sector financiero y laboral. En efecto, permite, por ejemplo, que las entidades enfoquen su atención solo en grupos que consideren más rentables para el otorgamiento de créditos o contratación de personal. En este orden de ideas, se puede llegar a discriminar en la calidad del servicio que se dé en atención a un cliente sobre la base de la rentabilidad que esta persona otorgue al mercado (Tene y Polonetsky, 2012). Otro caso común acontece cuando una mujer que está buscando trabajo puede ser discriminada por tener hijos por este procesamiento de datos personales; o que se le niegue el acceso a un crédito por pertenecer al género menos rentable y más costoso desde el punto de vista económico.[59] En este contexto, las mujeres son más propensas a ser discriminadas, pues por lo general reciben sueldos más bajos que los hombres y tienen mayores gastos asociados, sobre todo si tienen hijos y son el único sustento económico del hogar. En Chile esta situación va en aumento, pues se han duplicado los hogares encabezados por mujeres en los últimos 25 años.[60]

El hackeo y robo de información también es un tema al que debiese prestarse especial atención, dado que en la generalidad de los casos es difícil alcanzar la certeza del origen de los datos para analizar si provienen de una fuente legal o fueron obtenidos a través de un tercero que robó dicha información. En este último caso, en la hipótesis de que los datos tratados sean obtenidos mediante la vulneración de un sistema informático, la posibilidad de quedar expuesta información que contenga datos sensibles es mayor. En el uso de ciertos servicios, como el correo electrónico, plataformas de videojuegos o perfiles de usuarios creados en internet, las personas asumen que los datos que entregan son privados y, por lo tanto, otorgan aún más información sin verificar los fines del tratamiento de dichos datos ni la existencia de un sistema de seguridad robusto. Conocido fue el caso denominado Celebgate, en el que se filtraron fotografías íntimas de varias actrices desde la plataforma iCloud de Apple,

59. Alejandro Nieto, «Discriminados y marginados por el *big data*», *Xataka*, 7 de noviembre de 2016, disponible en https://bit.ly/3bZP2Vb.

60. Paulina Sepúlveda, «Hogares encabezados por mujeres se duplican en 25 años», *La Tercera*, 14 de mayo de 2017, disponible en https://bit.ly/2zUYz1y.

imágenes que fueron obtenidas a través de *phishing*, acceso remoto, forzando restablecimientos de contraseñas y usando ingeniería social para acceder a sus correos electrónicos, para luego ser difundidas en un conocido foro de internet. La filtración afectó únicamente a mujeres, mientras que quienes difundieron eran en su mayoría hombres (Marwick, 2017: 187).

El exceso de información, la falta de educación en temas de ciberseguridad y el desconocimiento de la perspectiva de género lleva a la conservación de sesgos patriarcales y machistas, como hemos visto a través de conductas humanas relacionadas con la discriminación y la marginación por parte de algoritmos, según los ejemplos ya expuestos. Estas discriminaciones están prohibidas tanto en el mundo físico como en el ciberespacio, pues, como hemos señalado, los derechos humanos también deben ser protegidos y cumplidos en el entorno en línea, de modo de asegurar que sea un espacio libre e inclusivo.

Pornografía no consentida

La pornografía no consentida, erróneamente denominada «pornovenganza»,[61] 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.[62]

Las mujeres son las principales víctimas de estas prácticas, y quienes cometen este tipo de actos habitualmente son hombres.[63] Dado lo anterior, la pornografía no consentida es reconocida como un tipo de violencia de género.[64] El prejuicio sociocultural que se ha construido históricamente respecto de la posición de la mujer en el mundo y la visión predominante sexualizada que se tiene de ella han traspasado las fronteras y se han masificado en el ámbito digital, con la pornografía no consentida y su falta de regulación como evidencia.

A nivel global, los países que han legislado en contra de la pornografía no consen-

61. No todos los autores de la difusión no consentida están motivados en la venganza, y el material difundido no siempre se puede enmarcar dentro de lo pornográfico, es decir, con la intención de producir excitación.

62. La definición fue elaborada por el proyecto latinoamericano Acoso Online, que nace como respuesta a la violencia de género través de la publicación no consentida de imágenes y videos sexuales o eróticos. «¿Pornovenganza?», Acoso Online, disponible en https://bit.ly/3cTvwdg.

63. Amanda Lenhart, Michele Ybarra y Myeshia Price-Fenney, «Nonconsensual image sharing: One in 25 Americans has been a victim of "revenge porn"», Data & Society Research Institute, 13 de diciembre de 2016, disponible en https://bit.ly/2hulSSA.

64. El Instituto Europeo de la Igualdad de Género de Naciones Unidas así lo ha manifestado. Véase «La ciberviolencia contra mujeres y niñas», Instituto Europeo de la Igualdad de Género, 2017, disponible en https://bit.ly/2QKIUoZ.

tida tipificándola como delito en su derecho interno son la excepción a la regla.[65] Esto se debe a una combinación de factores: falta de comprensión de la gravedad, alcance y dinámica del problema; indiferencia histórica y hostilidad a la autonomía de las mujeres; y, por, sobre todo, falta de comprensión de la noción de privacidad (Keats y Frank, 2014: 347).

El Instituto Europeo de la Igualdad de Género (EIGE) señala que los perpetradores de estos actos con frecuencia son excompañeros que han obtenido imágenes o videos en el curso de una relación previa y tienen por principal finalidad avergonzar y humillar públicamente a la víctima. Sin embargo, la venganza no siempre es la finalidad de la referida captación o divulgación. En efecto, muchas de estas prácticas tienen su origen en la búsqueda de lucro, entretenimiento o voyerismo, entre otros.

Diversos son los sitios web dedicados a la pornografía no consentida, en los que sus usuarios comparten gran cantidad de material fotográfico y audiovisual de carácter erótico o pornográfico, acompañado en algunas ocasiones de datos personales y sensibles de la víctima, como números de contacto o dirección domiciliaria, entre otros. Esto puede tener como resultado que sean hostigadas, extorsionadas, juzgadas, intimidadas y denigradas (Hearn y Hall, 2018), lo cual tiene graves consecuencias en desmedro de las víctimas, no solo desde el ámbito de transgresión de su intimidad y dignidad en general, sino que además es un atentado contra su integridad síquica y física: «De acuerdo con el estudio efectuado por Cyber Civil Right Initiative, sobre el 80% de las víctimas de pornografía no consentida experimentan grave angustia emocional, llegando algunas al extremo del suicidio» (Keats y Franks, 2014: 351).

En Chile, por motivo de la escasez de datos estadísticos, es difícil la visibilización de este problema. Sin embargo, de acuerdo con el informe «Violencia de género en internet en Chile» de la Fundación Datos Protegidos, en el cual se encuestó a mujeres y personas de la comunidad LGTBQ+, 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 consentimiento, y 10,2% de extorsión en la red (Matus, Rayman y Vargas, 2018: 14).

Respecto al ámbito normativo de Chile, la Ley 19.628 y la actual normativa del Código Penal no otorgan los mecanismos necesarios para proteger a las víctimas de la pornografía no consentida. Por una parte, según lo dispuesto en la Ley, las imágenes de una persona son un dato personal y, cuando éstas proyectan aspectos relacionados con el libre desenvolvimiento sexual, tienen la categoría de datos sensibles; por lo tanto, para que su tratamiento sea legal (como para difusión o almacenamiento), es necesario contar con el consentimiento del titular y utilizarlas en concordancia con la finalidad para el cual se otorgó (como el uso único y exclusivo del compañero

65. En Israel, Filipinas, Francia y Alemania es un delito.

sexual). Sin embargo, como bien hemos señalado respecto de las falencias de la Ley, el no disponer de un proceso judicial idóneo y carecer de una autoridad de control y protección en materia de datos personales lleva a que en la práctica las personas, que por lo general son mujeres, no puedan ejercer los derechos que les reconoce la Ley. Por otra parte, el Código Penal, ni en su artículo 161-A (tipifica delitos penales contra a vida privada) ni 161-B (chantaje) dispone sanciones en contra de la difusión *no consentida* de material íntimo o de carácter sexual que se obtuviera de manera *consentida*,[66] lo que deja en una completa indefensión a las víctimas de estas malas prácticas. Esto constituye una grave limitación a la autonomía y autodeterminación del propio cuerpo por limitar el desenvolvimiento y desarrollo de las personas, y en general de las mujeres, en el ámbito de su intimidad, ante el peligro de que el material que enviaron en un contexto íntimo y de buena fe sea difundido y conocido por terceras personas.

Lo anterior adquiere especial relevancia por la pandemia del covid-19, durante la cual las manifestaciones íntimas de carácter erótico y sexual se han incrementado a través del uso de las tecnologías. Es más, varias aplicaciones de citas habilitaron videochats para interactuar ante este nuevo escenario,[67] por lo que es imperioso que tanto el Estado como la sociedad en general comprendan que los derechos humanos deben ser respetados y promovidos en el ciberespacio.

Recomendaciones

El Estado, a través del Comité Interministerial sobre Ciberseguridad, debe definir qué se entiende por enfoque de género en el contexto del respeto y promoción de los derechos fundamentales en ciberseguridad. Solo de esta forma se podrán otorgar las directrices para enfrentar los desafíos y amenazas que impone el uso del ciberespacio a la ciberseguridad. Estimamos que, para la consecución de lo anterior, el Estado debe partir por identificar a través de estudios y encuestas periódicas los principales riesgos, amenazas y falencias que sufren las mujeres en Chile ante el desarrollo y uso del ciberespacio. Para tales efectos, consideramos que dentro de los indicadores que se deben incluir para el desarrollo de la perspectiva de género en ciberseguridad, destacan, para identificar el origen de la escasez de mujeres dedicadas a la ciberseguridad en Chile:

66. Para más información, véase el Boletín 12164-07, «Modifica el Código Penal con el objeto de sancionar la difusión no consentida de material con connotación o de índole sexual», 10 de octubre de 2018, disponible en https://bit.ly/2PWWUit.

67. El artículo hace alusión sobre cómo el confinamiento originado por la pandemia del covid-19 preparará el escenario para la revolución de la tecnología sexual. Tanya Basu, «Sexo y amor en tiempo de coronavirus: Las citas *online* se disparan», *MIT Technology Review,* 30 de marzo de 2020, disponible en https://bit.ly/3dgcDBd.

- Identificación cuantitativa de mujeres que estudian o trabajan en alguna de las ramas dedicadas a la ciberseguridad y sus motivaciones.
- Entrevistar a mujeres dedicadas a la ciberseguridad y consultar si consideran haber sufrido algún tipo de discriminación o violencia de género en el ejercicio de sus funciones.
- Elaborar encuestas a adolescentes y niñas para medir el conocimiento e interés que tienen en tecnologías y en específico en ciberseguridad.

Luego, para comprender la discriminación y violencia de género que sufren las mujeres de Chile en el ciberespacio, se sugiere:

- Identificar por grupo etario y étnico a las mujeres que hacen uso de internet y las finalidades de este uso.
- Consultar a las mujeres que hacen uso de internet si han sido víctimas de violencia de género o discriminación en línea y si conocen los derechos que pueden hacer valer ante alguna amenaza o transgresión.

Solo en la medida en que el Estado, en colaboración con el sector privado, la academia y la sociedad civil, pueda recabar y analizar esta información, podrá trabajar en las directrices y consejos dirigidos a los diversos actores sociales.

El Estado debe impedir que el argumento de seguridad nacional sea una excusa para que autoridades estatales y municipales ejecuten medidas de seguridad desproporcionadas en desmedro de los derechos fundamentales de la ciudadanía y en específico de las mujeres. Para tales efectos, consideramos que el Estado debe coordinar, entre sus agencias y las municipalidades, capacitaciones en temas de ciberseguridad y género, con el objetivo de que los funcionarios comprendan la importancia de la perspectiva de género en el ejercicio de sus labores desde un ámbito normativo y ético. Asimismo, desde el ámbito de compras públicas de índole tecnológica, sugerimos a las agencias considerar dentro de los criterios de evaluación en sus adjudicaciones, el otorgamiento de puntaje por el cumplimiento de cuota de género por parte de los oferentes de servicios y productos tecnológicos. Esto último con el objetivo de incentivar al sector privado en la contratación y capacitación de mujeres en tecnología.

El Estado y la sociedad en general deben dirigir sus esfuerzos a incentivar a las niñas y adolescentes a estudiar carreras relacionadas con la ciberseguridad. La generación de nuevos talentos no puede ser limitada por prejuicios sociales. Asimismo, es importante continuar motivando a las profesionales en el área para instar su empoderamiento a través de talleres y otorgando becas de especialización de capacitación en Chile y en el extranjero.

Por último, el organismo encargado de la protección de datos personales debe otorgar eficiencia y eficacia a la nueva normativa que se dicte en materia de pro-

tección de datos, para lo cual debe considerar el enfoque de género al momento de emitir sus informes, directrices y decisiones. En consecuencia, el organismo fiscalizador debe contar con las facultades necesarias de coerción para exigir, tanto al sector público como privado, altos estándares en materia de seguridad de los datos.

Conclusiones

La ciberseguridad debe ser comprendida desde una perspectiva de derechos humanos que propicie su aseguramiento, promoción y respeto en el ciberespacio. A partir de esta consideración, el principal objetivo de la Política Nacional de Ciberseguridad de Chile es mejorar los estándares de seguridad en el ciberespacio para asegurar el pleno goce de los derechos fundamentales de las personas en igualdad de condiciones.

Para concretar este objetivo, la colaboración y cooperación multisectorial es esencial. Los ciberataques afectan a todos por igual, por lo que la prevención y la gestión de incidentes en el ciberespacio deben ser abordados por todos los actores de la sociedad.

La importancia de considerar un enfoque de género en el respeto y promoción de los derechos humanos ha sido recalcada en diversos organismos internacionales, dado que existe acuerdo a nivel de los Estados de que mientras existan prejuicios, discriminaciones y arbitrariedades en desmedro de los derechos de ciertos grupos, como ocurre con las mujeres, la igualdad en los derechos humanos seguirá siendo solo un concepto idílico.

Por ello, la transversalización del enfoque de género es primordial para hacer frente a esta desigualdad. En la medida que todos los sectores de la sociedad colaboren en la implementación de estrategias políticas y técnicas que sean inclusivas con el género femenino, estaremos un paso más cerca de lograr la igualdad sustantiva en esta materia.

Cuanto menor sea la brecha de género, más próximos estaremos de lograr la igualdad sustantiva. En el ámbito de la ciberseguridad, esta brecha ciertamente es preocupante. Por una parte, se manifiesta en la falta de formación e inclusión femenina en el área; por otra, en los riesgos particulares que sufren las mujeres en el ciberespacio por el hecho de ser tales, particularmente la amenaza y transgresión de su derecho a la privacidad y protección de sus datos personales.

La falta de especialistas en temas de ciberseguridad es alarmante. Cada día surgen nuevas y creativas formas a través de las cuales se llevan a cabo ciberataques. En consecuencia, incentivar y generar nuevos talentos que provengan de todos los sectores de la sociedad es de vital importancia para mantener un sistema informático robusto y resiliente.

En la medida en que no se adopten directrices tendientes a incentivar a las mujeres desde la temprana edad a capacitarse en temas de TIC, la carencia de talentos

en áreas relacionadas con la ciberseguridad solo aumentará. Consideramos que esto tendrá por principal consecuencia la mantención de los sesgos de géneros en el desarrollo y uso de tecnologías que no son neutrales, sino que proyectan los estereotipos y patrones culturales de quienes intervienen en ellas.

Solo en la medida en que aseguremos e incentivemos una amplia participación femenina en el ámbito de la ciberseguridad, podremos lograr un ciberespacio libre, abierto, seguro, resiliente e igualitario.

Referencias

Álvarez Valenzuela, Daniel y Francisco Vera Hott (2017). «Ciberseguridad y derechos humanos en América Latina». En Agustina del Campo (compiladora), *Hacia una internet libre de censura II: Perspectivas en América Latina*. Buenos Aires: Universidad de Palermo. Disponible en https://bit.ly/2Lo8IvW.

Anwar, Mohd, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li y Li Xud (2017). «Gender difference and employees' cybersecurity behaviors». *Computers in Human Behavior*, 69: 437-443. DOI: 10.1016/j.chb.2016.12.040.

Bascuñán, Antonio (2005). «Delitos contra los intereses personalísimos». *Revista de Derecho de la Universidad Adolfo Ibáñez*, 1: 531-556.

Castaño, Cecilia (2008). *La segunda brecha digital*. Madrid: Cátedra.

Castro Valdebenito, Hugo y Alessandro Monteverde (2018). «Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito». *Espacios*, 39 (39). Disponible en https://bit.ly/3fgD3V5.

Conicyt, Comisión Nacional de Investigación Científica y Tecnológica (2017), «Igualdad de género en ciencia, tecnología e innovación en Chile». Disponible en https://bit.ly/2SvsGms.

Dammert, Lucía y Constanza Núñez (2019). «Enfrentando las ciberamenazas: Estrategias nacionales de ciberseguridad en el Cono Sur». *Seguridad, Ciencia y Defensa*, 5 (5): 1-23. Disponible en https://bit.ly/2XnklTM.

De Mauro, Andrea, Marco Greco y Michele Grimaldi (2016). «A formal definition of Big Data based on its essential features». *Library Review,* 65 (3): 122-135. DOI: 10.1108/LR-06-2015-0061.

Díaz, Regina (2007). «Delitos que vulneran la intimidad de las personas: Análisis crítico del artículo 161-A del Código Penal Chileno». *Ius et Praxis,* 13 (1): 291-314. DOI: 10.4067/S0718-00122007000100011.

Durack, Katherine T. (1997). «Gender, technology, and the history of technical communication», *Technical Communication Quarterly Journal*, 6 (3): 249-260. DOI: 10.1207/s15427625tcq0603_2.

Garrido, Romina y Sebastián Becker Castellaro (2017). «La biometría en Chi-

le y sus riesgos». *Revista Chilena de Derecho y Tecnología,* 6 (1): 67-91. DOI: 10.5354/0719-2584.2017.45825.

Hearn, Jeff y Matthew Hall (2018). «This is my cheating ex: Gender and sexuality in revenge porn». *Sexualities,* 22 (5-6): 1-23. DOI: 10.1177/1363460718779965.

Kay, Matthew, Cynthia Matuszek y Sean A. Munson (2015). «Unequal representation and gender stereotypes in image search results for occupations». En *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 3.819-3.828). Nueva York: Association for Computing Machinery. DOI: 10.1145/2702123.2702520.

Keats, Danielle y Mary Anne Franks (2014). «Criminalizing revenge porn». *Wake Forest Law Review*, 49: 345-391. Disponible en https://bit.ly/2KZ88i5.

Leiva, Eduardo (2015). «Estrategias nacionales de ciberseguridad: Estudio comparativo basado en enfoque *top-down* desde una visión global a una visión local». *Revista Latinoamericana de Ingeniería de Software*, 3 (4): 161-176. DOI: 10.18294/relais.2015.161-176.

Marwick, Alice E. (2017). «Scandal or sex crime? Gendered privacy and the celebrity nude photo leaks». *Ethics and Information Technology,* 19: 177-191. DOI: 10.1007/s10676-017-9431-7.

Matus, Jessica, Danny Rayman y Rodrigo Vargas (2018). *Violencia de género en internet en Chile*. Santiago: Datos Protegidos. Disponible en https://bit.ly/2KZ8xRD.

Noble, Safiya (2018). *Algorithms of oppression: How search engines reinforce racism*. Nueva York: NYU Press.

Peña, Paz (compiladora) (2017). «Reporte de la situación de América Latina sobre la violencia de género ejercida por medios electrónicos». Presentación para Naciones Unidas. Disponible en https://bit.ly/35tiss5.

Rodríguez, Patricio, Norma Palomino y Javier Mondaca (2017). «El uso de datos masivos y sus técnicas analíticas para el diseño e implementación de políticas públicas en Latinoamérica y el Caribe». Disponible en https://bit.ly/2Sv2Pve.

Sancho Hirane, Carolina (2018). «Ciberseguridad y política pública en Chile: Avance recientes, ¿optimismo futuro?». ANEPE. Disponible en https://bit.ly/35soXZn.

Tene, Omer y Jules Polonetsky (2012). «Privacy in the age of Big Data: A time for big decisions». *Standford Law Review,* 64. Disponible en https://stanford.io/2YwdjOL.

Viollier, Pablo (2017a). *El estado de la protección de datos personales en Chile.* Santiago: Derechos Digitales. Disponible en https://bit.ly/3c2UxCo.

—. (2017b). *La participación en la elaboración de la Política Nacional de Ciberseguridad: Hacia un nuevo marco normativo en Chile*. Santiago: Derechos Digitales. Disponible en https://bit.ly/2Svt2JU.

West, Mark, Rebeca Kraut y Han Ei Chew (2019). *I'd blush if I could: Closing gender divides in digital skills through education*. Unesco y Equals Skill Coalition. Disponible en https://bit.ly/2SzBDeF.

Sobre la autora

Paloma Herrera Carpintero es abogada. Licenciada en Ciencias Jurídicas y Sociales por la Universidad de Chile y diplomada en Ciberseguridad por la misma institución. Investigadora del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile. Su correo electrónico es pherrera@derecho.uchile.cl. https://orcid.org/0000-0001-6174-9822.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).