REPÚBLICA DE CHILE

DIARIO DE SESIONES DEL SENADO

PUBLICACIÓN OFICIAL

LEGISLATURA 368ª

Sesión 98ª, en jueves 1 de octubre de 2020

Especial

(Celebrada presencial y telemáticamente, de 10:11 a 12:00)

PRESIDENCIA DE SEÑORA ADRIANA MUÑOZ D'ALBORA, PRESIDENTA; SEÑOR RABINDRANATH QUINTEROS LARA, VICEPRESIDENTE, Y SEÑORA XIMENA RINCÓN GONZÁLEZ, PRESIDENTA ACCIDENTAL

SECRETARIO, EL SEÑOR RAÚL GUZMÁN URIBE, TITULAR

ÍNDICE

Versión Taquigráfica

Pág.

III. ORDEN DEL DÍA:

VERSIÓN TAQUIGRÁFICA

I. ASISTENCIA

Asistieron presencialmente las señoras y los señores:

—Alvarado Andrade, Claudio
—Chahuán Chahuán, Francisco
—Coloma Correa, Juan Antonio
—Ebensperger Orrego, Luz
—García Ruminot, José
—Letelier Morel, Juan Pablo
—Moreira Barros, Iván
—Muñoz D´Albora, Adriana
—Pizarro Soto, Jorge
—Pugh Olavarría, Kenneth
—Rincón González, Ximena

Asistieron telemáticamente las señoras y los señores:

—Allende Bussi, Isabel
—Aravena Acuña, Carmen Gloria
—Araya Guerrero, Pedro
—Bianchi Chelech, Carlos
—Castro Prieto, Juan
—De Urresti Longton, Alfonso
—Durana Semir, José Miguel
—Elizalde Soto, Álvaro
—Galilea Vial, Rodrigo
—García-Huidobro Sanfuentes, Alejandro
—Goic Boroevic, Carolina
—Guillier Álvarez, Alejandro
—Harboe Bascuñán, Felipe
—Huenchumilla Jaramillo, Francisco
—Insulza Salinas, José Miguel
—Lagos Weber, Ricardo
—Latorre Riveros, Juan Ignacio
—Montes Cisternas, Carlos
—Navarro Brain, Alejandro
—Órdenes Neira, Ximena
—Ossandón Irarrázabal, Manuel José
—Prohens Espinosa, Rafael
—Provoste Campillay, Yasna
—Quintana Leal, Jaime
—Quinteros Lara, Rabindranath
—Sabat Fernández, Marcela
—Sandoval Plaza, David
—Soria Quiroga, Jorge
—Von Baer Jahn, Ena

Actuó de Secretario General el señor Raúl Guzmán Uribe, y de Prosecretario, el señor Roberto Bustos Latorre.

II. APERTURA DE LA SESIÓN

—Se abrió la sesión a las 10:11

La señora MUÑOZ (Presidenta).– En el nombre de Dios y de la Patria, se abre la sesión.

III. ORDEN DEL DÍA

LANZAMIENTO OFICIAL DE MES NACIONAL DE LA CIBERSEGURIDAD

El señor GUZMÁN (Secretario General).– Por orden de la señora Presidenta, se ha citado a esta sesión especial, la cual fue solicitada por los Honorables Senadores Kenneth Pugh y señor Felipe Harboe, con el objeto de realizar el lanzamiento oficial del Mes Nacional de la Ciberseguridad.

En esta sesión intervendrán la señora Presidenta del Senado, Senadora señora Adriana Muñoz; el Senador señor Felipe Harboe; la señora Rosa Díaz, Directora General del Instituto Nacional de Ciberseguridad de España; el Senador señor Kenneth Pugh; y el señor José María Alonso, profesional en materia de informática español y CDCO de Telefónica, quien efectuará una presentación titulada “Ciberseguridad y Sociedad”.

Posteriormente, se entregará la palabra a quienes hoy día están asistiendo a esta sesión especial, para realizar preguntas.

Es todo, señora Presidenta.

La señora MUÑOZ (Presidenta).– Gracias, señor Secretario.

Entrego un saludo a las señoras Senadoras, Senadores presentes en esta sesión, muy especialmente a nuestros invitados: la señora Rosa Díaz, Directora General del Instituto Nacional de Ciberseguridad de España; y el señor José María Alonso, profesional español y CDCO de Telefónica.

Esta sesión especial tiene como propósito lanzar oficialmente el Mes de la Ciberseguridad.

Se trata de un hito que se ha venido consolidando en aplicación de la ley N° 21.113, cuyo objeto es la promoción y realización de ejercicios nacionales relacionados con la ciberseguridad y que convoca a actores públicos y privados al mundo de la academia y a la sociedad civil.

Quiero felicitar, asimismo, el empeño de los Senadores Pugh y Harboe, quienes han liderado este esfuerzo y, desde hace años, vienen encabezando una verdadera cruzada por visibilizar esta materia y relevarla en el debate público, incluso desde antes de que adquiriera la connotación que por la fuerza de los hechos ha tomado en la actualidad.

Como es de conocimiento público, el mundo ha tenido un salto notable en las últimas décadas en ciencia y tecnología.

Se han creado y puesto a disposición de la humanidad un número inimaginable de avances de enorme significación.

La inteligencia artificial, los metadatos, la robótica, unida a la masificación de las telecomunicaciones han generado transformaciones muy profundas en nuestro modo de vida cotidiano: se mejora la calidad de vida, se interconecta a las personas, se agilizan los procesos productivos, se simplifican los trámites.

Este mismo Senado viene funcionando hace meses en forma telemática, cuestión que para muchos de nuestros antecesores en estos escaños hubiera constituido un ejercicio de ciencia ficción.

Basta pensar como era la vida hace solo una o dos décadas y prescindir por un rato de los elementos que se han incorporado a nuestro quehacer doméstico en este lapso de tiempo, para representarnos los profundos cambios que hemos experimentado.

Sin embargo, como es propio de la naturaleza humana, cada desarrollo o avance científico o tecnológico genera también el riesgo de usos ilícitos o equivocados.

Cada día, en todo el mundo, miles de intrusiones, usurpaciones de identidad, sabotajes y delitos comunes realizados a través de medios informáticos afectan a personas y a entidades corporativas públicas y privadas.

Solo por poner algunos ejemplos:

Como sabemos, hace unos días BancoEstado sufrió un ataque que obligó a mantener varios días numerosas sucursales cerradas.

Al mismo tiempo, el Servicio de Migraciones argentino había sido objeto de una vulneración similar.

El pasado lunes ocurrió un ataque a CMA, CGM, una de las mayores empresas navieras del orbe.

Antes de ayer se registró uno de los mayores ataques de este tipo en la historia de los Estados Unidos, dañando los sistemas de atención de una gigantesca red de hospitales y centros médicos.

Y, así, los intentos frustrados o exitosos que se suceden a diario son innumerables.

Cabe destacar, asimismo, la enorme complejidad del asunto.

Primero, por sus características extraterritoriales o incluso, de algún modo, aterritoriales, y la dificultad investigativa que ello conlleva.

Segundo, porque se trata habitualmente de crimen organizado de gran envergadura, alta sofisticación y con experticia en la materia. Como se ha advertido, estamos ante verdaderas empresas dedicadas a los ilícitos tan especializados como lucrativos.

Es por ello que los países han ido poniendo de relieve su preocupación por estas materias. Tanto en el ámbito nacional como en el plano global se refuerzan medidas de prevención y seguridad.

El Convenio sobre la Ciberdelincuencia, del Consejo de Europa (Convenio de Budapest), abierto a la ratificación de otros países y suscrito por Chile, es sin duda uno de los principales esfuerzos mundiales. Establece directrices para las naciones adherentes y obliga a la cooperación para la investigación y persecución de estas conductas. También impone el deber de tipificar ciertas conductas y estable-

cer mecanismos eficaces de investigación.

Lamentablemente, nuestro país presenta importantes falencias.

Pese a haber suscrito dicho tratado y a haber puesto en marcha, ya hace años, la Red de Interconectividad del Estado, coordinando sus esfuerzos con instituciones públicas y privadas, nuestra legislación presenta retrasos severos.

La Ley de Delitos Informáticos, que data de los albores de esta tecnología, se apresta a cumplir tres décadas, lapso en que, como indicaba previamente, la materia ha tenido un avance vertiginoso. Vale decir, es un texto que está claramente desfasado: muchas conductas no se encuentran tipificadas y los procedimientos y sanciones son irrisorias. Esperamos, por cierto, que se agilice el trámite de la iniciativa respectiva.

Lo mismo puede decirse respecto de la protección de datos personales. Si bien el cuerpo legal respectivo ha tenido múltiples modificaciones en otros ámbitos, aún no contempla los estándares de protección que las ciudadanas y los ciudadanos merecen. Tampoco hemos dado con un organismo que asuma esta función.

A nivel privado, la situación tampoco es mejor.

Aún hay muchas entidades que no han tomado conciencia de la gravedad del asunto y operan con niveles de seguridad extremadamente bajos. La inversión en este punto suele ser insuficiente para la magnitud de la amenaza.

Por ello es muy importante la realización de este tipo de encuentros y todos los que se realizarán en este mes, que nos permiten tomar conciencia de la importancia de este desafío y aumentar el conocimiento que todas y todos tenemos sobre la ciberseguridad, y que nos alientan a asumir responsabilidades para legislar con la prisa que necesitamos.

Es de esperar que en estos días surjan los consensos necesarios para avanzar definitivamente en una ley marco que permita definir una institucionalidad y los responsables de una Estrategia y de un Plan Nacional sobre la Ciberseguridad coherentes con la importancia que este bien público ha adquirido para nuestra sociedad.

Les deseo, estimados colegas, mucho éxito en este Mes Nacional de la Ciberseguridad que inauguramos.

Muchas gracias.

He dicho.

El señor GUZMÁN (Secretario General).– A continuación, hará uso de la palabra el Senador señor Felipe Harboe.

El señor HARBOE.– Muchas gracias, señor Secretario.

Señora Presidenta, en primer lugar, quiero saludar a nuestros invitados internacionales: a la Directora del Incibe y, por cierto, también al "Chema" Alonso. Creo que es muy importante contar con la presencia de la autoridad nacional española en materia de ciberseguridad.

Ciertamente, como decía la Presidenta del Senado, hoy por hoy el mundo transita de manera muy rápida hacia lo que se ha denominado ya no solo "economía digital", sino que "era digital". Los derechos ciudadanos cada día se exhiben, se desarrollan y se ejercen de mejor manera en el ciberespacio, y por tanto es un rol fundamental de los legisladores y de las legisladoras tener la capacidad de adelantarnos y entender que el mundo digital requiere de la adecuación de nuestra cultura, de nuestras conductas, de nuestra legislación, de nuestra forma de hacer las políticas públicas. Y eso pasa necesariamente por tener, en primer lugar, conciencia de la relevancia del impacto de los procesos digitales en nuestro desarrollo democrático y ciudadano.

Dicho lo anterior, entonces, todo tipo de desarrollo informático requiere que se dote a los ciudadanos, a las empresas, a las multinacionales, y particularmente a los Estados, de condiciones de seguridad en el tránsito de la información, de los datos, pero también de las transacciones. En definitiva, dar certezas de

que es posible desarrollar un mundo digital.

La estrategia España Digital 2025, recientemente lanzada, es un ejemplo de política pública, para ubicar no solo al sector público, sino al país, a la nación, como una república de carácter digital.

Junto con el Senador Kenneth Pugh estamos trabajando en una propuesta que haremos prontamente, para que Chile sea una república digital muy luego. Y, por cierto, el plantear la creación, la instalación de una república digital, supone necesariamente, en primer lugar, el contar con una infraestructura de redes que nos permita interconectar a nuestros ciudadanos y ciudadanas, tener la posibilidad de que efectivamente gran parte de la relación entre el Estado y los ciudadanos sea digital, con tiempos reducidos, con criterios objetivos de decisión, y particularmente con una interoperabilidad que aumente la eficacia y la eficiencia en nuestras relaciones. Pero esa interrelación también va a suponer que esa infraestructura de redes permita crear una cultura digital, de tramitación digital, de gestiones digitales, de educación digital, de sesiones digitales, como estamos hoy día. ¿Y por qué no pensar en alternativas más estables en esta materia?

Para que todo esto ocurra se requiere -lo hemos planteado con el Senador Kenneth Pugh-, contar con una legislación adecuada. Bien lo decía nuestra Presidenta del Senado: Chile tiene una legislación del año 1993, antes de la existencia de Facebook, antes de la existencia de las redes sociales. Esa es la legislación en materia de delitos informáticos. Si bien Chile adhirió al Convenio de Budapest, lamentablemente han pasado muchos años de inactividad en estas materias. Nuestro Senado despachó hace un tiempo el proyecto que adecúa toda nuestra legislación en materia de delitos informáticos al Convenio de Budapest, que hoy está en la Cámara de Diputados, y esperamos que prontamente sea aprobado, para contar con un marco regulatorio que sancione a aquellos que hacen del cibercrimen su actividad habitual, o una forma de ir condicionando los procesos de desarrollo.

Pero, junto con ello, también se requiere hacer entender lo importante del ámbito preventivo, en el sentido de que en materia informática es exactamente igual que en la salud cuando se dice que es mejor prevenir que curar. Y la ciberseguridad es justamente la prevención, es decir, el conjunto de mecanismos que tienen por objeto evitar un impacto negativo en todos nuestros procesos digitales.

En consecuencia, creo que también se requiere crear una cultura de ciberseguridad, y para eso estamos esperando que el Gobierno de Chile mande el proyecto que se comprometió hace ya más de un año para establecer un marco de ciberseguridad, mediante la creación de una institucionalidad, que esperamos, con humildad lo decimos, que sea muy parecida al Incibe español, que ha tenido un desarrollo muy importante y ha aportado decididamente a dar condiciones de seguridad, lo que ubica hoy día a España como un referente en esta materia, dentro de los países líderes mundiales que seguir.

Por consiguiente, pienso que estamos en presencia de una revolución digital que demanda de los legisladores, de los gobernantes, de los líderes, del mundo de las empresas, del mundo de los ciudadanos, tomar conciencia de la importancia del desarrollo digital y de la ciberseguridad como un elemento fundamental.

Y junto con ello, evidentemente, lo que transita por las redes: información, datos, es esencial, es parte de nuestros atributos de la personalidad, y requiere una legislación adecuada. Hace ya más de seis meses despachamos un proyecto de ley sobre el particular en la Comisión de Constitución, y estamos a la espera de que se reactive para poder contar con una legislación que, además de entregar garantías en ciberseguridad, establezca el principio de responsabilidad y de seguridad de los datos personales. Estamos convencidos de que la pronta aprobación de un proyecto de esa natu-

raleza nos va a ubicar como país adecuado en la Comunidad Europea, porque así lo hemos conversado con todas las autoridades tanto españolas como de la Comunidad Europea.

Así que bienvenidos a este Mes de la Ciberseguridad. Agradezco a las Senadoras y los Senadores que sean parte, y por cierto espero que puedan aprovechar toda la experiencia del Incibe y de "Chema", que nos van a ilustrar con su experiencia en estas materias.

¡Bienvenidos a todos y a todas en el Mes de la Ciberseguridad!

El señor GUZMÁN (Secretario General).– A continuación, hará uso de la palabra la señora Rosa Díaz, Directora General del Instituto Nacional de Ciberseguridad de España.

La señora DÍAZ (Directora General del Instituto Nacional de Ciberseguridad de España).– Buenos días a todos.

Buenas tardes, desde España.

"Chema", Presidenta del Senado, Senadores, asistentes, un honor compartir con ustedes esta sesión especial de inauguración, hoy, primer día de octubre, Mes de la Ciberseguridad.

Recuerdo con mucho cariño mi participación en el II Seminario Internacional de Ciberseguridad en Chile, de manera presencial, hoy hace un año, y quiero agradecerle al Senador Pugh, al resto de su equipo, y a José Luis Manzanera, de la Embajada española en Chile, la cordial acogida con la que me recibieron. Es una pena que este año no hayamos podido estar allí.

Un año después estamos viviendo tiempos de cambio, en los que nos hemos visto obligados, todos, a replantearnos nuestro presente y nuestro futuro no solo como individuos, sino también como entidades que forman parte del relevante escenario global de la seguridad digital. Durante esta situación tan excepcional y extraña, que ha trastocado lo que antes conocíamos como normalidad, hemos tomado mayor consciencia de la importancia de la digitalización como una de las mejores soluciones a los retos que nos hemos ido encontrando en el camino.

En este tiempo hemos roto paradigmas digitales y si algo hemos aprendido durante estos meses es que, utilizando los recursos disponibles de manera segura, todos avanzamos y eliminamos las barreras que surgen a nuestro paso. Juntos hemos contrastado que los problemas pueden ser globales y afectar por igual a todos, sin diferenciar entre territorios, y que la única manera de afrontarlos con éxito es hacerlo unidos.

Hoy más que nunca la tecnología, lejos de separarnos, reduce distancias y nos acerca a todos mucho más.

Precisamente este mes se cumplen quinientos años del descubrimiento del Estrecho de Magallanes. Se trató de uno de los eventos históricos considerados como precursores de lo que hoy conocemos como "globalización". Ni el portugués Fernando Magallanes ni su sustituto en el mando de la expedición, el español Juan Sebastián de Elcano, pretendieron jamás circunnavegar la Tierra por primera vez en la historia. Solo buscaban las preciadas especias de las Indias Orientales.

Pero, al completar un giro al planeta, navegando siempre en dirección oeste, dieron, sin habérselo propuesto, un primer y remoto paso a la globalización, acercando países y continentes. Hablamos de nuevo de acontecimientos imprevistos que cambian la historia y nos obligan a adaptarnos a las nuevas circunstancias. Nos ha pasado recientemente este año con la pandemia.

La COVID-19 es uno de los mayores desafíos a que se ha enfrentado la humanidad en los últimos cien años. Su impacto sanitario y económico es visible en todo el mundo. Y más allá de esas cuestiones, sin duda prioritarias, la COVID-19 ha supuesto una aceleración de las necesidades de digitalización de las empresas, los ciudadanos y los gobiernos, y ha obligado a anticipar algunos escenarios, ante los cuales hemos tenido que responder de manera inmediata: teletrabajo, estudio telemático, ventas y

compras *online*, etcétera. Estas necesidades de digitalización ya estaban de alguna forma, por supuesto, en el guion, pero, sin duda, la pandemia los ha acelerado.

De esta manera, la seguridad en el ciberespacio se ha posicionado como uno de los objetivos prioritarios dentro de las agendas de muchos países, con el fin de garantizar su seguridad nacional y de crear una sociedad digital basada en la confianza y en la divulgación de la cultura de la ciberseguridad.

Además, la ciberseguridad es **un** elemento crítico y el pilar fundamental para el éxito de cualquier plan digital, siendo una palanca clave para salvaguardar y asegurar el crecimiento que impulsa la transformación digital.

En los últimos años, los países se han ido adaptando con diferentes velocidades a esta realidad, implementando programas para el avance digital. Lo ha comentado el Senador antes.

En el caso de España, cuando ha articulado su propuesta para los próximos cuatro años, España Digital 2025, la ciberseguridad tiene un papel relevante como uno de sus diez pilares estratégicos. Esta agenda impulsará la transformación digital en España para relanzar el crecimiento económico, la reducción de la desigualdad, el aumento de la productividad y el aprovechamiento de todas las oportunidades.

Por este motivo, la seguridad digital es una excelente oportunidad para la creación y el desarrollo de una industria nacional de ciberseguridad. Y también, por supuesto, es una fuente de creación de empleo. Esta industria requiere profesionales especializados en diferentes disciplinas, y no solo con perfil técnico. Por este motivo, ahora o nunca hay que dar a conocer este sector y capacitar a personas para que desarrollen toda su carrera profesional, desde los inicios, en este sector, o la reorienten hacia él.

Y es que el proceso de transformación digital abre enormes oportunidades al desarrollo socioeconómico. Pero, al mismo tiempo, no podemos olvidar que incorpora amenazas y riegos relacionados con la seguridad digital en una doble vertiente: por un lado, el daño causado por los incidentes cibernéticos en sí mismos y, por otro, el socavamiento de la confianza en el uso de las tecnologías digitales, que puede afectar a su adopción por parte de los actores económicos y la ciudadanía. Estos dos factores, protección frente a las amenazas y generación de confianza, tienen un impacto directo en el desarrollo económico de los países.

Con el aumento de la extensión de la superficie de riesgo cibernético, la ciberdelincuencia sigue creciendo y tenemos que saber que cada vez está más profesionalizada. Podemos ver diariamente ataques de todo tipo. La Presidenta ha comentado al principio el ataque a uno de los bancos más grandes y populares de Chile. También una red de hospitales en Estados Unidos fue atacada y parece ser uno de los hackeos más grandes en la historia del país a un sistema médico. Y en el Hospital Universitario de Düsseldorf se investiga el que podría ser el primer homicidio de la historia causado por un ciberataque.

Estos ejemplos ponen de manifiesto que la colaboración es la vía para vencer. Debemos trabajar unidos para frenar este tipo de incidentes, porque una característica de la ciberseguridad es su carácter trasnacional, y en un mundo virtual, sin fronteras físicas nacionales, los riesgos y amenazas suelen estar, en muchos casos, lejos del lugar que recibe el ataque. En ese entorno cobra cada día más importancia la cooperación internacional para la prevención de las amenazas y la persecución de los cibercriminales, porque unidos somos más fuertes.

Para finalizar, quiero indicarles que los organismos públicos que en España se dedican a la ciberseguridad -por supuesto, a nivel general-, tienen en Incibe un socio comprometido para trabajar juntos y conseguir un mundo digital más ciberseguro.

Mucho éxito en el Mes de la Ciberseguridad que se inaugura hoy.

Muchas gracias.

El señor GUZMÁN (Secretario General).– A continuación, hará uso de la palabra en la Sala del Senado el Honorable Senador señor Kenneth Pugh.

El señor PUGH.– Muchas gracias.

Señora Presidenta, Honorable Sala, distinguidos invitados:

¿Es posible construir entre todos una nueva República Digital en Chile, donde el reconocimiento a la dignidad de las personas se exprese diariamente con mejores servicios digitales del Estado y de las empresas, poniendo a los ciudadanos en el centro de sus decisiones?

Esa es la pregunta que me he hecho todos los días desde que la pandemia congeló nuestra economía física. Pero también desencadenó un proceso de transformación cultural nunca antes visto en la historia de la humanidad. Nos forzó a conectarnos digitalmente a la distancia, a seguir trabajando y estudiando, e incluso a llevar nuestra vida social de forma remota y conectados a internet.

Esto abrió nuestras mentes, pero a la vez desnudó el sistema y separó a los conectados digitalmente de los desconectados. Esta es la primera brecha que hoy debemos abordar, con un nuevo y vigoroso plan de urbanización digital, de alfabetización; luego, de educación digital, y finalmente, de inclusión digital.

Pero todo eso no es posible si no avanzamos primero con ciberseguridad, para garantizar la confianza digital, tan necesaria para entendernos entre semejantes. Se requiere un anexo digital al contrato social que, desde Rousseau, nos ha permitido generar un Estado de derecho, garantizado en nuestra Constitución.

Es necesario, entonces, fundar la nueva República Digital con la mejor plataforma de interoperabilidad que esté disponible, para permitir la certeza jurídica de los actos digitales del Estado, de las personas (naturales y jurídicas) e incluso de los dispositivos conectados a la red.

Pero también debemos reconocer un nuevo derecho constitucional: el derecho de los ciudadanos a relacionarse digitalmente con el Estado, para hacer un balance con la ley Nº 21.180, de Transformación Digital del Estado.

¡Basta de trámites presenciales y largas filas! ¡Basta de tramitar en papel voluminosos expedientes para permisos! ¡Basta ya de esperar de forma larguísima e incierta que algo ocurra!

Necesitamos poner al Estado al servicio del ciudadano y comprender que en la nueva era digital, con trazabilidad e integridad de la información en base a sistemas de *ledger* distribuidos, los computadores no deben ser usados como máquinas de escribir.

¡Basta de entregar tantas veces los mismos datos personales al Estado, sin saber cómo los custodia!

Tenemos que ejercer el derecho constitucional de la reforma del 2018, que protege los datos personales, pilar esencial de la ciberseguridad. Y se requiere que avancemos más rápido en la iniciativa de ley que crea la Agencia Nacional de Protección de Datos Personales y también en la que ya se ha citado, referida a la nueva ley de delitos informáticos, que se tramita en la Cámara Baja. Por lo mismo, saludo hoy a las Diputadas y a los Diputados que nos acompañan, a los Presidentes de Comisiones y al Grupo Bicameral de Ciberseguridad.

Estamos perdiendo por goleada contra todos los cibercriminales y agentes estatales que vienen a entrenarse a nuestro país con sus técnicas de engaño y decepción.

Debemos prepararnos, actualizar anualmente nuestros conocimientos y entrenarnos para enfrentarlos. Y todos debemos hacerlo, porque este no es un tema de las grandes empresas, del Gobierno o de los militares: es responsabilidad de cada ciudadano que vive en este país, dado que en ciberseguridad todos son importantes. Esta cadena se rompe solo por el eslabón más débil.

Crear conciencia a temprana edad mediante hábitos de "higiene digital" y desarrollar conocimientos avanzados son responsabilidades de cada uno de nosotros, porque somos la primera y última línea de defensa de nuestro hogar, trabajo y país. Debemos comprender que, incluso, la manipulación digital de las redes, a través de *fake news,* y de las elecciones puede destruir nuestra democracia.

Ese fue el espíritu que nos animó a los Senadores de la Comisión de Defensa el 5 de mayo del 2018 a presentar la moción para crear un mes dedicado a la ciberseguridad. La promoción de esos conocimientos y habilidades es esencial. Agradezco a los Senadores Araya, Bianchi, Elizalde y Víctor Pérez (ahora Ministro del Interior), por haber apoyado esa moción, y, en especial, al Senador Felipe Harboe, por acompañarme a impulsar esta cruzada nacional en la que estamos comprometidos.

Somos el primer país de Latinoamérica en adoptar esta práctica, que viene del hemisferio norte, para realizar actividades de ciberseguridad en octubre.

El año 2018 vimos nacer una notable organización: la Alianza Chilena de Ciberseguridad. Y me siento honrado de que hoy nos acompañe su Presidenta, doña Yerka Yukich.

En ese mismo año se dio vida a Incíber, con un destacado grupo de académicos de la Región de Valparaíso, compuesto por la doctora Romina Torres, por la señora Lidia Herrera y por el doctor Xavier Bonaire, profesionales de la Universidad Andrés Bello, de Inacap y de la Universidad Federico Santa María, respectivamente, por el prefecto Hugo Miranda, de la PDI y Lidia Fuentes, del Senado. Con mucho esfuerzo, ellos levantaron el primer seminario internacional el 1 de octubre, sin saber que, por coincidencia, la ley que declara octubre Mes de la Ciberseguridad sería publicada ese mismo día. Fue una feliz coincidencia para el nacimiento del Instituto Nacional de Ciberseguridad (Incíber), que tendrá su sede en la capital legislativa de Chile: Valparaíso, y que, junto con mi equipo legislativo, conformado por Mario Troncoso, Diego Pérez, Michael Heavey y Pascal de Smet, estamos llevando adelante.

Son las personas las que producen los cambios; la generosidad de ellas produce los grandes cambios.

Por eso, al iniciar el mes de octubre, debo recordar que hace quinientos años navegantes españoles y portugueses se encontraron con navegantes de nuestros pueblos originarios kawésqar y yaganes en el estrecho de Magallanes. Así fue descubierto Chile: por mar, abriendo nuevas rutas de conocimiento y comercio.

Por eso, agradezco a Rosa Díaz, Directora General del Incibe, quien nos está apoyando para sacar adelante nuestras iniciativas. Este es un centro de referencia europeo.

También expondrá, a continuación de mis palabras, "Chema" Alonso, quien es un gran evangelizador en estos temas.

Este es el espíritu de octubre, "Mes Nacional de la Ciberseguridad": actualizar nuestros conocimientos, entrenarnos, competir por encontrar a los mejores talentos y verificar que vamos avanzando como corresponde.

Quiero agradecer al Senador Alejandro García-Huidobro por habernos permitido plantear esta propuesta en el Parlamento Andino, la que fue aceptada. Así, a contar del próximo año, se declarará octubre "Mes Nacional Andino de la Ciberseguridad".

De la OEA, a Belisario Contreras y Moisés Benamor, por los laboratorios de ciberseguridad que llevamos adelante y también por los centros de innovación en ciberseguridad.

Pido un minuto más, señora Presidenta.

La señora MUÑOZ (Presidenta).– Lo tiene, señor Senador.

El señor PUGH.– Muchas gracias.

A Carlos Landeros y a Katherine Canales, del CSIRT de Gobierno, por los grandes logros alcanzados el último año y por incorporar plenamente a la mujer en las actividades de ciberseguridad. Tenemos una brecha de género

en ciberseguridad tremenda: apenas un 10 por ciento son mujeres en este ámbito.

Y, finalmente, quiero agradecer al Comité Interministerial de Ciberseguridad, compuesto por ocho Ministerios y presidido por el Subsecretario del Interior, Juan Francisco Galli, junto con la Subsecretaria de Telecomunicaciones, Pamela Gidi. En esa organización una mujer, Catherine Narváez, es la jefa de proyecto.

La ciberseguridad no es de Izquierda, de Centro o de Derecha; es un tema de Estado. Por eso, todos juntos podemos construir esta nueva República Digital, por la razón o la fuerza de los datos, pero avanzando siempre primero en ciberseguridad.

Muchas gracias, señora Presidenta.

He dicho.

El señor GUZMÁN (Secretario General).– Gracias.

A continuación, hará uso de la palabra el señor José María Alonso, profesional español y CDCO de Telefónica, quien presentará el tema "Ciberseguridad y Sociedad".

El señor ALONSO (CDCO de Telefónica).– Estimadas Senadoras, estimados Senadores; señoras y señores, amigos y amigas; y, por supuesto: hola, *hackers*.

Permitidme que os llame a todos vosotros "*hackers*", pues no se me ocurre otra forma de mostrar más respeto y admiración que utilizar ese término.

Durante años he usado el término "*hacker*" para dirigirme a la gente que venía a mis charlas, a mis conferencias, a los eventos, etcétera, pero también para nombrar a las personas que han hecho un avance significativo en nuestro mundo por medio -muchas veces, pero ni siempre ni necesariamente- de la tecnología.

Como muchos conocen, he peleado por alejar lo que para nosotros significa ser un *hacker* de lo que algunas veces se utiliza en los medios de comunicación y películas de cine, donde el *hacker* es alguien que se confunde con un criminal o un activista ideológico, y que, para más inri, suele ser pintado con algún trastorno mental y/o emocional.

Algunas veces me enfada y otras me da tristeza, pero yo no me canso. Y eso ha llevado a que lo tenga que explicar infinidad de veces.

Lo he hecho incluso ante la Real Academia de la Lengua Española, a la que agradezco que haya incluido como acepción una más cercana a nuestro uso, sentir y definición del término, reafirmándose como una institución adaptada a los nuevos tiempos, como ya lo demostró al extender a toda Latinoamérica los órganos de cuidado y evolución de nuestra lengua.

Es verdad que la acepción añadida no recoge todos los matices de lo que para nosotros es un *hacker*, pero sí queda ese uso positivo del nombre que se valora entre los que conocen a estas personas.

Permitidme que os lea la segunda acepción del término "jáquer": "Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.".

Esta acepción del término se acerca más a cómo nosotros lo sentimos y recoge ese espíritu de buscar fallos y encontrar soluciones que tanto definen las investigaciones de los *hackers*, que, como muchas veces he dicho, son más cercanas al trabajo de investigación que se realiza desde hace varios siglos en las universidades de todo el mundo que a una actividad sumergida e ilegal, como se pinta en las películas.

Aunque he de decir que lo que buscan los *hackers* no siempre es posible catalogarlo como fallos. Un *hacker* busca *bugs*, que es como se llaman los fallos informáticos, para encontrar soluciones. Pero también busca soluciones a carencias, a limitaciones, a malos funcionamientos, o interviene simplemente cuando hay una falta de capacidad para solucionar correctamente un problema.

Para nosotros, un *hacker* es una persona que busca en los límites de la tecnología, de los procesos, del arte, de la música, de las cosas en

general, para llevar las barreras que tenemos impuestas un poco más allá, un poco más lejos; para poder hacer más cosas o simplemente hacerlas mejor o distintas; o para hacer cosas nuevas de lo que era el propósito inicial de lo que se estaba hackeando.

Han sido, por tanto, siempre los primeros en alertarnos de los riesgos y peligros de algo existente, y pioneros en traernos cosas nuevas.

Por supuesto, ese espíritu *hacker* se aplica también a los que buscan mejorar la ley, la política, y se preocupan por la evolución de un país.

Esas personas dedican toda su energía a preguntarse el porqué de las cosas. Se plantean preguntas: "¿Y si hacemos esto de manera distinta?" o -mi favorita- "¿Qué puede pasar?". Lo hacen de forma natural en su forma de vivir, de trabajar, de disfrutar su tiempo.

Permitidme que os cuente una anécdota.

Mi hija pequeña, a la que no sé si le va a gustar la tecnología o no, con su propia visión del mundo descubrió un fallo en el álgebra matemática que yo no conocía, historia que he contado muchas veces.

Tenía solo seis años.

Todo empezó con una limitación que yo impuse en su vida: "No puedes ir a jugar hasta que termines los deberes de matemáticas". Refunfuñó; intentó negociar el número de operaciones que quería hacer; volvió a negociar para conseguir una rebaja, y al final accedimos a un acuerdo: de todas las operaciones matemáticas, debía hacer solo veinte, ni una más ni una menos.

Eso sí, por el camino intentó mediatizar la elección de las operaciones usando sus técnicas de ingeniería social con frases como: "¿Cuánto es 1+1, papaete?"; o "¿Y 2+2? Venga, que esa seguro que no me la sé".

Al final, le puse una lista de operaciones matemáticas formadas por sumas y restas. Y se afanó en la tarea. En menos de cinco minutos las tenía resueltas, y correctamente todas, tras mi revisión. Así que permití que se fuera a jugar y seguí con mis tareas.

Después algo levantó una alerta en mi cabeza, ya que mi memoria visual me decía que algo no encajaba. Había un fallo en la Matrix y tenía que localizarlo.

Repasé las operaciones y, sí, todas estaban correctas. Pero me di cuenta de que, por arte de magia, mi hija había convertido todas las restas, que son operaciones todas ellas complejas y aburridas, porque implican ir hacia atrás, en sumas, mucho más alegres, positivas y siempre mirando hacia delante, más cercanas a su carácter. Lo único que tuvo que hacer es poner un palito vertical sobre el signo de la resta exactamente igual que los míos, para que yo no notara la diferencia, y convertirlas en crucecitas.

Como ya he dicho, tradicionalmente hemos visto a los grandes *hackers* estar cerca del mundo de la tecnología, por todas las posibilidades que esta ofrece como herramienta para construir cosas.

Vinieron de ser autodidactas en casa, extendiendo lo aprendido en libros y en las clases que recibían, para pasar luego a ser grandes investigadores, en la universidad, en centros de innovación, y para estar hoy en las empresas que crean la tecnología que vertebran nuestros países.

Es en este último sitio, en la empresa, donde la tecnología que una compañía tiene puede marcar la diferencia entre ser una organización que crece en el mercado, que se expande y que tiene un futuro prometedor, o que, por el contrario, está abocada a ser un carruaje tirado por caballos en un mundo de coches autónomos eléctricos gestionados por inteligencias artificiales.

Y eso también les puede pasar a las instituciones públicas y a los gobiernos.

Muchos de estos grandes *hackers* han cambiado los límites, no solo de la tecnología, sino del mundo y la sociedad en la que vivimos. Han cambiado nuestra forma de vida hasta puntos insospechados.

No han pasado tantos años desde que Steve Wozniak, uno de los grandes *hackers* del siglo XX, creó aquel primer ordenador personal Apple. Y lo hizo en su tiempo libre, en su casa.

Y aunque hablamos de ello con distancia, la verdad es que ha sido solo hace bastante poco en la historia de la humanidad.

Muchos más lejanos son los ciento cuarenta años que han pasado desde el nacimiento de la Compañía de Teléfonos de Chile, hoy Movistar Chile, sin duda pionera en el mundo de las redes sociales.

Entonces, cuando se creó el primer ordenador personal, se buscaba explorar un mundo de posibilidades que aún se veía solo en las películas de ciencia ficción.

Y, sin embargo, hoy muchos tendréis un teléfono inteligente de Apple o de Google en el bolsillo, con tecnología y aplicaciones que usáis para la vida constantemente. Y para cosas de todo tipo, para hacer tareas básicas del día a día, sobre unos teléfonos que vienen evolucionados de aquellos primeros computadores soñados por los *hackers*. Cosas como quedar a cenar, organizar un cumpleaños, saber si has descansado bien o no, o si alguien ha encontrado la camiseta de tu hija que se ha dejado en el gimnasio. Algunas, supliéndonos a nosotros mismos de forma clara, como cuando lo usamos para encontrar la ruta más rápida para ir al trabajo, a ese al que vas cada día, al que sabes de sobra cómo llegar; pero aun así, les pides a los sistemas de *big data* e inteligencia artificial que te digan cómo debes ir.

Utilizamos la tecnología para encontrar pareja; para controlarnos la salud; para hacer deporte; para controlar la calefacción de casa; para saber dónde está tu coche; o para poder estar en contacto con la administración pública, el colegio de tus hijos, o tu universidad. Todo, desde donde estemos y a través de la tecnología y las redes de telecomunicación que vertebran nuestros países.

Imagínense por un momento esta época de pandemia que nos ha tocado vivir, en que hasta los abuelos hacen videoconferencias con los nietos, sin tecnología.

Los *hackers*, convertidos en investigadores, emprendedores y profesionales, han ayudado a cambiar la forma en que vivimos; han cambiado los ejes de la vida; han hecho que muchos de los límites que tenía nuestra forma de vivir hace cuarenta años hayan desaparecido, haciéndose mucho más difusos, llevándonos por caminos desconocidos en nuestra forma de sentir, de vivir, de trabajar y de disfrutar nuestro tiempo.

Y aquí estamos, con nuevos límites, pues los límites nunca desaparecen totalmente, solo los empujamos por caminos que nos llevan a nuevos paradigmas, con nuevos retos a los que enfrentarnos, con nuevas necesidades para las sociedades, para las personas y para la humanidad en su conjunto.

Y necesitamos una nueva generación de *hackers* que lleven nuestros nuevos límites hacia nuevos espacios.

Y, por supuesto, la tecnología es una vez más pieza importante en ese tablero.

No podemos, ni debemos, ni queremos dejar que el uso de este regalo en forma de servicios tecnológicos que nos han dado los *hackers*, investigadores y emprendedores se aplique de forma negativa.

Tenemos que reforzar la idea de que tanto las empresas, como los gobiernos, como la tecnología tienen la obligación de hacer que la vida de las personas sea mejor gracias a ellos, y no peor.

Y debemos hacerlo **de una forma humanista**, teniendo presente que cada ser humano debe ser tenido en cuenta de una manera directa y consciente en la creación de un nuevo avance social, empresarial y tecnológico.

Un gobierno debe preservar y expandir los derechos y libertades de las personas, así como las empresas deben ser motores de generación de riqueza y bienestar para las sociedades donde operan.

Al mismo tiempo, los gobiernos deben ser

capaces de proteger a la sociedad contra los que la quieren dañar, en ocasiones, a través de la tecnología.

No son pocas las veces que las empresas, las instituciones de un país o los propios ciudadanos son atacados por cibercriminales -por favor, nunca los llaméis "*hackers",* que para ellos es suficiente un correo de *phishing* para hacer su mal; *"hacker*" es una palabra demasiado grande para ellos-, cibercriminales que secuestran sistemas informáticos y datos por medio de técnicas de *ransomware*; que amenazan la disponibilidad de plataformas por medio de ataques de denegación de servicio; que roban la información para utilizarla en nuestra contra o en su provecho, o que realizan estafas a gran escala en la sociedad.

Igual que los gobiernos se han encargado de la protección de las personas, las instituciones y las empresas en el mundo físico, es necesario que lo hagan en el mundo digital, poniendo un marco jurídico adecuado a los tiempos en que vivimos, en esta **era digital**, donde tenemos tecnología maravillosa, pero donde debemos hacer que primen los valores de las personas, eso que nos hace humanos.

Para ello, necesitamos que los gobiernos entiendan bien el mundo en el que estamos. Y esto no va a pasar relegando a los *hackers*, a los creadores de tecnología a un segundo plano.

Muchas veces me han preguntado en entrevistas cómo debe afrontar una empresa la transformación digital, ese proceso que obliga a un negocio a ser capaz de vivir en este nuevo mundo digital y, gracias a él, ser competitivo. Y siempre he respondido con una afirmación sencilla: empieza dando poder en el directorio, en el equipo ejecutivo y la administración de la empresa a gente que entienda este mundo, ¡pero que lo entienda de verdad!

No sé cuántos de ustedes, Senadores y Senadoras, saben lo que es un *token* OAuth, un segundo factor de autenticación o la diferencia entre un sistema experto y una *GAN*. Pero, créanme, los utilizan todos los días. Y si no entienden sus detalles, va a ser difícil marcar el camino adecuado para el mundo en el que vivimos.

Sí, seguro que pueden preguntar a muchos de los grandes expertos ahora que yo les he hecho la pregunta, y encontrar las respuestas. Pero si no conocen los detalles de un sistema PAS en *cloud* o las implicaciones de la aplicación de protocolo https 3.0 en las redes de comunicaciones en su país, va a ser difícil que sepan hacer las preguntas adecuadas.

Para eso es necesario que los que entienden la tecnología, los *hackers* y los creadores de este mundo digital, sean parte de los que toman las decisiones y que no actúen solo como personajes secundarios.

Seguro que entre todos ustedes hay amantes y conocedores de la tecnología. Pero quiero aprovechar la oportunidad para resaltar que regular sin saber cómo funciona, por ejemplo, una inteligencia cognitiva de esas de las que ya hay cientos de miles en los hogares de todo el mundo, también en Chile, y poner sobre la mesa una sola de las centenares de tecnologías que nos rodean día a día, es como navegar en un océano sin mapa.

Pido perdón por haber usado ejemplos aleatorios sobre tecnología, pero quería ser explícito que para entender cómo de importantes son y qué consecuencias pueden tener en la sociedad, hay que conocerlas bien.

Esos avances tecnológicos se meten en nuestra vida.

Y como ejemplo de su importancia solo hay que analizar cómo impactó en nuestro tiempo el escándalo de Cambridge Analytica. Esta era una empresa que utilizaba los datos de los ciudadanos de un país para hacer propaganda dirigida en campañas democráticas, haciendo uso de técnicas de *big data* para generar *insights* de cada ciudadano y *fake news* dirigidas contra cada individuo para modificar la intención de voto.

En su web, la empresa decía que tenía entre

dos mil y tres mil datos de cada uno de los 230 millones de ciudadanos de Estados Unidos; y lo mismo respecto de cada país en donde operó. Dos o tres mil datos de cada ciudadano en una sola plataforma permiten realizar un perfilado ajustado de la situación personal de cada uno de ellos para saber cuál es la propaganda con noticias falsas más acertada, que va a mover su posición ideológica un 1 por ciento hacia el lado deseado. Solo un 1 por ciento de 230 millones de personas es un cambio enorme en un país que puede decantar una elección.

La realidad es que aquellos que desean cambiar un comportamiento de forma masiva en un país lo saben. Estos se van a comportar como anunciantes, y basta con que se vayan a las grandes plataformas de las redes sociales, seleccionen una muestra de usuarios objetivos y les digan a estas plataformas: "¡Eh!, muéstrales mi vídeo, mi noticia o mi *fake news* a todos los usuarios que sean similares a este".

Esto ha llevado a que los países en los que la sociedad se educa por los memes de WhatsApp, por el contenido en las redes sociales como Facebook o Twitter acaben yendo a la radicalización. Nos ha pasado en Europa y pasa aquí, en América. Países que se dividen y que radicalizan sus posiciones porque todos sienten que tienen razón. Las redes sociales se encargan de rodear a cada persona de una realidad llena de razones y verdades para reafirmarle en el color de su posición.

Decía el expresidente Barak Obama en su última visita a Madrid que antes dos políticos discutían sobre si algo que sucedía era bueno o malo, pero que hoy en día dos políticos discuten sobre si algo está sucediendo o no.

Y es que estas plataformas, que tienen tantos datos de los ciudadanos de un país, y lo más importante, que tienen esos datos en sistemas accionables, es decir, en los que se pueden automatizar acciones por medio del conocimiento que se extrae de esos datos, deben tener una responsabilidad extra. Porque la tecnología debe hacer que la vida de las personas sea mejor. Un avance tecnológico no puede significar que las personas, todas ellas o una sola, no sea tomada en cuenta y sufra por esa tecnología una disminución de sus derechos, libertades o capacidad para vivir su vida.

Un sistema informático de cualquier empresa que guarda los datos de personas debe ser garante de su privacidad. Porque, si no lo hace, todos aquellos que se vean afectados por una posible fuga de información o una brecha de seguridad pueden sufrir directamente en el devenir de su vida. Ello puede hacer que su vida sea mucho peor solo por eso.

Ya hemos visto en el pasado cómo una fuga de datos de una empresa ha llegado a truncar la vida de seres humanos, perdiendo amigos, trabajo, siendo infelices, sufriendo extorsiones o llegando a quitarse la vida.

Pero la seguridad y la privacidad de la información de las personas no es el único punto en el que la tecnología nos afecta.

Tenemos una intensificación de tecnología tal que para las personas es difícil llegar a entender cómo esta le afecta en su día a día y si realmente lo que está viviendo es consecuencia de algo que proviene de un mal uso de la tecnología.

Hoy en día sufrimos una catalogación constante de todos nuestros actos y de nosotros mismos. Cada cosa que hacemos cerca de la tecnología sirve para clasificarnos.

Es como si fuéramos a tomar un café todos los días a un bar y el camarero, que ya sabe mucho de nosotros, hiciera constantemente una ficha de nuestras conversaciones, de la ropa que llevamos, de lo que leemos, de lo que comentamos, de con quién nos juntamos, y todos esos datos fueran analizados y compartidos por todo el mundo.

De una forma similar los programas que se utilizan en plataformas de *big data* mediante algoritmos de *machine learning* están generando *insights* o conocimiento sobre las personas en función de lo que hacen, leen, de cómo lo hacen, de cuánto tiempo pasan escribiendo,

de cuánto tiempo pasan en la web o cuál ha sido la actividad completa en cualquier sistema informático.

Este conocimiento se utiliza para hacer que la publicidad sea más dirigida, que la recomendación de la película que te hacen sea más acertada, que la propuesta de viaje que te ofrecen sea más efectiva y que, por ende, los negocios generen riqueza más rápidamente para las empresas.

El negocio consiste en conocer bien a las personas y etiquetarlas a través de la tecnología para poder dar servicios más acertados e influir en su comportamiento, influir en las acciones futuras de esas personas, hacer que compren algo, que piensen algo, que usen algo.

No, no me toméis mal. Estoy lejos de tener una visión negativa del uso de los *insights,* y me gusta ir al bar al que mejor me conocen y estar con las personas que más saben de mí: mis amigos, mi familia, mis compañeros. Ellos saben mucho de mí, pero utilizan todos esos datos que tienen para mi bien y hacen que mi vida sea mejor. Saben cómo hacerme reír; cómo animarme cuando estoy triste; cuándo estoy alegre, o qué plan proponerme para un fin de semana. Utilizan sus conocimientos sobre mí para hacer mi vida mejor. Y así debería hacer también la tecnología y las empresas que utilizan estos avances tecnológicos.

Deben ser humanistas y tener como objetivo principal mejorar la vida de las personas, de todas y cada una de ellas, teniendo presente, en todo momento, qué riesgos existen.

Ver un conjunto de vídeos en una plataforma *online*, leer unos artículos en un blog o el contacto con determinados usuarios en redes sociales pueden llevar a que se generen *insights* de cualquier tipo asociados a cada uno de nosotros.

Muchas veces ni siquiera sabemos cuál es el universo de esas etiquetas que nos han puesto. Puede que sean desde el tipo de "le gustan los dibujos animados" hasta, por ejemplo, "tiene una ideología de un determinado partido político".

Son etiquetas que a veces nos pueden acompañar, sin saberlo, durante toda la vida. Y pueden ser correctas o no. Pero es la magia de los algoritmos basados en datos.

Puede que fallen en la catalogación de un porcentaje de las personas a las que se les ha asignado una etiqueta. Pero en total incrementan el grado de acierto medio. Tal vez solo fallen un 7 por ciento o puede que las personas cambien su parecer, o sus gustos, o sus ideas. Pero no tenemos el control total de esas etiquetas que se nos generan.

Y esos *insights* podrían ser utilizados de manera indiscriminada para afectar a las personas más vulnerables al explotar en las debilidades que tengan.

Creedme, si una etiqueta de "jugador de juegos de azar" se asocia a una persona con adicción al juego, lo último de lo que se va a preocupar la tecnología es de si esa persona se arruina o no por una enfermedad. Su algoritmo está configurado justo para lo contrario, para subir lo que se denomina como "*engagement"*.

Creedme, un indicador de éxito clave en cualquier sistema informático que "pretende" ser gratuito y que pagas con tu tiempo y tus datos es el *engagement*. Estos algoritmos de *engagement*, basados en inteligencia artificial, no han superado a la inteligencia humana aún, pero sí han superado a la debilidad humana hace tiempo.

Dijo Sean Parker, el que fuera presidente de una de las empresas más importantes de redes sociales en la parte de monetización, que lo que hacían era explotar las debilidades humanas, los miedos, las adicciones y las necesidades que se generan en la propia red. Pueden hacer igual de mal a una persona estas adicciones y estos problemas que se generan en la red que bien a una empresa, **si no se pone a las personas en el centro para hacer que la tecnología sea humanista.**

Es decir, repito, que tengan en cuenta el bienestar de todos los que la utilizan y no que

generen ansiedad, que den herramientas a acosadores, a abusones, o que sean un acelerador en la proliferación de mensajes de odio o desinformación.

La suma de todos estos ingredientes -la privacidad de los datos, la comercialización de estos, la generación de *insights* y el uso de redes sociales para la proliferación de noticias falsas- ha hecho que no sepamos si nuestro sistema de elección personal más importante, el voto en democracia, se haya visto afectado.

La tecnología se ha usado muchas veces para pintarnos un mundo horrendo, cuando los grandes indicadores de bienestar no hacen más que crecer, a pesar de las torpezas y errores que como especie seguimos cometiendo.

Hoy no sabemos si el mundo en el que vivimos es en el que deberíamos haber vivido. Podría haber sido otro si no se hubieran utilizado sistemas automáticos masivos de recolección de datos, generación de *insights* y masificación de la difusión de noticias falsas en las grandes elecciones.

No estamos seguros de que si los sistemas creados con tecnología hubieran tenido en cuenta que nuestros datos pueden afectarnos de una manera tan importante y se hubieran protegido de otra forma no viviríamos otra realidad de este mundo. No lo sabemos.

Sí que sabemos que se han utilizado estas plataformas tecnológicas de manipulación que he contado antes. Pero no sabemos si es culpa suya o culpa nuestra como personas, como países y como sociedad dejar que funcionen en nosotros las noticias falsas de una forma tan permeable; dejar que nuestras fuentes de información sean medios mantenidos por el poder del *click through* y el pago por visualización de los anuncios, donde lo más importante ha pasado a ser el número de visitas de una noticia *online* y no la calidad de la información que ofrecen estos medios.

El volumen de noticias tiene que ser alto, con estructuras de *clickbait* y con foco total en *SEO* (*search engine optimization)* y difusión rápida por redes sociales para conseguir visitas, muchas visitas, mucho tráfico, para conseguir que caiga el maná de los anunciantes *online* con el premio de haber conseguido mucha difusión, no mucha calidad de la información.

También se ven premiados con éxito y dinero aplicaciones y plataformas de entretenimiento que maximizan los parámetros, como el citado *engagement*, el parámetro que mide el tiempo que una persona pasa en la plataforma.

Los juegos *online* no llevan tacómetro, ni los servicios sociales que explotan las debilidades humanas para maximizar el tiempo de conexión.

El tacómetro, como sabéis, es ese dispositivo que hace que los conductores profesionales descansen cuando llevan demasiado tiempo conduciendo.

Ninguna plataforma digital, sin embargo, le dice a una persona que lleva jugando treinta y siete horas seguidas que ello puede afectarle en su vida personal o generar trastornos.

Y, por supuesto, con algoritmos de *machine learning* se puede saber que una persona empieza a verse afectada por pérdida de *engagement* para meterle una nueva dosis de dopamina, con un nuevo premio o una elaborada estrategia de gamificación, una de las más famosas técnicas de *growth hacking*.

En la famosa película de ciencia ficción llamada *Ready player one*, dirigida por Steven Spielberg -atención, *spoiler*- al final el protagonista decide apagar el mundo virtual un día a la semana para que la gente vuelva a vivir desconectada de la tecnología y disfrutar de seres humanos.

No. No me malinterpretéis, tampoco es esto. No estoy diciendo que haya que apagar internet los miércoles de cada semana. Tal vez acabaremos teniendo que controlar de alguna forma este tipo de sistemas para proteger a los usuarios y que los algoritmos de *engagement* no generen adicciones que afecten negativamente a las personas.

Escribe el antropólogo Yuval Noah Harari en su novela *Homo Deus* que el ser humano en el siglo XXI debe plantearse nuevos retos, tener nuevas miras en el horizonte; que la agenda de la humanidad debe aspirar a dotar a las personas de una esperanza de vida más larga, de la capacidad de llevar una vida mucho más plena gracias a entregar nuevas habilidades a los seres humanos; y, sobre todo, a que cada persona sea feliz en su existencia; todas y cada una de las personas, sin olvidarnos de nadie.

No sé si la humanidad alcanzará esos objetivos, ni si lo hará en este siglo XXI, que nos ha tocado vivir; ni tan siquiera sé si nos pondremos de acuerdo para perseguirlos. Pero sí que tengo claro que si lo conseguimos o si nos acercamos un poco a ellos, será con y gracias a la tecnología, no dejándola a un lado.

Será, por tanto, necesario que movamos muchos de los límites que tenemos y que hagamos que la tecnología crezca segura, robusta y por el camino humanista.

Debemos conseguir que todos -personas, empresas, instituciones, gobiernos y grandes plataformas tecnológicas- estemos alineados en los mismos incentivos: hacer que la vida de las personas sea mejor.

Ustedes, como responsables de dirigir el rumbo de este país, forman parte fundamental de hacia dónde va a ir la felicidad y la plenitud de la vida de sus ciudadanos. Y tendrán que establecer las reglas del juego para todos los implicados en esta ecuación.

No va a ser fácil; no se crean.

Las cinco empresas tecnológicas más grandes del mundo, que seguro que todos conocen y utilizan, tienen un valor cada una de ellas del orden de tres veces el producto interno bruto de Chile al año. No es sencillo marcar reglas de juego a dragones cuando son ellos los que han creado este mundo mágico que nos trae la tecnología.

Dinamarca, en Europa, ha comenzado a pensar en las grandes empresas tecnológicas como nuevas superpotencias, y ha nombrado un embajador para mantener relaciones con ellas. Y no se olviden de que son empresas con ánimo de lucro dirigidas por personas que no han sido elegidas por el pueblo.

No es que esté mal aquello, ya que las empresas son motores de riqueza y su incentivo debe ser generar dinero.

Es responsabilidad de los gobiernos, elegidos por las personas, poner el camino y la forma en que debe ser generada esa riqueza para que prime el bienestar de las personas. Un país con grandes empresas generando riqueza, que ponga el bienestar de sus ciudadanos en el centro: ¡ese debe ser el objetivo!

Senadoras, Senadores, no piensen jamás en los *hackers* como el problema que deben solucionar. Los problemas de ciberseguridad, las amenazas que vienen por el mundo cibernético y los retos para el bienestar de las sociedades en la era digital son enormes. Se trata de defender nuestros valores y de hacer que la vida de las personas sea mejor, así como de crear las herramientas adecuadas para que el país pueda progresar de forma sana, sacando lo mejor de lo que nos dejaron los primeros *hackers*: la tecnología.

¡Muchas gracias!

El señor GUZMÁN (Secretario General).– Le agradecemos al señor José María Alonso por su presentación.

A continuación, se les otorgará la palabra a quienes están participando en esta sesión especial tanto en la Sala como de manera remota o telemática, para hacer consultas o para efectuar alguna reflexión con relación a la temática planteada.

La señora MUÑOZ (Presidenta).– Ofrezco la palabra.

Ofrezco la palabra a quien quiera intervenir en esta sesión especial.

Tiene la palabra el Senador señor Harboe.

El señor HARBOE.– Señora Presidenta, en primer lugar, quiero agradecer las intervenciones de Rosa Díaz, Directora General del Instituto Nacional de Ciberseguridad de España, y

del "Chema" Alonso, porque ambas son muy relevantes.

Creo que la visión que nos ha dado Rosa Díaz acerca de la importancia de la institucionalidad pública y de la ciberseguridad como el elemento condicionante del desarrollo no solo de la economía, sino también de los derechos de las personas es fundamental, al igual que la orientación que nos entregó el "Chema" en torno a no cometer el error de intentar establecer regulaciones para limitar la participación de actividades ilícitas, sino más bien a crear una regulación que posibilite asegurar que el desarrollo tecnológico sirva para mejorar la calidad de vida de la gente.

Sobre el particular, a modo de complemento solo quiero señalar que hoy por hoy nuestras democracias no están ajenas también a los ataques de la cibercriminalidad.

Los últimos procesos electorales en que ha habido participación activa o mal uso de los datos personales con el objetivo de condicionar las decisiones ciudadanas son elementos relevantes que si bien no se hallan directamente relacionados con la ciberseguridad, tienen que ver con el principio de seguridad que debe inspirar todo lo vinculado con la protección de datos personales.

Lo ocurrido en las últimas elecciones norteamericanas, lo sucedido en Brasil necesariamente nos demanda como legisladores un esfuerzo mayor para establecer ciertas regulaciones que, manteniendo la libertad de expresión, manteniendo la posibilidad de desarrollar diferentes opiniones en la red, nos permitan disponer también de ciertos elementos de cuidado a fin de evitar que se mal utilice la información, o que lisa y llanamente se desarrolle una política orientada más bien a instalar las *fake news* o las mentiras en la red como una forma de condicionar las decisiones de los ciudadanos.

Por eso hemos impulsado además el desarrollo de un pacto ético digital mientras alcanzamos una regulación adecuada en nuestro país. Estamos trabajando con el Servicio Electoral, con los diferentes partidos políticos, con centros de estudios, con la Federación de Medios de Comunicación Social para que en los procesos electorales que realizará Chile -léase el plebiscito del próximo 25 de octubre y todo el calendario electoral que llevaremos a cabo durante el 2021- tengamos la posibilidad de lograr un compromiso de todas las instituciones que han de participar en ellos al objeto de evitar la proliferación de este tipo de noticias falsas, cuestión que constituye un elemento esencial.

Quiero destacar nuevamente la relevancia de esta materia. La ciberseguridad ya no es un problema solo de informáticos; no es un problema solo de expertos reguladores: la ciberseguridad es un elemento fundamental para el desarrollo de la economía digital.

Pensemos que anualmente Chile exporta cerca de 1.800 millones de dólares en servicios globales.

Un reciente estudio de la Facultad de Economía y Negocios de la Universidad de Chile nos señaló que si nuestro país tuviera una legislación adecuada en materia de protección de datos y de ciberseguridad y si además se diera certeza no solo a la industria sino también a los mercados internacionales, estas exportaciones podrían multiplicarse por tres. Incluso, si contáramos con un buen marco regulatorio, hoy día sería factible exportar más que la industria de la salmonicultura.

Creo que aquello igualmente es un elemento determinante para nuestro desarrollo.

El desarrollo de Chile no va a venir por una renovación del modelo exportador en materias primas. El desarrollo de Chile de verdad puede venir, con el tamaño de mercado que poseemos, por el desarrollo del conocimiento y de la industria de servicios globales. Y para ello, la ciberseguridad, es decir, darles a los usuarios la tranquilidad de que sus datos, que su información, que sus transacciones caminan por redes seguras, es un elemento extremadamente significativo.

Me parece que hoy la presencia acá de la sociedad civil, de expertos y expertas, de personas que han participado activamente en procesos de formación, resulta significativa.

Debemos considerar que solo este año Conicyt ha reconocido los estudios superiores o de posgrado en materia de ciberseguridad como un área clave para el financiamiento público.

En consecuencia, pienso que es importante además ir creando conciencia acerca de la necesidad de formar profesionales y técnicos especializados en estos temas que nos ayuden a ir mejorando la seguridad de nuestras redes y a darle a Chile la posibilidad de disponer de una relación público-privada mucho mejor.

Por último, estimo que también es un elemento condicionante para aquellos que miramos el desarrollo de los países, de las sociedades con una participación estatal relevante la existencia de un Estado moderno, ágil, eficiente e interoperable. Y para esto, evidentemente, un requisito fundamental es que los procesos informáticos e interoperables cuenten con condiciones de seguridad adecuadas para resguardar, ya no solo los datos y las transacciones, sino particularmente el funcionamiento de los servicios básicos. Tener la tranquilidad de que el sistema eléctrico; que el sistema bancario; que el sistema aeroportuario; que el sistema de transporte terrestre se hallan debidamente resguardados informáticamente es esencial para el desarrollo de nuestro país.

Así que quiero agradecer nuevamente las experiencias relatadas por nuestros invitados, las diferentes visiones expresadas. Conozco la trayectoria de ambos, y, por tanto, me parece un tremendo aporte que hayan participado hoy día en esta sesión que inaugura el Mes Nacional de la Ciberseguridad.

Reitero mis agradecimientos al Senador Kenneth Pugh por la colaboración y por todo lo que ha realizado en esta materia.

He dicho.

—Pasa a dirigir la sesión, en calidad de Presidenta accidental, la Senadora señora Rincón.

La señora RINCÓN (Presidenta accidental).– Muchas gracias, Senador Harboe.

Tiene la palabra el Senador Insulza.

El señor INSULZA.– Perdón, señora Presidenta, entiendo… *(falla de audio en transmisión telemática)*.

La señora RINCÓN (Presidenta accidental).– Se le apagó el micrófono, Senador.

El señor INSULZA.– Perdón, señora Presidenta. Entiendo que me dieron la palabra. No alcancé a escuchar.

La señora RINCÓN (Presidenta accidental).– Sí, señor Senador.

El señor INSULZA.– Muchas gracias.

Señora Presidenta, quisiera hacer una pregunta que es siempre compleja cuando se habla sobre todo de acciones ilegales, de crímenes o de delitos, en que generalmente las policías, quienes están a cargo de contrarrestar la acción ilícita, sienten que van un poco atrás, porque tienen que respetar determinadas normas. Y, probablemente, si ellas no se respetaran, sería más fácil combatir a los transgresores.

Tengo la impresión de que en el caso de la ciberseguridad nos pasa un poco lo mismo. Asistí por primera vez, cuando era Secretario General de la OEA, a las primeras reuniones masivas que se hicieron allá sobre ciberseguridad, y siempre se hablaba de cómo nos defendemos: qué hacemos cuando nos están atacando; cómo protegemos nuestros datos; cómo salvaguardamos nuestra información; cómo simplemente impedimos que haya disrupción de nuestros sistemas.

Entonces, la pregunta es si ya nos hallamos en una fase en que estamos siendo más proactivos, es decir, si somos capaces de predecir cuáles van a ser los próximos ataques que van a venir.

No sé si "Chema" nos puede ilustrar sobre eso. O sea, ¿es posible a estas alturas conocer de antemano lo que serán los ataques a nuestros sistemas, a nuestras redes de datos y a toda

nuestra estructura? ¿O todavía estamos en una fase defensiva, en que simplemente vamos conociendo los ataques a medida que se verifican?

Claro, los vamos rechazando de manera cada vez más eficaz. ¿Pero todavía no estamos en una fase en que podamos prevenir, más que curar, los daños que se producen?

Muchas gracias.

La señora RINCÓN (Presidenta accidental).– Tiene la palabra el Senador Araya.

El señor ARAYA.– Señora Presidenta, primero, quiero saludar a nuestros invitados y agradecerles la exposición que realizaron, que ha sido muy clarificadora en términos de lo que está ocurriendo hoy día en el mundo, de cómo tenemos que enfrentar los nuevos desafíos que se están originando por el mundo digital en que vivimos y respecto del cual nuestro país está haciendo tremendos esfuerzos para estar al día en materia de nuevas tecnologías, de nuevas políticas públicas sobre cómo abordar las cuestiones vinculadas con ciberseguridad.

Asimismo, deseo agradecerle también al Senador Kenneth Pugh, quien ha sido un fuerte defensor e impulsor de que el Senado se preocupe de estos temas y los pueda poner en la discusión pública, de forma tal que todos los chilenos y las chilenas entiendan la importancia de regular la ciberseguridad, de tener un sistema robusto en materia de telecomunicaciones, digital, que nos permita realizar día a día una vida normal.

En tal sentido, a mí me gustaría preguntarles a nuestros invitados, porque sin duda a nosotros, que nos movemos en los ámbitos político, de la información, de las noticias -y algo ya han dicho quienes me precedieron en el uso de la palabra-, uno de los temas centrales con que nos toca convivir tiene que ver con cómo se discute, qué cosa es real o no respecto de las famosas *fake news*, aquellas situaciones que se levantan como verdaderas cuando no lo son.

Entonces, quisiera saber qué mecanismos se podrían recomendar para un control de calidad de los mensajes, sobre todo políticos, en las redes; qué podemos hacer para evitar un poco lo que ocurrió en la elección de Estados Unidos.

Ahora bien, otra pregunta que también siempre surge en el debate cuando uno aborda estos asuntos es qué tan seguro es tener los datos en servidores en el extranjero y no en servidores propios. Me queda claro que en muchas ocasiones hay que crear este tipo de servidores. Muchos de nuestros datos personales se alojan en servidores que no están en el territorio nacional, sino que se hallan en el extranjero. De modo que siempre surge la duda de qué pasa con la seguridad, con la información de los datos.

En consecuencia, quisiera que nuestros invitados pudieran comentarnos estos dos temas: la seguridad de los servidores en el extranjero y qué mecanismos nos recomendarían para tener un mejor filtro sobre los tipos de mensajes que circulan, de qué manera podemos evitar el crecimiento de noticias falsas.

Muchas gracias.

La señora RINCÓN (Presidenta accidental).– Tiene la palabra el Senador Letelier.

El señor LETELIER.– Señora Presidenta, quiero agradecer mucho la iniciativa de hoy, que considero tremendamente importante.

Me parece que, junto con la discusión sobre ciberseguridad, hay un debate marco que tiene que ver con algo que está pendiente: que este tipo de instrumento, que el internet, como se dice en términos genéricos, sea un derecho esencial para todos. Algo que ha mostrado esta pandemia son las brechas digitales que existen en la sociedad, pues no todos son ciudadanos digitales. Y, en tal sentido, si tuviéramos que declarar hoy la frase de "avanzar hacia una república digital", parecería un gobierno bastante autoritario, porque la gran mayoría de las personas no tienen acceso a ser ciudadanos digitales, a tener conectividad, a contar con accesibilidad universal, sea por cobertura, sea por precio.

Pero ese debate también se halla pendiente.

Por ende, entendiendo que estamos en un momento especial de la humanidad, donde la pandemia ha ayudado a transparentar muchos fenómenos -la brecha digital y la importancia de la ciberseguridad-, quiero agradecerles a los expositores, a "Chema", porque a mi juicio se hacen una cantidad de preguntas tremendamente esenciales para esta época. Porque uno de los problemas que tenemos los legisladores -y es algo que discutimos en este Senado cuando se creó la Comisión de Desafíos del Futuro- es la necesidad de cerrar las brechas también entre los tomadores de decisiones y los conocedores de las fronteras del conocimiento, para que los marcos regulatorios no queden rezagados diez, veinte años con el avance del conocimiento y la toma de decisiones.

Deseo agradecerles, asimismo, sus provocaciones al señalarnos cuánto nos falta para entender más los fenómenos que están en juego, y al plantearnos de una forma humanista el debate acerca de la tecnología, para qué y cómo la regulación ha de contribuir al mejoramiento de la calidad de vida de las personas hacia la felicidad.

En el marco de la regulación, me gustaría plantear un tema que quizás es uno de los que él abordó: qué pasa con las noticias falsas, las *fake news*, o con el uso de los datos de las personas para cambiar comportamientos. Una de las posibilidades para que eso ocurra es que se usen *bots*, o máquinas; que se utilice un programa para influir sobre el comportamiento de las personas desde múltiples cuentas que no tienen una identificación clara acerca de quiénes son sus dueños. No hay una identidad fidedigna cuando se usan las plataformas.

En algunos países se ha tratado de regular el uso de *bots,* o de máquinas, por ejemplo, antes de las elecciones para que no influyan en el comportamiento de las personas.

Ese es un debate.

Pero también hay una discusión muy fuerte en lo que respecta a tratar de controlar la identidad fidedigna de las personas que acceden a las plataformas, de forma tal que deban hacerse responsables de sus hechos y dichos.

Creo que aquello está muy vinculado a la libertad de expresión.

En lo personal, soy partidario de que avancemos en cuanto a obligar, en materia de identidad fidedigna de quienes acceden a las plataformas, a eliminar las cuentas falsas, que no pertenecen a personas de carne y hueso. Sin embargo, deseo conocer la opinión de los expertos sobre el particular. Porque todos sabemos que la dirección IP permite rastrear desde donde se emiten datos, informaciones.

Debemos avanzar en el marco legislativo como un elemento de la ciberseguridad, y también para evitar el mal uso o las influencias no aceptadas por la sociedad, en que deba establecerse la identidad fidedigna de quienes acceden a ciertas plataformas.

Dejo planteado el punto, señora Presidenta, porque en Chile estamos trabajando en un proyecto de ley para que internet sea reconocido como servicio público, para que avancemos en el acceso universal. Se trata de un debate que se halla instalado en toda América Latina, y con seguridad, en todo el mundo.

Probablemente, en los próximos cinco años haya fibra óptica en la gran mayoría de los hogares -o deberían contar con ella- de los países. Por cierto, aspiramos a que así sea también en el nuestro. Pero la pregunta es cómo regular para que no se haga mal uso de esta tecnología, para que no incida en el comportamiento de las personas, porque el acceso a nuestros datos por el momento, en verdad, es muy difícil revertirlo. Y ahí debemos ver qué cortapisas podemos poner. Pero a mi juicio el uso de los *bots* y el mal uso de las noticias falsas es urgente de abordar.

Gracias, señora Presidenta.

La señora RINCÓN (Presidenta accidental).– Vamos a darle la palabra, después de las intervenciones que restan -son dos-, al profesor José María Alonso, para que pueda respon-

der a los comentarios y consultas que se han hecho.

¿Después o antes?

El señor COLOMA.– Después.

La señora RINCÓN (Presidenta accidental).– Sí. Después de que intervengan los Senadores que faltan podrá intervenir el profesor.

Tiene la palabra el Senador Coloma.

El señor COLOMA.– Señora Presidenta, primero quiero agradecerles al Senador Pugh -lo han hecho varios- y a los expositores, que nos han remecido.

No hay nada más importante que cuando a uno desde el punto de vista intelectual lo fuerzan a ir más allá de los contornos normales en que quizá se acostumbraba a manejar y le plantean nuevos retos, a partir de nuevos cambios en otros ámbitos; y creo que eso es fascinante. Pero, de alguna manera también es muy exigente, porque, a contrasentido, el entender que puede haber avances en muchos temas relevantes de la sociedad moderna, sin asumir el rol que tienen los contrapesos razonables a eso, puede generar obviamente un espacio de desacople respecto de las instituciones que emergen con, justamente, los resguardos positivos que tienen que asumir.

Quizá la mejor forma de plantear lo que quiero decir es hacer un símil. Aquí hay políticas públicas importantes en nuestro país que, de no generar los espacios de control o desarrollo, pueden terminar de mala manera. Imaginémonos, por ejemplo, los parques nacionales, que son bienes de uso público muy relevantes; que fueron importantes en el pasado y todo parece indicar que van a servir no solamente como un resguardo patrimonial, sino como una reserva muy valiosa de nuestro planeta en asumir cómo se comportan.

Imaginemos un parque nacional que no tiene política de guardabosques o de guardaparques. Naturalmente, uno puede diseñar una idea, pero si no tiene asociada, no solamente una forma de control, sino que una forma de marcar, una forma de educar y una forma también de combatir en determinados momentos los involucramientos indeseados, al final, lo que puede ser una buena idea termina simplemente arado en el mar.

Y un segundo ejemplo puede ser el funcionamiento de un edificio. ¡Claro!, los edificios se pueden construir; pero si no hay mantención, un conserje -planteémoslo para este efecto-, obviamente eso va a funcionar en forma caótica.

Bueno, yo creo que lo mismo nos están diciendo respecto de toda la innovación en materia digital. Si no va acompañada de políticas de ciberseguridad importantes; algo que está destinado potencialmente a generar un bien muy relevante puede desvirtuarse o ser utilizado de mala manera.

Probablemente, la palabra misma "ciberseguridad" es bien moderna dentro del léxico mundial. Es, sin duda, más propia de este siglo que de siglos o milenios pretéritos, desde que existe el lenguaje, la escritura. Pero también las cosas que se abordan son de otra magnitud -algún Senador lo planteaba-, y con un universo bastante desconocido hacia adelante. Si uno supiera exactamente a qué se va a enfrentar tanto en lo positivo, como es el desarrollo digital, como en lo negativo, que es la instrumentalización o mala utilización de esos medios, todo sería bastante más fácil. El problema es que además estamos con una serie de incógnitas que generan parte de la fascinación, pero parte también de la obligación de quienes tenemos por definición que generar políticas públicas, instituciones, resguardos es considerar este elemento cuando se habla también del otro.

O sea, a mí me queda claro, después de lo que uno va escuchando y oyendo, que hablar de un desarrollo digital o hablar creyendo que el número de "G" es lo que va definiendo -y es verdad- mucho del acceso de las personas a las sociedades masivas del conocimiento o vinculación de las cosas, sin asociar a ello políticas de ciberseguridad, obviamente puede signifi-

car un paso en falso, en circunstancias de que podría ser, en vez de uno malo, dos buenos.

Por eso, Presidenta, yo valoro mucho esta reunión, esta modalidad, que no sé si los invitados lo saben -es bueno que lo conozcan-, pero es muy escasa. Uno puede contar con los dedos de una mano las sesiones en que un Senado funcione con personas que no sean del Ejecutivo, como invitadas en su calidad de expertas. Y creo que es sano, es una buena modalidad. Y ustedes han demostrado que son escenarios a los que uno tiene que recurrir cada vez más, porque aquí necesitamos tener, en forma mucho más potente, esa conversación entre los expertos y quienes hacemos políticas.

Una gran iniciativa.

He dicho.

La señora RINCÓN (Presidenta accidental).– Gracias, Senador Coloma.

Tiene la palabra el Senador Jorge Pizarro.

El señor PIZARRO.– Muchas gracias, Presidenta.

Sé que estamos, bueno, sobre la hora de la sesión; pero seré bien breve.

Quiero agradecer a los expositores y a los colegas que han hecho un esfuerzo por socializar estos temas y transformarlos en un debate de prioridad pública; y sobre todo, además, por ponerlos en la agenda legislativa.

Es evidente que estamos expuestos cada día más a una situación de vulnerabilidad respecto de los datos personales, pero no solo las personas: las empresas, los gobiernos, los organismos internacionales. Todo el espacio cibernético hoy día, así como entrega enormes facilidades, genera también enormes incertidumbres. Y, por lo tanto, la ciberseguridad tiene que ser un derecho que debemos estar en condiciones de garantizar.

El problema es que no tenemos legislaciones que puedan ser sólidas o potentes para el combate contra los riesgos en esta materia; y en nuestro país estamos a años luz, en pañales. En América Latina y el Caribe hay una situación de gran vulnerabilidad en este tipo de delitos, que no tienen fronteras y que se producen en cualquier lugar desde cualquier lugar del mundo. Y, en eso, creo que los expositores que hemos escuchado han sido extraordinariamente claros y gráficos.

Nosotros, en el Parlamento Latinoamericano, estamos haciendo un trabajo por generar un marco legal modelo que sirva para que después se pueda ir aplicando, mejorando en las legislaciones nacionales. Pero aquí, Presidenta, tiene que haber una decisión política, de los Ejecutivos tanto como de los Congresos, en orden a avanzar en una institucionalidad legal que permita enfrentar este fenómeno global de manera más eficiente.

Y, como siempre, hay inquietudes. Están los problemas de si se cede o no se cede soberanía; de cuáles son los organismos jurisdiccionales; de dónde se pueden establecer las sanciones, etcétera, etcétera. Eso va generando un flanco débil, sobre el cual quienes se dedican a desarrollar este tipo de delitos o de crímenes actúan con mucha impunidad y, lamentablemente, con mucha eficacia para cometer sus delitos.

De manera que la consulta mía a ambos expositores, a la señora Rosa Díaz y a don José María Alonso, es de qué manera más efectiva, de acuerdo a la experiencia que ellos tienen, sobre todo en la Comunidad Europea, se puede llevar adelante, a través de los Estados y de la coordinación y cooperación de los Ejecutivos, junto con los Parlamentos nacionales, una legislación que pueda ser más eficaz en la prevención de estos ciberdelitos.

Presidenta, quería dejar constancia de eso. Sería muy bueno, si es posible, tener más información o más detalle.

El señor PIZARRO.– Y una cosa de orden reglamentario, Presidenta, antes de que levante la sesión: quiero pedir una ampliación de plazo para presentar indicaciones al proyecto del boletín N° 11.571-21, que modifica la ley

N° 18.892, General de Pesca y Acuicultura, en materia de prohibición de captura de especies provenientes de cultivos de acuicultura, en específico del salmón.

Si hubiera acuerdo de la Sala, Presidenta, pediríamos una semana más, a lo menos; o unos diez días más.

La señora RINCÓN (Presidenta accidental).– Gracias, Senador.

Nosotros lo habíamos conversado efectivamente en la Comisión de Pesca, para solicitarlo en la próxima sesión.

Si le parece a la Sala, se ampliará el plazo de indicaciones para el proyecto señalado hasta el viernes 9 de octubre, a las 12.

—Así se acuerda.

La señora RINCÓN (Presidenta accidental).– Vamos, entonces, a darle la palabra al profesor José María Alonso, para que pueda responder las consultas o comentarios, y obviamente a cualquiera de los otros invitados, a los que agradecemos su participación en esta sesión especial.

Perdón, antes ha solicitado la palabra el Senador Bianchi. No lo había visto.

Tiene la palabra, señor Senador.

El señor BIANCHI.– Gracias, Presidenta.

Bueno, lo primero es saludar a nuestros invitados, a nuestras invitadas, y a quienes han permitido que tengamos esta sesión. Y agradezco al Senador Kenneth Pugh por haberme hecho parte del proyecto que precisamente coloca este mes como el Mes de la Ciberseguridad en nuestro país.

Yo quiero llevar este tema de la vulnerabilidad de los datos y todo lo que aquí se ha dicho a una materia sobre la que no escuché opinar, dentro de lo que fue esta discusión, probablemente porque estamos hablando de ciberseguridad. Me refiero a algo de la mayor preocupación, pues tiene que ver con la vulnerabilidad de las personas, de los trabajadores, producto de esta misma pandemia; con cómo se adelantó todo el proceso tecnológico; con cómo ha habido un avance en la automatización, fundamentalmente en el orden laboral.

En algún momento hice un proyecto de ley que apunta a que los empleadores se reúnan cada año con los gremios, a fin de establecer cuánto, en qué porcentaje se va a automatizar el trabajo al año siguiente.

Aquí, si bien se habla de la vulnerabilidad de los datos, de lo que debe ser la seguridad, creo que no se puede dejar de lado al ser humano, a la persona. Y si bien en el presente hay una tecnología indetenible, que avanza, que además nos permitió, en pandemia en el mundo, tener las videoconferencias, los encuentros, en fin, y todo lo que ya se ha dicho acá, quiero dejar puesto, Presidenta, el tema de la vulnerabilidad en lo laboral, porque los Estados van a tener que hacer algo con esto. Las empresas se van automatizar.

Por lo tanto, más allá de lo que tiene que ver con la seguridad de los datos, siento que también necesitamos, como Congreso, avanzar en buscar resguardos para las trabajadoras y los trabajadores, quienes se van a encontrar con una realidad en que lo más probable es que un porcentaje importante de las industrias se automatizarán.

Con el proceso de automatización, el Estado efectivamente se va a encontrar con la imposibilidad de personas que no están avanzadas hoy en día en lo tecnológico, ni con el conocimiento suficiente. Es decir, se va a enfrentar a la realidad de una humanidad sin posibilidades laborales.

Ese es un tema que también tenemos que abordar, Presidenta, y quiero dejarlo instalado en esta oportunidad, agradeciendo el espacio y agradeciendo todas las intervenciones.

Gracias.

La señora RINCÓN (Presidenta accidental).– Gracias, Senador.

Ahora sí, le damos la palabra al profesor José María Alonso.

El señor ALONSO (CDCO de Telefónica).– Gracias, Presidenta, y gracias a todos los Senadores por las intervenciones que han tenido después.

He tomado notas de ellas. Me han salido como ocho preguntas de las siete intervenciones, y voy a responder algunas. Creo, sí, que hay una en concreto que la tiene que contestar nuestra compañera Rosa Díaz.

Voy a empezar por parte.

En la primera intervención, el Senador preguntaba si se puede prevenir un ciberataque, si estamos en disposición hoy en día de prevenir los ataques y no solo de reaccionar ante ellos.

La respuesta es que garantizar que una organización no vaya a tener un ataque con éxito es prácticamente imposible. Tú no puedes garantizar que vas a crear un sistema invulnerable -y esto es algo que hemos repetido hasta la saciedad-, pero que puedes proteger el sistema para que no te afecte de manera masiva, por supuesto.

Nosotros hace mucho tiempo que hablamos de aplicar medidas de defensa en profundidad, de aplicar seguridad preventiva, de aplicar detección, de invertir en la detección de que alguien está intentando hacer un ataque, de aplicar medidas para responder en el caso de que el atacante tenga éxito y de aplicar medidas de restauración de vuelta hacia atrás.

Desde hace mucho tiempo, las empresas preocupadas por ciberseguridad pues utilizan sistemas de ciberinteligencia que están detectando cuándo se están moviendo datos de una compañía en internet, o cuándo están apareciendo informaciones en grupos de redes sociales o en canales de conversación de chats privados, etcétera, que puedan afectar a la seguridad de la compañía porque se está preparando un ataque. Estos son servicios de ciberinteligencia y las empresas de seguridad es algo que damos desde hace ya muchos años a las grandes corporaciones.

¿Tenemos garantías de que vamos a detectar y poder evitar todos los ataques? Por supuesto que no, por supuesto que no. Pero sí que conseguimos reducir, hacer mucho más complicado ese número de ataques. Y todas las empresas que están preocupadas por la ciberseguridad y todas las instituciones y gobiernos pues aplican estas inversiones en prevención, en detección, en respuesta y en ciberinteligencia para mitigar al máximo el riesgo de éxito de un ataque.

En la segunda intervención, el Senador nos hacía dos preguntas. La primera es si existe alguna manera de prevenir las *fake news*. Y luego, si tenía valor o un mayor riesgo que los datos estén en servidores fuera del territorio nacional.

Respecto a la primera pregunta, sobre prevenir las *fake news*, puedo decir que Estados Unidos, como probablemente todos sean conscientes, es uno de los países más afectados en las elecciones por los ataques de *fake news.* Y una de las redes sociales más importantes del mundo, Facebook, está bajo escrutinio sobre cuáles son sus responsabilidades en la diseminación y en la difusión de las *fake news*.

Sin embargo, una de las cosas que han conseguido las grandes plataformas de internet es eximirse de las responsabilidades. Si una cadena de televisión emite ahora mismo un anuncio que va contra los intereses de la sociedad, pues tiene una sanción, está regulado, no puede hacerlo y, desde luego, la cadena de televisión no puede eximir su responsabilidad de haber emitido ese anuncio. Deben tener medidas de protección y de prevención para que esos anuncios no lleguen a emitirse, para que en horario infantil no se hagan determinados tipos de anuncios, para que no se hagan anuncios pues de reportajes falsos, de propaganda falsa o incluso de productos que puedan generar adicción a las personas, como el tabaco, el alcohol, que están regulados en muchos países. Y tienen ese control y esa responsabilidad.

En algún momento, en el análisis de estas plataformas, hemos conseguido que le dieran la vuelta. O sea, que se eximan de responsabi-

lidades en su modelo de negocio. Ellos son capaces de eximirse de responsabilidad de emitir esos anuncios, de hacer esas campañas de difusión, porque lo pusieron en sus términos y condiciones del contrato. Y como queda escrito, se eximen de la responsabilidad.

Está claro que este no es el buen camino. Nosotros estamos intentando, como ellos se eximen de la responsabilidad, generar todas las herramientas o ver si creamos grupos para que decidan si una cosa que funciona, que se promociona y que se paga por promocionar… No olvidemos que no estamos hablando de *fake news* que las comparte una persona en su *timeline* y se hace popular. Estamos hablando de campañas de *fake news* que han dado al botón de promocionar, han pagado a la plataforma para que lleguen masivamente a todo el mundo.

Y estamos hablando de crear tecnología. Una Senadora en Estados Unidos decía que las empresas de tecnología estaban ofreciendo más tecnología para arreglar el problema que ellas habían generado con la tecnología, con su negocio.

Es una reflexión difícil de resolver; es una ecuación complicada. Pero lo que tengo claro es que, evidentemente, no se pueden eximir de su responsabilidad.

Y os pongo otro caso muy sencillo: el YouTube, una plataforma de vídeos, donde cualquier persona sube un vídeo que es pirata e ilegal. Y lo que te dice la plataforma es: "Dímelo, y lo quito, pero si no me lo dices, yo mientras tanto estoy generando dinero con él". De nuevo, se eximen de la responsabilidad de que la piratería está sucediendo gracias a ellos.

Esto es algo que, como reguladores, pues tenemos que pensar si a estas plataformas les permitimos algo que no le aceptamos a nuestras cadenas de televisión nacional o a nuestras empresas de tecnología nacional.

En cuanto a si el riesgo es mayor o menor por el hecho de que los datos estén en servidores extranjeros, pues, bueno, el debate aquí ya alcanza a otro nivel. Ya estamos hablando de temas de seguridad nacional, de ciberespionaje o de ciberguerra. Estamos hablando de otro tipo de situaciones, donde ya el nivel de confianza no es con las propias empresas, sino con los propios países.

Como probablemente saben los Senadores y Senadoras, en Europa tenemos una política muy férrea de *data residency*, de que los datos tienen que estar en nuestras empresas, en nuestros territorios, y ello está generando bastante polémica con ciertas plataformas tecnológicas. Supongo que nadie está ajeno a la guerra de Estados Unidos-China por el control de las tecnologías, dónde están almacenados esos datos y quién tiene acceso a esos datos, que está llevando, pues, a que se estén tomando medidas de baneo, de prohibición de determinadas plataformas en suelo americano y en suelo de otros países.

Entonces, esto ya es una decisión de seguridad nacional. Cada Estado debe valorar si se siente cómodo o no se siente cómodo con sus políticas de seguridad nacional.

En otra intervención, tengo puesto que el Senador agradece que el discurso haya sido provocador y haya traído por lo menos material para pensar. Y le agradezco, por supuesto, el comentario y la reflexión. Si tuviera que quedarme un mensaje de esto, me gustaría que por lo menos las Señorías, los Senadores y Senadoras, se llevaran la sensación de que las cosas no son tan fáciles ni tan triviales; que una página en blanco que sirve para buscar cosas, probablemente no es todo lo que parece; no es solo una cosa en blanco para buscar cosas, sino que hay un mundo detrás, de tecnología, de negocio, de implicaciones, de almacenamiento de datos, de sistemas que analizan y recolectan información, etcétera, y que deberíamos por lo menos tener presente que hay que conocer mucho más a las tecnologías, sobre todo para ser capaces de tener una visión de qué nos podemos enfrentar en el futuro. Eso es importante.

Si consigo que con esta intervención ese

pensamiento haya calado en sus mentes, para mí será todo un éxito.

La siguiente pregunta que tengo aquí puesta es de una intervención en que se habla de los *bots*, de cómo detectar a los *bots,* y si podríamos, para protegernos mejor contra los cibercriminales, tener una identidad robusta a la hora de conectarse a las plataformas y exigir esas identidades robustas para hacer que cada uno sea responsable de sus acciones en internet.

Desde luego, una identidad robusta no es la dirección IP. Existen ya desde hace mucho tiempo formas de enmascarar direcciones IP. Estamos hablando de un mundo en donde las direcciones IPv4 se han agotado. Ya estamos hablando de direcciones IPv6, que se asignan dinámicamente; estamos hablando de conexiones a través de redes en la *deep web*, de proxys, de conexiones TOR, que enrutan a través de muchos servidores el tráfico para enmascarar las direcciones.

Efectivamente, esa no es la identidad. Y cuando se ha intentado proponer una identidad robusta a los usuarios cuando se conectan a las plataformas ha sido prácticamente imposible. Estamos en un mundo donde, por desgracia, porque nuestras decisiones todavía consideran operaciones en paraísos fiscales, existen países que no tienen documento nacional de identidad porque no quieren ser vigilados por sus gobiernos; donde todavía seguimos sin ser capaces de decidir si queremos quitar el dinero físico y poner todo el dinero de manera virtual para que queden rastros de todas las operaciones. Poner en internet una identidad robusta es algo que se ha planteado alguna vez, pero que ha sido muy complicado de realizar.

Ha sido muy difícil y es complicado que una plataforma tecnológica en uno de esos países, donde no tienen ni documento nacional de identidad, se avenga a permitir que se exija una identificación de los usuarios de su plataforma. Pero es algo que está en el ADN del nacimiento de internet.

La siguiente intervención hablaba de que no tenía sentido, decía el Senador, crear un bosque sin guardabosque, o un edificio sin sistema de seguridad, y lo cierto es que, por desgracia, primero hemos encontrado muchas tecnologías que se crean sin protección, en que la seguridad siempre ha sido un añadido, algo que, si no pasa nada, te lo puedes ahorrar. Si no ha pasado nada, pues me he ahorrado la inversión en seguridad.

Porque el problema de la seguridad es que si inviertes mucho en ella y no pasa nada, la gente se pregunta por qué estamos invirtiendo tanto en seguridad si no pasa nada. Esto es algo en que la percepción social es muy importante. La gente exige más inversión en seguridad cuando tiene sensación de peligro, y menos inversión en seguridad cuando no tiene esa sensación de peligro. Y sin embargo la ciberseguridad es algo en lo que tienes que invertir para que no pase nada; es gastarse mucho dinero para no tener nada mejor, no tener un mejor coche, un mejor servicio, sino un servicio al que no le ha pasado nada.

Y eso es algo que exige mucho a las personas responsables de los presupuestos, a las personas responsables de los grandes proyectos: aprendizaje e interiorizar cómo funciona el mundo de la tecnología, porque, si no, es muy complicado justificar las inversiones en seguridad si no pasa nada. Ese es el gran problema.

Luego se preguntaba de qué manera se puede hacer más eficaz la legislación para luchar contra el ciberdelito. Yo creo que esa pregunta la debería contestar mejor nuestra compañera Rosa, porque ella conoce mejor todo este ámbito en el que hemos operado en España. Así que me gustaría pasarle la pregunta a la señora Rosa Díaz.

Respecto de la última consulta que hacía el Senador, la última reflexión, que es muy acertada, referida al reemplazo de los puestos de trabajo o laborales por tecnología, lo que él llamaba la "vulnerabilidad humana", en verdad es algo que tenemos que enfrentar como

sociedad, porque va a suceder de aquí a treinta años. Probablemente el 70 por ciento de los puestos de trabajo que realizan hoy en día personas van a ser reemplazados por tecnología o sistemas de inteligencia artificial. Y vamos a tener una reacción en contra de las personas que pierdan sus puestos de trabajo. Creo que como políticos responsables del bienestar de la sociedad es algo que se debe atacar, y se debe atacar desde la formación y la preparación de la sociedad para el nuevo mundo, para el mundo que viene.

Yo pongo un ejemplo que, probablemente, todos conocen. Hoy en día vamos al cine y está lleno de películas que usan masivamente efectos especiales hechos por ordenador, películas preciosas, donde tenemos grandes estudios haciendo efectos especiales por ordenador. El propio Steve Jobs invirtió en la compañía Pixar, que creó la primera película de animación; se llamaba "Toy Story" y era todo por ordenador.

Sin embargo, años antes, años atrás, una película que se llamaba "Tron", donde los personajes eran seres humanos que iban dentro de un ordenador, no pudo competir en la Academia de Hollywood porque los efectos especiales de la película habían sido hechos por ordenador y lo consideraban trampa, así que no la dejaron competir. La industria de los profesionales de los efectos especiales se rebeló contra una película que utilizaba herramientas digitales.

Y esto lo vamos a ver en los próximos treinta años de manera masiva. Vamos a ver coches autónomos, vamos a ver trabajos mecánicos, vamos a ver inteligencias artificiales que van a ser capaces de realizar muchas de las tareas que realizan las personas hoy en día: atender en los *contact centers* llamadas de teléfonos, pedidos.

Muchas de esas tareas van a ser reemplazadas por inteligencia artificial, y eso es algo que no podemos eludir. Tendremos que ver de qué manera fomentamos una transición humanista, donde no dejemos a nadie atrás, donde preparemos a las personas y las ayudemos si no están preparadas para el nuevo mundo.

La señora RINCÓN (Presidenta accidental).– Muchas gracias, profesor.

Usted quería que una pregunta fuera respondida por la profesora Rosa Díaz. Lamentablemente, ella ya está desconectada, así que no podrá hacerlo. Y además ya estamos en la hora de término de la sesión.

Por lo tanto, les agradezco la participación a todos quienes nos han acompañado, a los invitados especiales, y obviamente a nuestros colegas, por sus intervenciones.

Creo que ha sido una sesión tremendamente importante, que da cuenta de los desafíos que enfrentamos como país en ciberseguridad, tema que se ha instalado y que requiere nuestra acción y la toma de medidas.

Así que les agradezco a todas y a todos. Nos quedamos con el desafío que nos ha propuesto el Senador Kenneth Pugh y quienes nos han acompañado el día de hoy.

Muchas gracias.

Habiéndose cumplido su objetivo, se levanta la sesión.

—Se levantó a las 12:00.

Julio Cámara Oyarzo
Director de la Redacción