



## The gender focus in Chile`s National Cyber Security Policy<sup>1</sup>

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

Paloma Herrera Carpintero  
Centro de Estudios en Derecho Informático  
Facultad de Derecho, Universidad de Chile

#### 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).

Las fronteras físicas 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, 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 infraestructuras críticas (banca, salud, transporte, entre otros) y al robo de información (por ejemplo, *phishing*).

El ciberespacio debe ser comprendido como un ámbito de información digital que va más allá de internet y que incluye las interacciones humanas que allí se producen (Álvarez Valenzuela y Vera Hott, 2017: 40). Por lo tanto, es un ámbito en el que las personas proyectan su libertad y desarrollo. Lo que ha aumentado producto de la pandemia del Covid-19, la que ha provocado que las personas dependan aún más de las TIC. La importancia del ciberespacio, hace necesario replantear la noción de derechos humanos, con el fin de que sean respetados, cumplidos y protegidos en el ciberespacio.

La ciberseguridad, no solo se debe entender 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 hay que considerarla

---

<sup>1</sup> El presente texto fue elaborado por Daniela Olivares Rojas, asistente de investigación del Centro de Estudios en Derecho Informático, y corresponde a un resumen del artículo *El enfoque de género en la Política Nacional de Ciberseguridad de Chile*, de Paloma Herrera Carpintero, publicado en la Revista Chilena de Derecho y tecnología, Vol 9 Núm 1. (2020), elaborado para ser presentado en el evento internacional "Gender approaches to cyber security". Disponible en: <https://rchdt.uchile.cl/index.php/RCHDT/article/view/51577/61679>



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 debemos contar con la cooperación de los sectores públicos y privados, la sociedad civil y la ciudadanía en general.

En materia de ciberseguridad una de las grandes preocupaciones a nivel mundial es la falta de talento y profesionales especializados. El informe Cybersecurity Work Force de 2019<sup>2</sup> señaló que la fuerza laboral global de técnicos y profesionales necesita crecer 145% y que los profesionales de ciberseguridad tienen el doble de probabilidades de ser hombres.

Las mujeres, por razones históricas y culturales, son discriminadas por el hecho de ser tales (Durack, 1997), son discriminadas por el solo hecho de ser tales (Durack, 1997), sesgo que también se ha traspasado en el diseño e implementación de la tecnología, la cual no ha sido ni es neutral. Ejemplo de esto es la feminización de los asistentes virtuales como Siri, Alexa o Cortana.

### **La Política Nacional de Ciberseguridad de Chile<sup>3</sup>**

En el año 2015 se crea el Comité Interministerial sobre Ciberseguridad (CICS), entidad encargada de proponer la Política Nacional de Ciberseguridad y asesorar en la coordinación de acciones, planes y programas a los distintos actores institucionales.

A principios de 2017 se crea la 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 las personas en igualdad de condiciones. La mencionada 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; iv) gestión de riesgos del ciberespacio.

La Política estableció velar por el respeto y promoción de los derechos fundamentales en el ciberespacio (página 12). También señala que, en materia de derechos fundamentales, se empleará «un enfoque de género, que permita hacer visible y enfrentar desigualdades que enfrentan los diversos grupos en el ciberespacio» (página 15). Lo anterior es relevante, porque a nivel latinoamericano Chile ha sido el único país que dispuso explícitamente la necesidad del enfoque de género en materia de ciberseguridad.

La promoción de los derechos fundamentales en el ciberespacio en la Política, concuerda con la Carta de Derechos Humanos y Principios para Internet<sup>4</sup>, 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).

<sup>2</sup> Disponible en <https://bit.ly/3f5NQ4k>.

<sup>3</sup> «Política Nacional de Ciberseguridad», Gobierno de Chile, 2017, p.12, disponible en <https://bit.ly/2Rgcipj>.

<sup>4</sup> Disponible en <https://bit.ly/3g64UYD>.



Para conseguir lo anterior, los Estados deben intensificar sus esfuerzos para prevenir y eliminar cualquier violación, abuso, discriminación y violencia contra mujeres y niñas en el contexto digital.

Es necesario evidenciar que en la Política se omitió el establecimiento de parámetros explícitos respecto de los 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. Al no contar con estos parámetros, no es posible verificar si el estatuto de las mujeres ha mejorado en la sociedad.

Una de las principales medidas a considerar para lograr un cambio sustancial en 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. Sin embargo, estas prácticas actualmente en Chile son casi inexistentes.

Para que se pueda cumplir de manera eficaz el postulado de la Política Nacional de Ciberseguridad referente a la perspectiva de género, es necesaria la generación de encuestas e informes que de cuenta de la relación de las mujeres en Chile con el ciberespacio y en específico con la ciberseguridad. Como mínimo, se debiese considerar un indicador laboral (estadística 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.

### **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 las mujeres han sido discriminadas y privadas de participación en trascendentales instancias del acontecer social, esto que esta presente en el espacio físico puede intensificarse en el espacio digital.

Para aminorar la discriminación que sufren las mujeres, desde la década de los noventa la comunidad internacional de derechos humanos comenzó a hacer alusión al enfoque de género y a 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 del papel de la mujer»<sup>5</sup>. 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.

El enfoque de género fue definido en 1997 por el Consejo Económico y Social (ECOSOC) de Naciones Unidas, como:

---

<sup>5</sup> «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/3b1jyN0>.



«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»<sup>6</sup>.

ONU Mujeres 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.

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.

Desde el ámbito de las TIC y en específico desde la ciberseguridad, la baja participación e inclusión de mujeres, se traduce en una falta de recursos humanos y de herramientas técnicas necesarias para enfrentar los desafíos y riesgos actuales en el espacio digital. A nivel mundial, la ciberseguridad no ha logrado cumplir con la demanda de profesionales 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.

### **La brecha de género en el ámbito de la ciberseguridad**

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, señala que a nivel latinoamericano, si bien mujeres y hombres tienen el mismo acceso a computadores y conexión a internet, al analizar el uso de las tecnologías existe una brecha digital, siendo el porcentaje de mujeres menor al de hombres. Esto demuestra falta de interés y desconocimiento generalizado en este aspecto por parte del grupo femenino, en gran medida por los estereotipos de género negativos en torno a las TIC.

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

---

<sup>6</sup> «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>.



promocionar la participación de mujeres en el área requiere de un esfuerzo social 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 por prejuicio sociales inculcados desde muy temprana edad<sup>7</sup>.

La educación en temas de TIC y ciberseguridad es el principal mecanismo para lograr la desconstrucción del machismo en este ámbito y el fin de las conductas abusivas contra las mujeres en el ciberespacio. Para tales efectos, los planes de educación deben iniciarse a temprana edad, para que las mujeres tengan el empoderamiento, la flexibilidad y la habilidad de desarrollar un análisis crítico, libre de prejuicio y discriminaciones basadas en el género.

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

El derecho a la privacidad y el derecho a la protección de datos personales son especialmente afectados en el ciberespacio.

Como los estereotipos de discriminación del mundo físico se manifiestan en el mundo virtual, las mujeres tienen una tasa más alta de acoso en línea en comparación con la población masculina, traspasando muchas veces el acoso y las amenazas el mundo virtual, generando efectos negativos en las mujeres que son víctimas de estas conductas.

Para cumplir con la Política, el análisis con perspectiva de género de la vida privada y la protección de datos personales debe comprender las amenazas particulares a las cuales están predispuestas las mujeres en el ciberespacio, para establecer indicadores, medidas de prevención y coerción en caso de vulneración.

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 la tecnología han dejado a las mujeres expuestas a: i) vigilancia focalizada, descontrolada y abusiva; ii) tratamiento abusivo e indiscriminado en el contexto de *big data*; iii) pornografía no consentida; entre otros.

#### **i) Vigilancia focalizada, descontrolada y abusiva**

El uso de tecnologías de vigilancia 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»<sup>8</sup>.

Independiente de que este tipo de tecnología se ha implementado con la justificación de la protección de la seguridad nacional, en la práctica se ha convertido en una política de vigilancia masiva y altamente intrusiva.

---

<sup>7</sup> 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>.

<sup>8</sup> «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/3giRIVB>.



Si bien este tema afecta a la ciudadanía en general, el uso de estas tecnologías puede vulnerar aún más a las mujeres. En 2011 una ONG norteamericana American Civil Liberties Union, advirtió que, los drones podrían ser utilizados incluso para registrar la intimidad sexual de las parejas en sus hogares con finalidades voyeristas<sup>9</sup>. Cuestión que ya está corriendo a nivel global, por lo que abunda material en internet obtenido con drones, donde las mujeres son las más afectadas, al verse expuestas a la cosificación sexual.

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

En el presente texto entendemos por *big data* 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 correlacionar en un determinado contexto.

Los beneficios que conlleva la utilización de *big data* por parte de los diversos sectores de la sociedad son innumerables. Destaca el ámbito público, donde el *big data* ha tenido fuerte impacto en el diseño, implementación y evaluación de políticas públicas, como 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. Para la obtención de este beneficio, los actores intervinientes en su desarrollo, implementación y análisis deben considerar un enfoque de género en la ejecución de sus labores, ya que la tecnología no es neutral y está condicionada por los sesgos históricos y culturales de sus desarrolladores y demás intervinientes. Por lo que el *big data* se puede transformar en un mecanismo abusivo y discriminatorio que vulnera los derechos humanos de las personas y, en situaciones específicas, los de las mujeres por el solo hecho de ser tales.

Otra arista importante, es 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, los algoritmos son creados y formulados por seres humanos, quienes reproducen en ellos sus sesgos, por lo que contar con la participación de mujeres y de las minorías en áreas relacionadas con la tecnología es primordial para el desarrollo de tecnologías que respeten y promuevan los derechos fundamentales.

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, otorgan información sin verificar los fines del tratamiento de los datos ni lo robusto del sistema de seguridad, lo que los hace susceptibles a ataques de ciberseguridad. Ejemplo de ello es el caso Celebgate, en el que se filtraron fotografías íntimas de varias actrices desde la plataforma iCloud de Apple, 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 difundir las imágenes. La filtración afectó únicamente a mujeres, y quienes más difundieron las imágenes fueron hombres (Marwick, 2017: 187).

---

<sup>9</sup> Informe disponible en <https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>



### iii) Pornografía no consentida

La pornografía no consentida involucra la captación o divulgación de material gráfico audiovisual de tono erótico o explícitamente sexual, sin el consentimiento de alguna de las personas retratadas y sin propósito legítimo<sup>10</sup>.

Las mujeres son las principales víctimas de estas prácticas, y quienes comente este tipo de actos habitualmente son hombres, por lo que la pornografía no consentida es reconocida como un tipo de violencia de género<sup>11</sup>.

A nivel global, los países que han legislado en contra de la pornografía no consentida tipificándola como delito en su derecho interno son la excepción<sup>12</sup>. Esto se debe a la: 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 tiene por principal finalidad avergonzar y humillar públicamente a la víctima. Sin embargo, el objetivo también puede ser el lucro, entretenimiento o voyerismo.

Diversos son los sitios web dedicados a la pornografía no consentida, en los que sus usuarios comparten gran cantidad de material fotográfico y audiovisual, acompañados en algunas ocasiones de datos personales y sensibles de la víctima (número de contacto, dirección domiciliaria, entre otros). Esto puede tener como resultado que sean hostigadas, extorsionadas, juzgadas, intimidadas y denigradas (Hearn y Hall, 2018), lo cual además de ser una transgresión de su intimidad y dignidad en general, atenta 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, los escasos de datos estadísticos hacen difícil la visibilización de este problema. Sin embargo, de acuerdo con el informe «Violencia de género internet en Chile» de la Fundación Datos Protegidos, en la 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).

## 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 directrices para enfrentar los desafíos y amenazas en el ciberespacio. Para la consecución de lo anterior, el

---

<sup>10</sup> La definición fue elaborada por el proyecto latinoamericano Acoso Online, que nace como respuesta a la violencia de género a través de la publicación no consentida de imágenes y videos sexuales o eróticos. «¿Pornovenganza?», Acoso Online, disponible en <https://bit.ly/3cTvwgd>.

<sup>11</sup> Véase «La ciberviolencia contra mujeres y niñas», Instituto Europeo de la Igualdad de Género, 2017, disponible en <https://bit.ly/2QK1UoZ>

<sup>12</sup> En Israel, Filipinas, Francia y Alemania es un delito.



Estado debe partir por identificar por medio de estudios y encuestas los principales riesgos, amenazas y falencias que sufren las mujeres en Chile ante el desarrollo y uso del ciberespacio.

Para identificar el origen de la escasez de mujeres dedicadas a la ciberseguridad en Chile, se debe:

- Identificar el número 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 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, 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, con el objetivo de incentivar 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. Además, es importante empoderar a las profesiones en el área a través de talleres y otorgando becas de especialización de capacitación.

Por último, el organismo encargado de la protección de datos personales 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 el cumplimiento de altos estándares en materia de protección de 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 por diversos organismos internacionales, ya que existe acuerdo 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.

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, como 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 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 género 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 & 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>.

CASTRO VALDEBENITO, Hugo & 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>.

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](https://doi.org/10.1207/s15427625tcq0603_2).

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](https://doi.org/10.1177/1363460718779965).

KEATS, Danielle & Mary Anne Frank (2014). «Criminalizing revenge porn». *Wake Forest Law Review*, 49: 345-391. Disponible en <https://bit.ly/2KZ88i5>.

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](https://doi.org/10.1007/s10676-017-9431-7).

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

RODRÍGUEZ, Patricio, Norma Palomino & 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>.