**La secretaria diputada María Eugenia Hernández Pérez:**… Marivel Solís, Juanita Guerra Luna, de la presidenta de la Comisión de Seguridad, y a todos los ponentes que el día de hoy nos van a acompañar.

Buenas tardes a todas y a todos. La ciberseguridad adquiere una relevancia cada vez mayor en la comunidad internacional porque se trata de una cuestión estratégica para la seguridad de los estados nacionales, así como para la seguridad e integridad de las personas en todo el mundo. Los crímenes que se cometen a partir del uso indebido de tecnologías de punta crecen cada día, cada vez se vuelven más sofisticados y representan un desafío constante para las autoridades y la sociedad.

La ciberdelincuencia es un fenómeno de tal complejidad que hoy por hoy aún no hay consensos internacionales para tipificar los ciberdelitos específicos, y porque el nivel de organización de los grupos que practican esta actividad delictiva logran vencer rápidamente barreras nacionales, protecciones tecnológicas, sistemas de inteligencia y demás instrumentos que el mundo ha desarrollado para garantizar la seguridad de las personas.

En estos momentos de tiempos difíciles de pandemia, hemos conocido que los ciberdelitos que afectan a la población se multiplican a través de clonación de teléfonos y cuentas bancarias, robo de identidad, fraudes de compras en línea, etcétera. Las empresas también son presa de estos delitos por medio de piratería sofisticada, suplantación de personalidad comercial, espionaje industrial.

Todos estamos expuestos a la ciberdelincuencia, pero lo más inquietante es que las áreas estratégicas de los estados nacionales suelen ser vulneradas por este tipo de prácticas; ya ha ocurrido en México en empresas del Estado como Pemex y la Comisión Federal de Electricidad. Pero también puede ocurrir en áreas como las comunicaciones, los transportes, los circuitos hacendarios, la inteligencia civil y militar, entre muchas otras.

De hecho, la ciberseguridad es una cuestión de seguridad nacional, estoy convencida de ello, razón por la cual presenté una iniciativa de reforma a la Ley de Seguridad Nacional, con el objeto de que el ciberespacio y la ciberseguridad sean considerados como asuntos de seguridad nacional. Que la ciberdelincuencia sea asumida como una amenaza importante a la integridad y la estabilidad del Estado Mexicano. Por todas estas razones, hemos impulsado el análisis abierto y multidisciplinario de los retos que enfrenta el mundo en materia de ciberseguridad.

Hemos llevado a cabo una serie de diálogos para abordar esta problemática desde la diversidad de ángulos que implica, desde el punto de vista tecnológico, hasta el enfoque legislativo, criminal, financiero, cultural y social. Reitero el tema, es sumamente complejo, por ese motivo realizamos este Foro Latinoamericano de Ciberseguridad, precisamente para conocer cómo se prepara la región para enfrentar los nuevos desafíos tecnológicos en la materia.

Como ya se dijo, el fenómeno de la ciberdelincuencia es internacional, tiene una dinámica que le permite actuar coordinadamente en tiempo real desde diversos países, lo cual permite a los grupos criminales eludir las medidas de seguridad. Esta circunstancia obliga a establecer mecanismos de colaboración y coordinación entre los países de una región que tienen mucho en común como lo es América Latina. En este foro abordaremos la situación de la ciberseguridad en México, la dimensión de la ciberseguridad en la región, así como los crecientes desafíos y recomendaciones globales.

Tenemos el honor de contar con la participación de distinguidos legisladores, investigadores, autoridades, especialistas y comentaristas de los diversos países de América Latina. Se abordarán temas relativos a protección de datos, infraestructura, investigación, capital humano, el contexto regulatorio, la experiencial en internacionales y multilaterales, entre otros enfoques, con el objetivo de lograr una mirada integral del desafío global en materia de ciberseguridad y el momento actual que se vive al respecto entre los países y los pueblos de América Latina.

Finalmente, no queda más que agradecer de antemano a los participantes de este foro, a la Comisión de Ciencia y Tecnología e Innovación, de la Cámara de Diputados, presidida por la diputada Marivel Solís Barrera, y sobre todo, a quienes nos distinguen con su atención al desarrollo de los trabajos que se desplegarán en los tres bloques de discusión y análisis. Estoy segura que este esfuerzo colectivo se traducirá en un aporte a la experiencia, a la masa crítica existente en materia de ciberseguridad, esa es la idea, enriquecer en debate, plantear propuestas, y difundir este importante tema en beneficio de los pueblos latinoamericanos. Muchas gracias.

Enseguida, le vamos a dar la palabra a la senadora Beatriz Paredes.

**La senadora Beatriz Elena Paredes Rangel:** Muchísimas gracias, estimada diputada. ¿Me escuchan? Muchísimas gracias. Saludo a la presidenta de la Comisión de Ciencia y Tecnología de la Cámara de Diputados, diputada Marivel Solís. Saludo a los integrantes y a la representante de la Comisión de Seguridad de la Cámara de Diputados, la diputada Juanita. Saludo a los distinguidos invitados especiales y a los legisladores que se encuentran entre nosotros, y a los invitados internacionales que atendieron esta importante convocatoria.

En primer lugar, quiero dar testimonio de mi felicitación a la Comisión de Ciencia y Tecnología de la Cámara de Diputados, por la decisión permanente de estar presente en… generar debate, reflexiones compartidas sobre los grandes temas de nuestro tiempo. Nos parece muy relevante el que la comisión este abordando siempre con un espíritu democrático y plural las temáticas más importantes del siglo XXI. Aprecio mucho a la diputada María Eugenia Hernández me haya convocado a este evento.

Participo en esta oportunidad como presidenta de la Comisión de Relaciones Exteriores para América Latina y el Caribe, del Senado de la República, acompañando un evento internacional de la colegisladora, y lo hago con gusto porque conozco del interés de los integrantes de la Comisión de Ciencia y Tecnología, particularmente de la diputada Marivel Solís, por el proceso de internacionalización de nuestras actividades.

Por otra parte, les comento que soy integrante de la Comisión Bicamaral de Seguridad Nacional, una Comisión Especial que existe en el Congreso Mexicano, creada por la Ley de Seguridad Nacional, en donde concurrimos tres senadores y tres diputados para expresar el punto de vista del Congreso Mexicano sobre las políticas de seguridad nacional, y desde luego, de defensa de nuestra soberanía. Es con esas dos circunstancias, dos condiciones, que les hago un muy breve comentario.

La problemática de la ciberseguridad es un gran tema de nuestro tiempo, es impensable que en otro momento de la historia pasada pudiéramos reunirnos a conversar sobre como la tecnología ha logrado transformar de manera definitiva y estructural las relaciones en nuestras sociedades. Y así como ha habido una transformación positiva por la Revolución Cibernética e Informática en el mundo, por las telecomunicaciones, también se han presentado nuevos riesgos, y uno de los riesgos más relevantes es la presencia de delincuentes cibernautas, de la delincuencia que pone en riesgo los sistemas que operan con servicios informáticos, que son prácticamente todos.

Es por ello, que a lo largo y ancho del planeta tierra se preguntan los sistemas cómo pueden atender y proteger todas sus estructuras que utilizan recursos tecnológicos. Esto es clave para el sistema de protección militar y de seguridad, es muy relevante para el sistema financiero, es esencial para la secrecía y discreción de procesos en los gobiernos y en las grandes empresas, y evidentemente, para los servicios energéticos que están vinculados con cursos tecnológicos sofisticados.

Todas las grandes actividades humanas de esta etapa de la historia del mundo están relacionadas con el uso de la tecnología. Por ello, considero de la mayor relevancia este encuentro, conocer las experiencias de otros países, escuchar a los expertos para que el criterio de los legisladores, que estamos conscientes de que hay que legislar en esta materia, se nutran de su conocimiento y de su especialización.

Para concluir mi comentario, quiero decirles que una de las cuestiones que más me lastima en materia de ciberseguridad es la existencia de pornografía infantil. Creo que uno de los asuntos que debemos atacar con mayor rigor, con mayor convicción, tanto con los recursos tecnológicos apropiados como con la normatividad penal que corresponda, es la circunstancia de pornografía infantil, que lamentablemente es uno de los graves problemas que se presentan en nuestro país y en la región de América Latina.

Dándoles la más cordial bienvenida, solo reiterarle a mis compañeras y compañeros diputados la disposición del Senado de la República de participar activamente en este proceso para que encontremos la normatividad y la legislación más idónea para atender la realidad de la ciberseguridad en México. Muchísimas gracias.

**La secretaria diputada María Eugenia Hernández Pérez:** Pues muchas gracias por sus palabras, senadora Beatriz Paredes. Enseguida le vamos a dar el uso de la voz a la diputada Juanita Guerra Mena, que nos va a hacer una exposición de motivos. Adelante, diputada Juanita. Bienvenida.

**La diputada Juanita Guerra Mena:** Gracias, diputada María Eugenia Hernández, compañera legisladora en la Cámara de Diputados. Saludo con mucho respeto a la presidenta de la Comisión de Ciencia y Tecnología, Marivel Solís. Amiga, gracias por darme la oportunidad.

Pero también darle las gracias a la senadora Beatriz Paredes por esa experiencia que tiene, de su gran trayectoria política, pero, sobre todo, en este tema de seguridad, y más aún que está en la bicamaral, que es la soberanía y salvaguarda de seguridad nacional.

Quiero compartirles que en la Comisión de Seguridad Pública nos encontramos en este momento en el análisis del proyecto de dictamen, por lo subsecuente a la iniciativa presentada por la diputada María Eugenia Hernández.

Como bien lo señaló, hay temas relevantes en lo económico, en lo social y en lo político, pero sobre todo en la soberanía nacional de nuestro país. Al hablar de ciberseguridad y cibercrimen pareciera que el destino y el tiempo nos alcanzó, que en las formas elaboradas a partir de la ciencia y el derecho con el objeto de regular el comportamiento de personas en sociedad se encuentra un importante grado de… frente al actuar en una delincuencia actualizada y que ha usado y ha abusado de la tecnología para las actividades ilícitas.

Hace unos meses, en un espacio similar a este, reflexionamos sobre cómo la pandemia del Covid-19 transformó de manera en que establecemos vínculos en el resto de la vida cotidiana. Con ello surgen complicaciones que se materializan como consecuencia de la necesidad de establecer vínculos, pero también de desarrollar nuestras actividades con la mayor… posible, con lo que más cercana es una convivencia armónica, lo mismo que es en la escuela o en el trabajo, con los amigos, así como la familia y en algunos casos hasta con personas que son cuestiones de negocio.

En el mundo virtual había venido desplazando los mecanismos de socialización en las nuevas generaciones, a lo que le denominan nativos informativos. La pandemia, la necesidad de establecer mecanismos remotos colaborativos ha acelerado este desplazamiento en la vida real. Y los instrumentos de interconexión forman parte de los insumos cotidianos en el hogar o en el trabajo.

Tenemos, así como temas, como Zoom, WebEx o pago de Netflix, la membresía del PayPal, las… de online, como Amazon, han venido a sumar una clase de línea a las sesiones de distancia, en este caso de mecanismos de colaboración remota y a un cúmulo de instrumentos que, sumados a las redes sociales, han evidenciado que para muchos se ha dado la posibilidad de generar una interacción, y una interacción social, que es relevancia para el país.

Con todo esto surge la pregunta: si en el mundo virtual es parte de la vida cotidiana, ¿no tendría el orden jurídico que es de adecuarse para sancionar conductas virtuales de la misma manera en que se sancionan las conductas presenciales? La respuesta, sin dudar, lo es, por supuesto que sí.

El reto legislativo para los próximos años es enorme, adecuar las leyes a la realidad virtual, a fin de armonizar en el marco legal en materia de seguridad el uso de las nuevas tecnologías a un ritmo que es vertiginoso., de tal manera para que las leyes vayan al ritmo de la innovación, que sean tan eficaces en el combate de los nuevos tipos delictivos, como es el mismo del día que fueron promulgadas.

Legislar para la seguridad es regular temas como los ciberdelitos. El cibercrimen es una actividad que se desarrolla a la par del desarrollo tecnológico y en supuesta de un alcance para todos. En el hackeo o en la tal información que ha sido evolucionada ha logrado el día de hoy, en diversas agencias internacionales reportan importantes pérdidas para las empresas como consecuencia de una vulneración en sus sistemas de información.

Los modelos de sanción legal son a todas luces insuficientes para sancionar una conducta, que es naturaleza. Es preciso destacar que los países que se han enfocado a actualizar sus mecanismos coactivos cuentan con agencias especializadas y forman parte común, en este los participantes activos, los mecanismos de cooperación internacional y el intercambio de información para la implementación de mejoras prácticas en el nivel global.

Hay conductas delictivas que se dan en Google, en este caso, en el uso de las redes sociales, y eso es una realidad. Lo señaló la senadora Beatriz, se está viendo lo del tema de pornografía, pornografía infantil, que es lamentable, pero también de trata de personas. Lamentablemente utilizan esto para enganchar a no solo personas, sino a menores, para este crimen cruel para la sociedad y, sobre todo, para los menores.

También lo es el hecho de que cada surge una nueva iniciativa para sancionar las conductas delictivas realizadas en el medio de las redes, como el caso de los retos de la inducción al suicidio. Surgen voces que a priori sin fundamento acusan de pretender establecer leyes de mordaza o limitar las libertades. Es una discursiva que pareciera diseñada por los propios delincuentes cibernéticos y cuya falta de empatía en las víctimas en este tipo de delitos es abrumadoramente preocupante.

Esto hay que decirlo, y decirlo de forma muy clara, qué vamos a hacer con aquellos modus operandi en las redes de trata de personas que enganchan a las víctimas en Facebook, qué pretendemos hacer las y los legisladores cuando en los medios te reportan otro joven fallecido para hacer uno de los retos lanzados en unas redes sociales, cómo vamos a establecer tipos penales a quienes de manera encriptada en la denominada Deep web manejan redes de pedofilia y tráfico de órganos.

Son muchas y cada vez más graves y agresivas las conductas delictivas que se dan desde el mundo cibernético. En nuestro país, México, el reto que seguirá y seguirá siendo el de la construcción de una pronta y oportuna legislación de ciberseguridad, con énfasis de protección a los grupos más vulnerables, en donde se establezca el intercambio de cooperación y aprovechamiento de los casos con éxito en la materia. Pero también atendiendo que regular el internet no es limitar las libertades, es proteger a nuestras niñas, niños, adolescentes y mujeres.

Los retos para todos nosotros en Cámara de Diputados y Cámara de Senadores tienen que ser desde que se instaló y consigna en hacer como la diferencia en el frente a la sociedad, pero a la sociedad darles una garantía que les pueda establecer mejores derechos y oportunidades a las y a los ciudadanos, pero sobre todo garantizar la seguridad.

Y, recordemos, en Cámara de Diputados, como también en Cámara de Senadores, estamos ocupados en el tema de seguridad, porque la seguridad la hacemos todos. Es cuanto, presidenta.

**La secretaria diputada María Eugenia Hernández Pérez:** Bien, muchas gracias por su exposición de motivos, diputada Juanita Guerra. A continuación, vamos a tener el mensaje institucional e inauguración de parte de la presidenta de la Comisión de Ciencia, Tecnología e Innovación de la Cámara de Diputados, la diputada María Marivel Solís. Adelante, diputada presidenta.

**La presidenta diputada María Marivel Solís Barrera:** Muchas gracias, diputada. Muy buenos días. Saludo a los participantes del foro virtual latinoamericano de ciberseguridad. De manera especial a la senadora Beatriz Paredes Rangel, presidenta de la Comisión de Relaciones Exteriores. Como siempre, senadora, para mí es un honor que esté usted con nosotros en este evento.

En especial también a la diputada María Eugenia Hernández Pérez, secretaria de la Comisión de Ciencia, Tecnología e Innovación, a quien públicamente hago un reconocimiento por todo el trabajo que ha desarrollado desde hace varios meses, enfocándose fuertemente a este tema tan importante de ciberseguridad.

A la diputada Juanita Guerra Mena, presidenta de la Comisión de Seguridad Pública, muchas gracias por acompañarnos. También al diputado Alfonso Pérez, secretario de la Comisión de Ciencia, Tecnología e Innovación. También está con nosotros el diputado Brasil Acosta. Él forma parte de esta comisión y agradezco mucho su participación y también actualmente está impulsando el desarrollo de un libro enfocado a este tema tan importante. Agradezco muchísimo, de verdad, a todos los invitados especiales, a todos los ponentes.

La pandemia de los últimos meses ha puesto de manifiesto la relevancia que tiene la investigación científica, el desarrollo tecnológico y la innovación. Quienes pertenecemos a otras generaciones hemos tenido que aprender a comunicarnos de forma remota mediante el uso de plataformas digitales desde cualquier punto del país. Y también a nivel internacional tenemos la gran oportunidad, como hoy, de podernos enlazar en diferentes eventos.

Hemos sido testigos de la profunda brecha digital que persiste en nuestras naciones. Hemos tenido que adaptar el sistema educativo, el comercio y las actividades burocráticas a la nueva realidad marcada por el distanciamiento físico y tecnológico. Hemos sido testigos de la evidente necesidad de cambiar aspectos relacionados con el consumo, la seguridad y el trabajo. Estamos viviendo una etapa crucial en la que la ciencia, la tecnología y la innovación serán fundamentales para resolver problemas como la pandemia actual, el cambio climático, la desigualdad, la pobreza, la corrupción o la falta de oportunidades para mujeres y hombres.

Las experiencias que serán compartidas a lo largo de esta jornada nos permitirán repensar el cómo podemos garantizar la seguridad de los millones de usuarios de internet y de las redes de comunicación globales. Hace unos meses, si recuerdan, el Banco Interamericano de Desarrollo y la Organización de Estados Americanos publicaron el informe Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe.

Esta edición, que actualiza los datos de 2016, es una reflexión en torno a lo que en los países latinoamericanos debemos trabajar para fortalecer las capacidades en materia de ciberseguridad, con miras a lograr el diseño más adecuado de políticas y de instrumentos normativos indispensables para garantizar un uso responsable y seguro de la tecnología.

La madurez que han alcanzado Uruguay, Colombia y las naciones andinas en el tema de ciberseguridad son un ejemplo para la región. Nos preguntamos, ¿cómo debemos responder ante los desafíos que representan una mayor digitalización de nuestras actividades cotidianas? Considero que es fundamental que seamos capaces, como señala el informe de la organización internacional y el Banco Interamericano de desarrollo, en primer lugar de crear capacidades para prevenir y reaccionar.

Las instituciones públicas deben ser de alguna manera más eficaces para investigar y sancionar los delitos cibernéticos. Por ello la adecuación a la legislación es vital en este proceso de creación de capacidades. Debemos garantizar los derechos de los usuarios ampliando el acceso a internet y cerrando la brecha digital, facilitando la existencia de ambientes seguros y confiables.

En segundo lugar, el papel de la cooperación internacional es clave para generar sobre todo un espacio abierto, libre y seguro que no limite de alguna manera las fronteras físicas ni biológicas. Por eso celebro y acompaño la iniciativa de la diputada María Eugenia Hernández, anfitriona de este evento, porque justo ha centrado su mirada en proponer reformas indispensables para preservar la soberanía del país frente a los desafíos cibernéticos.

Durante el primer panel se va a contar con especialistas nacionales que hablarán del estado que guarda la ciberseguridad en México. Sobre todo destaco que esta mesa será moderada por el diputado Alfonso Pérez, secretario de la Comisión de Ciencia, Tecnología e Innovación.

Durante el segundo panel, los expertos de varios países de la región hablarán de las tendencias y del estado actual de la ciberseguridad en América Latina. Mesa que será coordinada por Raisa Valda, directora de Warmi, corporación especializada en temas de ciberseguridad en Bolivia. Muchas gracias, de verdad, por acompañarnos.

Finalmente, destaco que durante la mesa tres que moderará el doctor Javier López Casarín, a quien saludo de verdad con gran estimación y respeto. Gracias. Él es el presidente del consejo técnico del conocimiento y la innovación.

Aquí los especialistas ofrecerán sus recomendaciones para fortalecer la protección de datos, el uso de inteligencia artificial para atender los ciberdelitos y la necesidad de contar con un plan para México en esta materia. Siendo las 11:35 horas del día 29 de octubre del año 2020, para mi es un honor inaugurar el Foro virtual latinoamericano de ciberseguridad. Muchas gracias a todos. Y deseo el máximo éxito y continuaremos fortaleciendo este tema tan importante de la Ley de Ciberseguridad. Muchas gracias a todos.

**La diputada María Eugenia Hernández Pérez:** Muchas gracias por sus palabras de inauguración, diputada Marivel Solís Barrera. Y pues ya inaugurado el evento pues vamos a iniciar -ya lo comentó la diputada- con el panel número uno, en donde es Ciberseguridad en México. Le vamos a dar la palabra a nuestro diputado federal, Alfonso Pérez Arroyo, quien nos hará el honor de ser el moderador de este panel. Bienvenido, diputado Alfonso y a iniciar los trabajos.

**El diputado Alfonso Pérez Arroyo:** Gracias, diputada.Saludo con todo respeto a todos los presentes en este foro virtual latinoamericano sobre ciberseguridad. Le vamos a dar la palabra y bienvenido al maestro Javier Nieto Miranda. Él es maestro en Administración pública, por el Instituto Nacional de Administración Pública. Cuenta con estudios en el ámbito de gobierno electrónico… liderazgo y negociación política y desarrollo de tecnologías.

Se ha desarrollado como profesional de la innovación tecnológica, destacándose como director de desarrollo tecnológico en el Instituto Nacional de Medicina Genómica, como director de Infraestructura tecnológica en el Instituto Federal de Telecomunicaciones, como titular en tecnologías de la información en el Instituto Nacional de Perinatología, así como diversos puestos en el Instituto Nacional de Cancerología y la Secretaría de Salud. Ha sido reconocido como CEO destacado IP4… en el 2017, así como con la distinción CEO 100 en los años 2018, 2019 y 2020. Sea usted bienvenido, maestro. Le cedo la palabra.

**El ciudadano Javier Nieto Miranda:** Muchas gracias. Buenos días a todos. Agradecerles la invitación a la Cámara de Diputados, a la diputada Marivel Solís, a la diputada Juanita Guerra, a la diputada Maria Eugenia, también a la senadora Beatriz Paredes. Y bueno, a todos los panelistas que hoy nos acompañan, también mis cordiales saludos.

Iniciando con los temas de ciberseguridad, los ciberataques, pues me voy a permitir compartir mi presentación -si es posible- para poder platicar al respecto. Un segundito nada más, por favor. A ver si ahí ven mi presentación. Sí pueden verla, ¿verdad? ¿Me escuchan? ¿Sí? Bien.

 Pues bueno, en el ámbito de los ciberataques sabemos que es un incidente que puede tener un evento inesperado, no deseado y desde luego que tiene probabilidad significativa de comprometer la operación de una institución, de una organización y puede provocar una pérdida o uso indebido de información o desde luego la interrupción parcial o total de un sistema.

En México, 73 por ciento de las organizaciones han experimentado al menos un incidente en materia de ciberseguridad y los más comunes son por *malware*, *software* malicioso 34 por ciento; *ransomware*, secuestro de información en 25 por ciento; exposición de datos internos, en un 28 por ciento; robo de credenciales , 19 por ciento; *cryptohacking* o minería de criptomonedas o monedas digitales, un 10 por ciento.

Bien, la situación actual de los ciberataques en el mundo es también no es menor. En Nueva Zelanda a finales de agosto, se tuvo un ataque a la Bolsa de Valores por una denegación de servicios. También Mapfre, en el mes de agosto tuvo un ataque *ransomware*. Honda y Enel, durante el mes de junio y EasyJet, durante el mes de mayo. La compañía de energía en Portugal EDP a principios de abril también tuvo un ataque de *ransomware*.

En el caso de México, pues los conocidos como es la empresa paraestatal Pemex en noviembre de 2019 tuvieron un ataque *ransomware*. La Secretaría de Económica en febrero, un ataque hacia la red informática interna y, la Secretaría de Trabajo y Prevención Social durante el mes de febrero.

De tal forma que, si bien las tecnologías de la información son esenciales para el desarrollo socioeconómico de un país, su empleo nos lleva a la aparición de nuevos riesgos y de nuevas amenazas que puedan afectar tanto a la seguridad pública como a la seguridad nacional. Y desde luego, a la reactivación económica.

Hoy en día en el ámbito de esta nueva normalidad de nuestra situación sanitaria pues, desde luego que se han exponenciado no solo las tecnologías, pero también se han exponenciado los riesgos que nosotros tenemos en el ciberespacio.

En el mundo, el Foro Económico Mundial señaló que el fraude hubo el robo de datos se encuentra en los principales ataques cibernéticos. En marzo del 2020 también en el CMEC, recibió más de dos millones de notificaciones de material pornográfico en línea, más del doble, en comparación con el mismo mes del año anterior 2019.

En el caso de México, se encuentra dentro de los 15 países con más ciberataques en el mundo. Es el segundo lugar en América Latina y se calcula que en 2019 el costo de los ciberataques fue de 8 mil millones de dólares.

Desde luego, también esto impacta a nuestra ciudadanía ¿cuáles son los principales ataques? Pues el *Phishing,* noticias falsas sobre la vacuna del coronavirus, esto se ha difundido mucho a través de correos electrónicos y pues bueno, desde luego CERT-MX registra más de 35 mil incidentes cibernéticos en 2019, destacando fraude y extorción, agravios contra personas, denuncias ilícitas de varios motivos y, esto se ha potencializado en los últimos meses justo con la pandemia ¿no?

Aquí voy a presentar un mapa del índice de amenazas global. Como pueden ver es un mapa... que puede identificar cuáles son los países que tiene mayor número de incidentes cibernéticos. Desde luego México no es la excepción, como bien dije, el segundo lugar de América Latina, pero no estamos muy lejos tampoco del continente europeo, que también representa un gran número de ataques, esto se basa en la posibilidad de que una máquina, un ataque de… puedan atacar por *malware* o algún otro mecanismo, delegación de servicios o ciberataque.

Bien. Si lo vemos en un ámbito de regiones, podemos ver que el 22 por ciento de los ataques a nivel mundial son por *cryptominrs*, el 18 por ciento son dispositivos móviles. De igual forma el 18 por ciento son por *malware* tipo *botner.* Y bueno, podemos también ver en caso del continente americano, el continente europeo y el continente asiático cómo se van representando cada uno de los ataques que hoy se pueden identificar en el ciberespacio.

También, pues este tipo de ataques se pueden representar en uno de los ejemplos que tenemos es el *Emotet* que es un *botnet,* que es una red de robots informáticos, que se ejecutan de manera autónoma o automática y que, se propagan a través de campañas temáticas, tienen una amplia base de infecciones. Comienzan como un tipo de infección y después, termina como un *ransomware*, es el más común a nivel mundial hoy en día y ha mostrado una intensa actividad de enero a la fecha, con una compañía relacionada con el Covid-19. Hoy en día esta, de cierta forma controlada, pero se espera que a finales de este año vuelva a retomar fuerza.

Bien, otra de las ciberamenazas en el ámbito global, pues son los *VPNFilter* una red global de dispositivos infectados, hoy día tenemos más de 500 mil routers infectados y, obviamente también tenemos ataques a FBI, Cisco y otras compañías de ciberseguridad. El *Sea Turtle* son técnicas de secuestro de sistema de DNS y esto a afectado a embajadas y a dependencias de gobierno. El *Magecart* es un *malware* que recolecta detalles de tarjetas de crédito y esto, desde luego, tiene un impacto en servicios de comercio electrónico.

Otras ciber amenazas que hemos identificado en el continente europeo, aquí las describo, son las dominantes que son Ciberamenazas relacionadas con la pandemia, el *Ransomware* de doble extorsión, amenazas a dispositivos móviles, como bien lo comenté en las diapositivas anteriores, son las que más se pueden identificar. Ataques dirigidos a la nube (*cloud*) hoy en día la nube también es atacada y, lo que hoy se llama ciberguerra fría.

El *phishing* ese es el punto de partida del 90 por ciento de los ataques que se producen, aunque pues el abanico de virus maliciosos que se transfieren a través de mensajes de texto, correo electrónico, es muy amplio.

¿Cómo se originan estos ciberataques? Hoy se tienen la creencia que los países de origen con más cantidades de ciberataques son Rusia, Irán y Corea del Norte, pero también hay que considerad que Colombia y Kenia ya tienen un gran número de ataques cibernéticos hacia otros países.

El APT-C-36 proviene de un país latinoamericano que se centra en robar información secreta de importantes empresas del mundo, de ciertas agencias de gobierno, a través de correos maliciosos. Para lograr que se escondan bajo direcciones y se enmascaren IP y usan servicios de Proxy y VPN, para evitar a las autoridades

Aquí podemos ver los grupos de hackers más sobre salientes es, el top 10 de Elliott Gunton, que es de la juventud en rebelión. Evgeniy Mikhailovich Bogachev en Cronos de la vida real y bueno, hay los piratas del Eje del mal, un zarpazo a la democracia, son grupos que pues se dedican al ataque cibernético.

Desde luego también en Kenia hay un grupo del sector financiero que ha penetrado dos robos de gran magnitud. No existe mucha información acerca de cómo lo consiguieron, pero han logrado acceder a cuentas bancarias de diferentes usuarios y cambian los límites de las tarjetas y usan esas tarjetas en los cajeros automáticos para obtener beneficios.

Y bueno, esto es solamente un ejemplo de lo que hoy día hemos encontrado en los ciberataques. Desde luego, también existen algunos otros rubros como son el ataque a la ciudadanía y, pues es también muy importante porque ahí intervienen otros factores como son las conductas … para que se puedan presentar en delitos cibernéticos en el ciberespacio hacia nuestra ciudadanía y, eso, pues desde luego afecta la seguridad ciudadana de las personas que desde luego se desenvuelven en el ámbito digital. Esta sería mi participación. Es cuanto.

**El diputado Alfonso Pérez Arroyo:** Muchas gracias, maestro. Hoy le damos paso a la intervención del ingeniero Arturo García Hernández, consultor especialista en ciberseguridad. Cuenta con más de 10 años de experiencia en el área de tecnología de seguridad. Es egresado del instituto Tecnológico de Estudios Superiores de Monterrey en la carrera de Ingeniería en Sistemas Computacionales. Cuenta con una maestría en Sistemas Distribuidos por la Universidad Kent de Inglaterra y otra en Seguridades Nacional otorgada por la Universidad Naval, especializándose en el tema de ciber poder. Actualmente cursa el doctorado en Defensa, Seguridad Nacional, en la misma instituciona. Así mismo, cuenta con la especialización en dirección de seguridad de empresas por la Universidad Pontificia Comillas de Madrid. La certificación en… que proporciona la organización… y las… de la organización…

Fue colaborador en el libro *Seguridad y Defensa* del Ciberespacio, escribiendo el capítulo *Una visión del poder económico en la ciberseguridad*, editado en el año del 2015, por la Secretaría de Marina

y autor de la obra *CiberMéxico: voluntades y acciones en el ciberespacio*, publicado en enero de 2019. Le damos la palabra, ingeniero.

**El ciudadano Arturo García Hernández:** Qué tal, muy buenos días a todos. Primero que nada, agradezco muchísimo la invitación y de verdad que es un honor estar compartiendo con la Cámara de Diputados. Muchas gracias por la invitación y, por supuesto, un saludo muy fuerte a todos los colaboradores, los participantes, ponentes, que estamos aquí, y un saludo a todas las personas que atentamente nos escuchan.

Este es un tema de gran magnitud, es una parte fundamental en todo el Estado mexicano. Bien lo mencionaban en la introducción. Es un tema de seguridad nacional. Es un tema en donde tienen que estar involucradas varias partes, varios sectores. Es un eje transversal en donde debemos estar… fuertemente tener una atención completa de lo que estamos haciendo.

La verdad felicito y fomento este tipo de eventos en donde dan una participación completa y una participación de varios sectores… A mí lo que me gustaría en este momento participar es poner un grano de arena sobre lo que sería la seguridad en el sector financiero. Es una parte compleja. La ciberseguridad, como podemos ver, como un ambiente en donde tiene varias aristas, y dentro de estas aristas, si vemos el sector financiero, vemos que una transacción puede tener tres componentes fundamentales:

En el primer pilar, en el primer participante, están todos los ciudadanos y todos los que son cuentahabientes y todos los que tratan de hacer una transacción y tienen la confianza en hacerlo. En esta parte, lo admite el primer punto y de uno de los más fundamentales que tenemos que proteger. Es el punto en donde inicia, ya sea la delegación, la transacción digital, la visita, la caída, en donde empiezan los problemas en donde está involucrado el cibernauta, la persona que está navegando. Este sería el primer factor, es quien está iniciando.

Un segundo factor… es la entidad financiera en donde está haciendo o el comercio electrónico o el proveedor o quien va a dar al gobierno sus servicios. Y en esta interacción es donde empezamos a tener un poco de problemáticas, en donde, como bien lo mencionaba ahorita al principio, vamos a empezar a tener problemas… problemas en donde tenemos una usurpación de identidad, tenemos ahí que nos están robando datos, están…

Pero habría que ver en estos dos sectores el primero… qué tanta participación tiene. La mayoría de las situaciones… los problemas comienzan lamentablemente desde el origen, cuando tenemos una mala, por decir, una salud informática de seguridad, donde tenemos poca protección, donde tenemos algo que nos está faltando de protecciones, de actualizaciones, de buenas prácticas de detección hacia donde estamos navegando.

El segundo factor es en donde tenemos un participante, una entidad financiera -ya sea un banco, el comercio electrónico, una casa de bolsa- en donde vamos a hacer nuestra transacción. Ahí también puede haber un problema, puede haber un robo, pueda haber una mala protección de la información, la que estamos otorgando.

En estos dos puntos es donde estamos viendo que empiezan los problemas a suscitarse mucho, lo que estamos ahorita viendo es sobre ese tipo de confianza: la confianza tanto en la entidad financiera como desde dónde está generando esa solicitud.

Un tercer participante -y esto es muy importante de mencionar- es, por ejemplo, la banca central, en nuestro caso el Banco de México, en donde también está participando, pero además como un intermediario entre algunas transacciones que se están haciendo desde diferentes bancos en algunos participantes. También requiere cierta participación porque parte de nuestras transacciones que están atravesando todo el ciberespacio están yéndose a través de ese intermediario que está viendo, está revisando y está concentrando.

Bueno, estos son los tres puntos fundamentales que debemos de tener en cuenta cuando pensamos en una transacción. ¿Dónde se encuentra el problema?, ¿dónde se encuentran las mayores probabilidades de robo?... robo es cuando tenemos una mala conciencia y una mala protección desde el origen. Un segundo punto es donde podemos tener que la entidad financiera pueda tener una baja, un robo, una baja a nivel de protección o un tercero sería en el banco central. Pero, bueno, en este ecosistema complejo es un evento complejo en donde podemos tener varios tipos de robos -ahorita lo mencionaron perfectamente bien-, hay algunos tipos de robos en donde… ataques en diferentes formas en donde entramos y podemos tener algún tipo de ciberataque…

Si nosotros queremos proteger todas las transacciones, tenemos que recuperar esta confianza que creo que es algo importante. Lo que se ha perdido es la confianza en este mundo digital, en la economía digital, como se ha mencionado.

Yo creo que uno de los puntos más fundamentales es desde el origen. Si nosotros podemos proveer cultura, conciencia, desde el origen de la transacción, vamos a superar mucho… vamos a poder eliminar algunos de los ataques más fuertes. Por ejemplo, cuando no conocemos algún correo o cuando no vamos a necesitar alguna liga, cuando no ponemos nuestra… ejecución o de un correo, ahí estamos alimentando y estamos ayudando. O simplemente el robo de identidad que tanto nos aqueja fue por otro lugar, fue por otra liga y no necesariamente durante la transacción o durante la visita a una banca electrónica. Simplemente… de antes o simplemente… infectado desde antes. Ese es un problema grave y lo podemos solucionar todos los que estamos utilizando, todos los que somos cibernautas y todos los que estamos adentro.

Ahora bien, este problema yo creo que tiene dos puntos importantes tanto buenos como… Los puntos a favor es que en todo este ecosistema tenemos una gran… y tenemos un personal que ya cada vez está más calificado -ahorita… van a hablar desde el sector académico, creo que es muy importante- y ahí tenemos muy buen personal.

También tenemos avances en la colaboración entre entidades financieras, tenemos un grupo de respuesta a incidentes que podemos ponerlos en colaboración con varios de los participantes. Tenemos avance en la regulación, en la supervisión -Banco de México, CNBV, están cada vez incorporando mejores técnicas más avanzadas, más innovadoras, para poder supervisar y revisar todo el ecosistema-.

Y tenemos algunas iniciativas -ahorita lo mencionaban muy bien las diputadas y el diputado que está con nosotros, la senadora-. Esto de involucrar todo lo que es la legislación, eso se da avanzando. Hay un comité especializado en seguridad e información… que apoya la Secretaría de Gobernación.

Yo creo que ese tipo de avances son buenos. Sin embargo, no es todo lo que… no podemos decir que ya hemos madurado -ahorita mencionaban el nivel de maduración-. En el nivel de maduración, creo que todavía tenemos muchas cosas que hacer, tenemos que trabajar más en la cultura -como les decía, son tres puntos importantes, empezando por la cultura… en las transacciones-. Tenemos que ser más rápidos. En el sistema financiero, la adopción de tecnología tiene que ser muy ágil y tenemos que dar un servicio cada vez más complejo y más rápido. Tenemos a la vuelta de la esquina ya el uso de Fintech, de monedas electrónicas, tenemos lo del bitcoin. Tenemos que ir cada vez mas rápido, tenemos que ir supervisando y regulando esto.

Y, finalmente, también… un punto que creo que no hemos atacado de manera concreta e integral: es que estamos ante un riesgo sistémico. Estamos ante un efecto dominó en donde tenemos un problema que puede iniciar en alguna entidad financiera, que puede empezar con algún usuario; sin embargo, esto va creciendo y al no poder comprar y al no poder pagar, no poder hacer la transacción, entonces tenemos que esto se va incrementando.

Creo que el riesgo sistémico es una tarea pendiente y no solo de México. Creo que esta es una tarea mundial y es un punto muy importante que tenemos que atender en todo el mundo en que estamos pegados unos a otros. Estamos en un mundo en donde estamos interconectados.

Agradezco mucho que estemos aquí y la verdad es que es… muy fuerte estar con todos los… compañeros… y yo creo que por ahí es un excelente inicio y esto lo tenemos que seguir agrandando y lo tenemos que llevar todo este esfuerzo hacia diferentes países. Les agradezco mucho y es mi participación.

**El diputado Alfonso Pérez Arroyo:** Bien. Muchas gracias, ingeniero. Hoy le vamos a dar la palabra al maestro Juan Manuel Casanueva. Él es investigador y promotor de proyectos de TIC para el desarrollo y acción social. Es fundador de la organización no gubernamental SocialTIC, asociación civil, dedicada al habilitamiento de actores de cambio a través del uso estratégico de la tecnología digital y la información.

Juan Manuel ha liderado y asesorado proyectos de uso de TIC con diversos organismos internacionales y organizaciones locales latinoamericanas en temática de TIC para la transparencia, rendición de cuentas, incidencia cívica, participación ciudadana, datos abiertos y seguridad digital. Cuenta con estudios de maestría en ciencia, en gestión de implementación de proyectos de desarrollo, por la Universidad de Manchester, con especialidad en innovación social, licenciatura en ingeniería industrial en sistemas por el Instituto Tecnológico de Monterrey … Estado de México. Cuenta con 15 años de experiencia en el sector de la sociedad civil en ámbitos de tecnología educativa y de ambiente y tecnología para el desarrollo. Adelante, ingeniero, le toca su turno.

**El ciudadano Juan Manuel Casanueva:** Muchas gracias. Gracias por el espacio y por tener un grupo polímero en este panel no tan diverso. Me sorprende la falta de diversidad, sobre todo, de una legislatura de quitas de género, pero sí es muy importante que estemos hablando de temas de ciberseguridad en una lógica multiactor.

Si algo le debemos aprender a los espacios de gobernanza de internet es que la formación de política pública de tecnología, justo porque abarca ámbitos no únicamente tecnológicos, empresariales, sino también sociales y cívicos, debería ser contemplado con una perspectiva multiactor y muchas creces dentro de los espacios legislativos están limitados hacia estos grupos de sociedad civil.

Habiendo dicho eso, me gustaría hacer tres reflexiones en materia de ciberseguridad. La primera, siento que nosotros al igual que diferentes colegas que estamos trabajando en materia de tecnología para fines sociales y derechos digitales, tenemos la perspectiva de derechos humanos como un eje central y prioritario y ahí muchos de los aspectos que se han mencionado previamente tienen que ver en cómo las políticas públicas sobre ciberseguridad afectan y favorecen justamente a las personas.

Sabemos que a nivel de riesgo, como ya se han mencionado varios, las personas más afectadas son las personas que igual están en grupos vulnerables. Se mencionó ya el riesgo en materia de pornografía infantil, se mencionó ya el riesgo de noticias falsas, también el tema de violencias en donde hay grupos que muchas veces no tiene las capacidades de defensa y la formación para poderse defender y son las víctimas de estos procesos.

Sabemos que en materia de espionaje los y las periodistas, personas defensoras de derechos humanos han sido víctimas de espionaje, tanto estatal como también privado y que son las víctimas de este tipo de aspectos. No sin hacer de lado mucho de lo que ya se mencionó en materia de contexto de la ordenación a empresas privadas y del sector público, que ya hablaré de eso un poco más adelante, pero sí para tener en perspectiva que muchas veces las víctimas de la ciberdelincuencia son personas que no tienen las capacidades para poderse defender. Y que muchas veces en materia legislativa, la falta de definiciones, ahí voy hacia la segunda reflexión, la falta de definiciones claras pueden llegar a limitar otros derechos, como lo es la libertad de expresión, de asociación y la privacidad en sí misma.

Uno de los principales retos en materia legislativa en ciberseguridad ha sido la falta de definiciones claras, textos vagos en donde, por ejemplo, dicen que cualquier persona que sea identificada haciendo alteraciones a una plataforma cibernética o sistema, esas son definiciones antiguas, eso puede ser cualquier persona que puede estar jugando con sus computadoras o que está alterando nuestros programas.

Eso puede llegar a ser ampliamente criminalizante en lugar de ser algo preciso enfocados en atender los delitos y las acciones de ciberdelincuencia que pueden ser muy fácilmente identificados y que, afortunadamente, los colegas que me precedieron han sido muy claros en ello. Entonces, una de las principales reflexiones que tenemos muchas veces desde los grupos de sociedad civil es que las leyes vagas que tienen una definición clara de cuáles son los delitos, en específico con su componente tecnológico y su componente jurídico llegan a ser muchas veces riesgosos y pueden violentar otros derechos y tener consecuencias muy graves a diferencia de su primario que era el de mantener la seguridad de la ciudadanía.

Otra definición que también hay que tener en materia de legislación y ciberseguridad tiene que ver con cómo entendemos internet, desde sus principios hasta su aplicación más práctica y vemos muchas veces también como peligro entender por posiblemente de manera justificada en … de la seguridad, le queremos dar atributos, por ejemplo, a los proveedores de telecomunicación e internet o a grupos del Estado para que rompan con los principios más básicos de internet, como puede ser la neutralidad en la red.

El hecho de que alguna organización, alguna autoridad tenga la capacidad de estar espiando, vigilando o monitoreando paquetes de internet, no solo violan la neutralidad de la red, sino que muchas veces en … de ciertas búsquedas de seguridad se estaría poniendo abrir la puerta para el uso discrecional de la vigilancia, tanto masiva como selectiva.

Entonces, estos principios que muchos son de revisión e inspecciones de paquetes por parte, ya sea de empresas que proveen los servicios de internet como algunas autoridades, deben estar perfectamente establecidas en materia de cuáles son las características que pueden tener las superadas para solicitar ese tipo de inspección y bajo qué situaciones para que sean legalmente justificadas, que sean proporcionales y que no den paso a un abuso posiblemente dirigido o segmentalizado de estas capacidades en contra de la ciudadanía.

Y esto lo digo lamentablemente con la tercera reflexión general que me gustaría aportar. México como país tiene grandes retos en materia de ciberseguridad que se vinculan no solamente con este tema, sino aspectos institucionales básicos. Lamentablemente México tiene un oscuro pasado de vigilancia estatal y me refiero a nivel nacional y a nivel estatal, que no tiene aún controles democráticos para que se sepa y se puedan castigar los abusos que agencias puedan tener. Sabemos que hoy en día hay … un personaje prófugo de la ley que fue responsable de operar el mal … dentro de la sociedad anterior en contra de sociedad civil, en contra de periodistas, en contra de ciudadanos sin ninguna base legal y con un despropósito total.

Y que la falta de la certeza por parte de la ciudadanía de que las mismas autoridades y los len te los terceros que están colaborando en ámbitos de seguridad y justicia puedan abusar de las capacidades de vigilancia, pues hacen pensar que debemos replantear muy fuertemente no solo las definiciones legislativas, sino las capacidades y los controles que deben de tener las dependencias gubernamentales para ejercer este tipo de capacidades.

Y también recordar que uno de los aspectos que son un reto para el país y como institución de gobierno sigue siendo la impunidad. La definición legislativa de delito, si mantenemos el grado de impunidad que se sigue teniendo, pues muchas veces no sirve de mucho. Entonces, esas tres reflexiones me parecen fundamentales tenerlas siempre en la mente cuando hablemos de ciberseguridad y, sobre todo, cuando estamos hablando de procesos legislativos.

Mis colegas de otras instituciones más con perspectivas de derechos digitales y jurídica tendrán más aportaciones que hacer en la materia, pero simplemente para ahorrarles voz me gustaría plantearles algo que se ha difundido por parte de nuestros colegas de R3D desde hace ya varias semanas y que son los principios de ciberseguridad. Si me dan la oportunidad los menciono brevemente mientras comparto mi pantalla.

Aquí está la página de R3D ciberseguridad. Los 10 principios de ciberseguridad en derechos humanos que implican, como ya mencioné, los derechos humanos sean un eje rector, que hay una participación multiactor, justamente como la que estamos teniendo aquí en palabras de definiciones de política pública y también para los controles democráticos y de transparencia.

La protección y el derecho a la privacidad, mucho en relación a elementos que ya mencioné hace un momento, pero también aplica para aspectos más técnicos como lo es el cifrado, por ejemplo. Controles democráticos de vigilancia, defensa y fortalecimiento del cifrado. Proximidad de la reducción de habilidades y movilización; recolección y almacenamiento de datos, sobre todo, en una era en donde estamos viendo que el capitalismo está basado en la recolección de los datos personales, los datos privados que la ciudadanía tiene a través de los distintos servicios y aplicaciones digitales.

Y, por último, la disponibilidad de internet y protección… informativo, la protección de derechos humanos frente a acciones u omisiones de actores privados. También la regulación y persecución de delitos informáticos con apego a los derechos humanos. Lo dejo aquí como este decálogo que viene de la sociedad civil, justamente para que lo consideremos en todo momento y en las diferentes conversaciones más adecuadas.

Me gustaría cerrar con dos elementos puntuales en materia de ciberseguridad. Lo primero, regresando, es a los usuarios. Nosotros desde SocialTIC, como una organización que atiende caso, sobre todo, en ámbitos de sociedad civil, periodismo, de abusos, de violencias todos los días, notamos que la indefensión y la educación es algo que hay que considerar por parte de todas las informaciones, tanto las privadas como las públicas. Y que la ciudadanía si bien hay que ir construyendo capacidades de defensa y de prevención, es importante que, pues, sea mucho más abierto y haya más esfuerzos justamente en la educación, en donde sepamos justamente cómo reducir los riesgos y los ataques que ya mencionó Javier, que ya mencionó Arturo, en todos sus ámbitos, ¿no?, tanto los aspectos técnicos como también los aspectos humanos, los que tengan que ver con fake news, los que tengan que ver con violencias digitales, sobre todo en contra públicos específicos.

Y aquí hay que establecer una balanza entre poder favorecer que la ciudadanía tenga mejores capacidades de mitigación y defensa, pero también se pueda garantizar el que podamos tener mejor infraestructura de defensa.

Y, por último, haciendo otra vez el reconocimiento a este espacio, sobre todo porque la agenda de ciberseguridad habíamos notado desde afuera de espacios públicos que había estado desdibujada, así es que agradezco el liderazgo, pero es muy necesario que México tenga una agenda multi actor, pero también intergubernamental de ciberseguridad.

No podemos hablar que una ley lo va a resolver todo, tenemos que tener una perspectiva en materia de, sobre todo el Ejecutivo, en cuanto a cuáles son las políticas de ciberseguridad del país, aspectos tan claves que ya nos mencionaron previamente, que tienen que ver con la infraestructura crítica nacional, tanto las dependencias de gobierno, pero también nos podemos ir a aspectos tan básicos para la ciudadanía, como puede ser el suministro de la electricidad. También están en riesgo. Y es importante que haya una congruencia de una agenda que nos permita establecer justamente los presupuestos y los lineamientos uniformes de ciberseguridad para la administración pública, algo que muchas veces en la práctica nos damos cuenta cuando cosas y abusos y ataques suceden. Y esos son de los que nos enteramos desde afuera.

Entonces, sí, con mucha preocupación, pero también con mucho optimismo y por espacios como este vemos que están los elementos puestos en la mesa para que se puedan establecer políticas públicas integrales, sensibles a los derechos humanos, pero que atienda a las necesidades que seguramente tienen –y lo saben con mayor detalle quienes son responsables de los sistemas en las diferentes dependencias públicas–, que pues debemos prevenir, porque, como ya se mencionó múltiples veces, pues, los ataques y los riesgos están ahí y que el contexto va evolucionando día con día; y, a medida que como personas y como instituciones no estemos preparadas para atender esos riesgos, en la práctica, en la operación va a ser muy difícil podernos defender ante cualquier ataque. Muchas gracias, otra vez, y hasta aquí dejo el espacio.

**El secretario diputado Alfonso Pérez Arroyo:** Bien. Gracias, maestro Casanueva. Corresponde la participación al maestro César Contreras González. Él es coordinador de Desarrollo Tecnológico en la Secretaría de Comunicaciones y Transportes.

César Contreras es maestro en administración pública, con especialidad en desarrollo económico y político por la Universidad de Columbia, y en administración de tecnologías de la información por el Tecnológico de Monterrey.

En su cargo anterior colaboró en la admisión permanente de México ante la Organización de las Naciones Unidas, en Nueva York, donde asesoró en las discusiones para la definición y el financiamiento de la Agenda 2030 para el desarrollo sostenible. Asimismo, participó en negociaciones sobre iniciativas de reforma de la ONU, incluyendo la estrategia revisada de tecnologías de la información.

Tome la palabra, maestro César Contreras.

**El ciudadano César Contreras González:** Muchísimas gracias, diputado. Y voy a compartir mi pantalla. Me confirman que la pueden ver, por favor. Perfecto. Muchísimas gracias. Bueno, quiero iniciar agradeciendo la invitación a la Comisión de Ciencia, Tecnología e Innovación de la honorable Cámara de Diputados.

Es para nosotros un gusto tener la oportunidad de compartir la visión de que tenemos en la Secretaría de Comunicaciones y Transportes sobre la ciberseguridad y algunos de los esfuerzos que hemos estado realizado en la materia.

Quisiera comenzar con lo referente a cómo vemos nosotros el desarrollo tecnológico, cómo vemos el sector telecomunicaciones y radiodifusión, porque aquí es donde se insertan de manera muy natural los esfuerzos que hemos estado realizando en ciberseguridad.

Vemos en esta lámina, en la parte izquierda, cinco ejes, que son los ejes que desde el principio de esta administración se identificaron en la Secretaría de Comunicaciones y Transportes como los que van a regir todo el trabajo que se va a hacer en el sector telecomunicaciones y radiodifusión.

Vemos, en la parte izquierda, primero el eje de infraestructura de telecomunicaciones y radiodifusión, como ese elemento habilitador para la generación de las redes y de la conectividad, la cobertura social, el acceso como un elemento para precisamente otorgar a la ciudadanía ese acceso, valga la redundancia, a los servicios de telecomunicaciones y radiodifusión.

Luego un tercer eje, que es el que tiene que ver con el desarrollo de habilidades y capacidades digitales. Esto con el objetivo de poder dotar a los seres humanos, a las personas, a los mexicanos de esas habilidades que permitan sacar el máximo provecho de estos dos componentes adicionales.

Después vemos el eje cuarto, que es el que se centra en el desarrollo tecnológico y en las nuevas tecnologías. Y, por último, un eje que articula la participación interinstitucional, que la comentaba el colega que me antecedió en el uso de la palabra, como un elemento importante de la participación de múltiples actores interesados, y obviamente la evaluación y la identificación del progreso que se está haciendo en la materia.

Me quiero enfocar en el eje cuarto, que es el de desarrollo tecnológico y nuevas tecnologías, por eso los demás los ven sombreados y este lo ven en color vivo, porque el objetivo de este eje es promover el desarrollo tecnológico en diversos campos de las telecomunicaciones y radiodifusión para promover en el país la transformación e inclusión digital.

Y vienen varios elementos aquí del lado derecho que podrán observar, como la identificación de las nuevas tecnologías, el monitorear tendencias tecnológicas, el proponer recomendaciones y mejor prácticas, pero viene un último elemento que es no menos importante y que es de naturaleza transversal, el uso severo irresponsable de las comunicaciones y las tecnologías de la información, que es precisamente el tema que nos convoca el día de hoy.

Vemos que existen muchos esfuerzos a nivel internacional para identificar y medir los avances en ciberseguridad de los diferentes países. Y uno muy reconocido es el Índice Mundial de Ciberseguridad, que genera la Unión Internacional de Telecomunicaciones de la Organización de las Naciones Unidas, que se enfoca en evaluar cinco pilares: las medidas legales, las medidas técnicas, las medidas organizativas, el desarrollo de capacidades y la cooperación como elementos de evaluación para saber en dónde estamos situados como país.

Si nos ponemos a ver, se hace básicamente a través de estos cinco pilares, se redondean todos los, digamos, diferentes actores del ecosistema que tendrían que estar participando. Y precisamente nos da gusto ver que esfuerzos como este, impulsados por el Legislativo, buscan ver desde la trinchera de los diferentes actores qué es lo que debemos de estar promoviendo para mejorar la ciberseguridad, ¿no?

Ahora bien, ¿cómo estamos nosotros situados en el Índice Mundial de Ciberseguridad? Es una medición que se elabora, bueno, se publicó por tercera ocasión en 2018, en 2017 estuvimos en el lugar 28 como país, luego pasamos al 2018 al lugar 63.

Y ahora les platicaré más adelante como parte de mi intervención qué hicimos con respecto a la cuarta integración del Índice Mundial de Ciberseguridad, pero, ¿por qué esto es importante? Porque significa, por un lado, que estamos tal vez quedándonos sin esfuerzos suficientes o no articulándolos de manera adecuada para poder darles la notoriedad suficiente que amerita la ciberseguridad. El ver este rezago que ocurrió en 2017-2018 nos debe de prender las alertas para decir: necesitamos articularnos de una mejor manera, necesitamos impulsar esos compromisos complejos que se necesitan y que hemos buscado desarrollar como país, necesitamos efectivamente hacerlos instrumentales, ¿no?

En ese sentido, en la Secretaría de Comunicaciones y Transportes el tema de la ciberseguridad lo adoptamos de una manera muy comprometida a partir de 2019, fruto el cambio de administración el 1o. de diciembre de 2018, y empezamos con una serie de acciones precisamente para entender cómo es que en el contexto del sector precisamente telecomunicaciones y radiodifusión, que a través de la política pública que generamos estamos buscando esa conectividad, esa adopción de nuevas tecnologías, es importante saber cómo es que tenemos que generar en los usuarios esas habilidades para fomentar su resiliencia.

En ese sentido iniciamos con unas mesas de trabajo el año pasado, las desarrollamos en enero y febrero de 2019, a través de los Centros de Inclusión Digital, que –como muchos de ustedes conocerán– es una red de 32 centros, una en cada entidad federativa y en la Ciudad de México. Y el objetivo de este ejercicio fue identificar cuáles son algunos de los roles y de las conductas en las que incurren los usuarios comunes y corrientes, como son los beneficiarios de los socios de los Centros de Inclusión Digital para entender en cuáles de esas situaciones deberíamos de buscar generar como, digamos, aspectos, líneas de trabajo para fomentar esa concientización.

Las mesas de seguridad agruparon a más de 5 mil usuarios, como les decía, en los Centros de Inclusión Digital, y a raíz de ahí publicamos en marzo de 2019 un estudio con los resultados de dicho ejercicio, que precisamente lo que busca es visibilizar, a nivel incluso entidad federativa, cuáles son las actitudes y las acciones y las conductas de riesgo que los usuarios nos reportaron, para que precisamente ese diagnóstico ayude a orientar esfuerzos, incluso como le decía, a nivel estatal si lo queremos ver así, sobre ciberseguridad.

A partir de ese estudio en el que se resumieron los hallazgos más importantes, desarrollamos un simulador de ciberseguridad, en el que se incluyó una guía, materiales y el software en sí mismo, en que permita a los usuarios de una manera muy interactiva, de una manera muy ágil, muy atractiva, tanto para niños como para adultos en ese formato de caricatura que se ve ahí en la diapositiva, el poder identificar esas actitudes de riesgo, esas acciones, esas conductas de riesgo en las que están incurriendo y conozca los diferentes escenarios que se van planteando dependiendo de las acciones que tomen los usuarios del simulador pueden llevarlos a situaciones no deseadas.

Y al final el propio simulador precisamente en esa búsqueda de crear conciencia sobre los seguros de los servicios, va una especie de recapitulación de los diferentes elementos en los que el usuario actuó de una manera indeseable y cómo es que se provén recomendaciones para evitar esas conductas en el futuro, cuando en realidad ya el usuario este en la vida real y cotidiana. A la fecha tenemos más de 57 mil visitas en el simulador, y ahí viene la liga, la estamos dejando como parte de nuestro interés en socializar este esfuerzo.

Hicimos también como parte de la labor de coordinación, del interés que tenemos en entender el rol que cada uno de los actores tiene en la ciberseguridad, y nosotros particularmente en la Secretaría de Comunicaciones y Transportes, un taller con entidades federativas y representantes de la federación, para discutir una visión, identificar retos en conjunto y proponer soluciones que contribuyan a los planes, de la SCT de entrada como les decía en ciberseguridad, pero que bien pueden ayudar a abonar a los intereses de otras entidades.

El taller lo desarrollamos en marzo de 2019, participaron más de 100 personas representantes de la federación, de las entidades federativas, 26 entidades federativas estuvieron aquí en la Ciudad de México acompañándonos en el taller y participando en el mismo; 14 dependencias de la Administración Pública Federal; un organismo internacional que fue la organización de los Estados Americanos; y un gobierno extranjero, el gobierno del Reino Unido, que fue precisamente el que proveyó los recursos para hacer posible este ejercicio.

Luego, después de eso, con esos hallazgos del taller con entidades federativas de la federación, hicimos al interior de la Secretaría de Comunicaciones y Transportes un ejercicio de priorización para identificar esas líneas más relevantes de ciberseguridad en las que vamos a trabajar en esta administración, y se identificaron temas prioritarios como infraestructura critica en telecomunicaciones y radiodifusión, es decir, esa infraestructura que hace posible que las redes existan, considerando que la ciberseguridad no solamente ocurre en el mundo virtual, sino tiene vínculos al mundo físico a través de esta infraestructura.

La educación en ciberseguidad, es decir, la generación de capacidades, de habilidades de formación de los ciudadanos como usuarios, pero también de la profesionalización de los cuadros que van a ayudar a hacer esa ciberseguridad de proveer soluciones al país. La industria local de ciberseguridad, como precisamente el elemento que nos ayudará a generar nuestras propias soluciones como país para evitar dejar de depender de las soluciones que importamos de otras naciones. Nuevamente la regulación, el marco jurídico, no menos importante, considerando que todo este cambio hacia el mundo digital ha impuesto también ciertos retos a la aplicación de la regulación, y como es importante que el marco jurídico sea amigable y considera la particularidades del mundo digital ¿no?

Algunas acciones que desarrollamos durante la contingencia por Covid-19, hemos mantenido la participación con entes públicos y privados: se mencionaba anteriormente por otro de los participantes el tema del comité especializado en seguridad de la información. Nosotros participamos en la Subsecretaría de Comunicaciones como ente invitada, como un mecanismo de articulación con otras entidades de gobierno, pero también con entes privados en esfuerzos impulsados por la organización de los Estados Americanos como los consejos de innovación en ciberseguridad.

Publicamos también muy al inicio de la declaración de la pandemia, la guía para las familias sobre el uso de las tecnologías de telecomunicaciones y radiodifusión, en las que les damos a las familias mexicanas elementos para que puedan hacer el mejor uso del teléfono, de la televisión abierta, y obviamente, de la conectividad a internet en labores de educación, labores de comunicación, etcétera, y ahí incorporamos elementos de ciberseguridad como nociones básicas que deben de buscar cómo estas medidas de higiene.

Después muy enfocadas ya a ciertos aspectos publicamos en junio y en agosto, las guías de ciberseguridad, primero en apoyo a teletrabajo, luego en apoyo a la educación, considerando que el teletrabajo nos impuso a muchos ciertos retos, sobre todo en aquellos sectores de micro, pequeñas y medianas empresas en donde no existen departamentos responsables de la ciberseguridad de los trabajadores, como es importante que se generara esos lineamientos que ayudaran a los tele trabajadores a poder hacer su trabajo de una manera más segura; y sobre la educación, buscando dar, dotar de elementos a la comunidad educativa, tanto a maestros como a padres de familia y a los propios niños, niñas, jóvenes adolescentes, para poder asumir un mejor uso de estas capacidades.

Integramos también en el contexto de esta contingencia la parte y creación que es a lo que me refería al principio de mi intervención, del índice mundial de ciberseguridad de la Organización de las Naciones Unidas, que haciendo un diagnóstico a través del envío del cuestionario que generó la UIT, Unión Internacional de Telecomunicaciones para este propósito, a diversos actores se integró la respuesta y se mandó a la UIT con el objetivo de tener nosotros una parte de integración del índice que mira de una manera muy autentica los esfuerzos que estamos realizando y tener, digamos, ese termómetro muy bien calibrado para identificar que esfuerzos adicionales se tienen que realizar.

Y por último, hemos continuado la participación en eventos relevantes en los que se impulsa, precisamente, la participación de las mujeres, por ejemplo, en los esfuerzos de ciberseguridad, sabemos que hay muchísimo talento, hay muchísimo interés, uno de esos esfuerzos fue de Cyberwomen Challenge, impulsado por la OEA; otros son los Consejos de Innovación de Ciberseguridad de la misma organización; y la sexta semana nacional de ciberseguridad impulsada, como todos los sabemos, por la Guardia Nacional, entre otros esfuerzos.

Me detengo aquí, sé que ya excedí el tiempo que me habían muy cordialmente regalado, quedo a sus órdenes, está mi nombre, mi correo electrónico, para la comunicación que ustedes gusten que podamos tener. Esta presentación la compartiré para que la puedan circular. Y bueno, quedo a sus órdenes, y nuevamente muy agradecido por la oportunidad.

**El secretario diputado Alfonso Pérez Arroyo:** Gracias, maestro César Contreras. Hoy corresponde el turno al doctor Gabriel Sánchez Pérez, que es doctor en comunicaciones y electrónica en el Instituto Politécnico Nacional. Es miembro del Sistema Nacional de Investigadores del 2017-2018-2019 y 2020. Miembro del Comité Técnico, asesor del Instituto Nacional Electoral. El en 2017 miembro del Comité Estratégico de Seguridad de la Información del Instituto Politécnico Nacional. Del 2016 al 2018, representante del sector académico en las jornadas de Estrategia Nacional de Ciberseguridad México, en la Presidencia de la República.

En el 2018-2019 coordinador académico de la maestría en Ingeniería, Seguridad y Tecnología de la Información del Instituto Politécnico Nacional. Es asesor del titular de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Policía Federal Ministerial, perteneciente a la Fiscalía General de República. Es profesor titular del Instituto Politécnico Nacional. Adelante, doctor Gabriel Sánchez.

**El ciudadano Gabriel Sánchez Pérez:** Muchas gracias, diputado Alfonso Pérez, por su presentación. Saludamos a la diputada Marivel Solís, presidenta de la Comisión de Ciencia, Tecnología e Innovación de la Cámara de Diputados. A la senadora Beatriz Paredes, también un gusto por su aportación al inicio de este trabajo. A la diputada Juanita Guerra, asimismo por la invitación y agradecemos siempre a la diputada María Eugenia Hernández y al diputado Alfonso Pérez Arroyo, por su excelente presentación que nos acaba de hacer a cada uno de nosotros.

A nombre de nuestro director general, el doctor Mario Alberto Rodríguez Casas, director general del Instituto Politécnico Nacional, es que hago esta presentación, solicitada a través de un tópico que consideramos bastante estratégico que es el reto de la formación de capital humano en aspectos de cibeseguridad.

Como ustedes saben el estudio del Instituto Nacional de Ciberseguridad en 2016 hablaba que para 2025 nuestro, el número de personas que necesitaríamos para estar trabajando en las áreas de ciberseguridad estaba alrededor de los 825 mil recursos humanos. El 19 de octubre de 2020, una publicación de… habla de que en el año 2024 necesitaremos 10 millones de profesionistas en áreas de la ciberseguridad. Eso quiere decir que en no más de 4 años se ha exponenciado este requerimiento de recursos en ciberseguridad por lo menos en 10 veces. Eso habla de que la necesidad de generación de capital humano con conocimientos en las áreas de ciberseguridad o seguridad de la información es crucial y sumamente importante.

Se habla también en uno de los trabajos que pública recientemente en el mes de octubre el Foro Económico Mundial, en su trabajo de The Future of Jobs, nos dice que las tres principales áreas de trabajo que se van a tener que incrementar o poner principal atención sobre estos trabajos es el Cloud computing con un incremento del 17 por ciento. Tenemos también el análisis del big data, todos los datos que estamos generando a través de cualquiera de las conexiones que tenemos en el mundo, se incrementa un 2 por ciento.

El… el internet de las cosas que hoy es una cosa sumamente importante y casi fundamental en nuestro trabajo diario con esta pandemia que tenemos, mucho con el teletrabajo o la teleeducación que hacemos todos el día a día, se ha incrementado y la seguridad de los dispositivos pues tiene que ser fundamental. Se ha incrementado en un 9 por ciento.

Pero, un dato revelador es que los datos encriptados y la parte de ciberseguridad se ha incrementado en un 29 por ciento. Entonces, eso quiere decir que el tema que hoy nos aqueja y muy puntualmente abarca la Comisión de Ciencia, Innovación y Tecnología de la Cámara de Diputados es un tema fundamental.

Estos 10 millones de personas, recursos humanos que deben estar trabajando sobre las áreas de ciberseguridad, deberán tener alguna capacitación. Esta capacitación deberá ser como lo han hecho ya en otras latitudes, sobre todo en Europa, escogiendo perfiles idóneos desde los niveles, inclusive elementales como es la educación primaria, después pasando por actividades de la educación secundaria. Una vez que hayan sido detectados estos perfiles o estas personas que tienen habilidades sumamente potenciadas a través del uso de las tecnologías de información, son canalizadas a través de escuelas, ya sean de estudios profesionales o de estudios técnicos en los cuales, pues van a hacer aquellos trabajadores que nos van a estar proviniendo de la tecnología o de la capacidad de administración o de desarrollo tecnológico para estos niveles.

¿Cómo es que nuestro país aborda este tipo de reto fundamentalmente? Bueno, pues podemos hablar de que las universidades importantes de nuestro país, como es la Universidad Nacional, el Instituto Politécnico Nacional, el Instituto Superior de Estudios de Monterrey, el Tecnológico de Monterrey, la Universidad de las Américas en Puebla, la Universidad Iberoamericana, El ITESO en Guadalajara y la Universidad Autónoma de Nuevo León. Han sido estas entidades misionarias, las cuales han puesto recursos humanos, recursos económicos y, sobre todo, aquella visión en la cuales han visto oportunidad para poder presentarle a nuestra comunidad académica, programas desde los niveles de educación básica, en este caso la licenciatura y, algunos otros que hemos trabajado en niveles superiores como es el posgrado.

¿Esto qué nos habla? Que hoy, tenemos al menos un déficit importante en México de generación de recursos humanos. Estos recursos humanos que estamos generando estas universidades que yo ya hice mención hace unos segundos, estamos generando recursos humanos enfocados a la aplicación de la tecnología, enfocados a la parte de ciencia y desarrollo de tecnologías y otros a la parte de la dirección, conducción de estas áreas de ciberseguridad que todas las organizaciones deben tener.

Pero, es importante también decir que, no es suficiente el esfuerzo que estamos realizando. Necesitamos que todas aquellas entidades públicas y privadas que aún no han observado dentro de sus prioridades estratégicas el tener programas en ciberseguridad, creo que es el tiempo expedito hoy, idóneo para poder poner lo que se tiene que hacer para generar más recursos humanos en este aspecto.

Lo decían mis compañeros que me antecedieron en la plática, todos aquellos desde su visión estratégica, Arturo en la parte de bancos, Javier en la parte de seguridad pública, Juan Manuel desde la parte de la perspectiva de las comunidades que son, pues que tienen la voz de la parte pública. César desde el área de gobierno a través de la Secretaría de Comunicaciones y Transportes y todas aquellas diputados y diputadas que han comentado a través de este foro que hoy estamos hablando hoy aquí, podemos decir que, la ciberseguridad es algo que estamos permeado en todas las labores del día a día en nuestras casas, en nuestros trabajos y, en la educación constante para nuestros hijos y nuestros alumnos.

Puedo decir que, la visión estratégica que ha tenido el doctor Mario Alberto Rodríguez Casas al interior del Instituto Politécnico Nacional, aprobando programas de ciberseguridad desde el nivel medio superior, superior y posgrado. Habla de que estamos plenamente convencidos de que esta necesidad de generación de recursos humanos en estas áreas es fundamental.

El apoyo desde la Dirección General de nuestro instituto ha sido pues un pilar para que los laboratorios, los profesores y, pues los estudiantes haya más lugares para poderlos ofertar. Sabemos que el esfuerzo aún realizado es importante, pero debemos de invitar a todos aquellos que no se han sumado a este esfuerzo a poderlo compartir.

Y finalmente, cerrar mi intervención, diciendo que pues todas estas universidades que he mencionado e incluimos la que yo pertenezco, el Instituto Politécnico Nacional, pues siempre estará dispuesta a colaborar con los trabajos que el gobierno federal y los ámbitos tanto legislativos, como en otros órdenes se nos requiera para poder abonar a esta estrategia que hoy firmemente se ve como un camino fundamental, para poder llevar lo que siempre hemos dicho y nuestro lema es, poner siempre la técnica al servicio de la patria. Sería todo y gracias por la invitación.

**El diputado Alfonso Pérez Arroyo:** Gracias, doctor. Pues bien, con esa intervención cerramos el primer panel, pero antes quiero manifestar que ha sido muy interesante sus conocimientos vertidos acá, esto definitivamente coadyuvará para generar políticas públicas y un andamiaje legal más acertado. Agradecemos su intervención y esperamos seguirlos viendo, seguir fortaleciendo el tema este, el de la ciberseguridad. Adelante, diputada.

**La secretaria diputada María Eugenia Hernández Pérez:** Muchas gracias al invitado Alfonso Pérez Arroyo por su moderación en la primera Mesa, estamos sugiriendo que las preguntas a los ponentes se realicen al final de los tres bloques. Entonces, vamos a iniciar ahorita ya con la segunda mesa de trabajo. En este bloque dos nos va a ayudar a moderar Raisa Valda Ampuero que es de Warmi Red y es directora fundadora de esta empresa. Cuenta con más de ocho años de experiencia en proyectos de tecnologías social en Latinoamérica, es becaria del… 2016 y, Datos con Enfoque de Género.

Pues bienvenida Raisa para esta moderación, te cedemos el uso de la voz. Adelante. No sin antes recordar que hay que insistir que las presentaciones son de siete minutos, de favor ¿sí? Muchas gracias y adelante.

**La moderadora Raisa Valda Ampuero:** Muchas gracias, diputada. Muy buenas tardes a todas y todos. Muchas gracias por esta invitación y este espacio. Yo voy a hacer un pequeño repaso de lo que ha estado pasando en Latinoamérica recientemente, como antesala justamente a la charla que tenemos planeada en este bloque, que es ciberseguridad en la región.

Creo que es importante recordar y mencionar un elemento bien importante que se habló en el anterior bloque justamente Juan Manuel Casanueva lo mencionaba, que es el enfoque de derechos humanos. Porque hemos visto revueltas populares, revueltas a nivel Latinoamérica que se han ido sumando, ha empezado Chile, se sumó Ecuador también mi país, Bolivia ha sido parte de todo ese movimiento y creo que es importante analizar todo ese contexto porque ha habido varios elementos que nos tienen que llamar la atención para también comprender que el marco normativo con el que vamos a trabajar pueda por momentos ser desproporcionada con las personas a las que queremos proteger.

Yo revisaba bibliografías, hace poco, poco después de la revuelta popular de Chile hacia el 18 de octubre, más o menos identifiqué un estudio monográfico, lingüístico sobre el discurso del presidente Piñera y como pasaba de temas económicos y medio ambientales y cambiaba su discurso, por ejemplo, hace un aval sobre las fuerzas de seguridad, un discurso de guerra aplicado al espacio público.

Este fenómeno no es ajeno a las revueltas populares dentro de Latinoamérica, vemos que hay una reproducción de la criminalización desde el discurso oficial. En Chile, por ejemplo, a los movimientos movilizados se les ha llamado vándalos, los han llamado… en Bolivia se los ha llamado…, se les ha llamado salvajes y este discurso oficial empieza a permear en la población, empieza a permear en los usuarios de determinadas plataformas de casi todas, y termina justificando también el actuar desproporcionado de las fuerzas del orden. Por ejemplo, con un despliegue de policías y militares, que ya vimos e Ecuador, que lo vimos en Bolivia, también el Chile y en ese ámbito, o sea, los hechos de violencia que ocurren en… que pueden ser las golpizas, el abuso sexual, lesiones, asesinatos, masacres.

También, reproducen otras situaciones no menos complejas, no menos complicadas en el ámbito digital, entendiendo que internet no es un espacio neutral necesariamente y es un espacio donde se promueven ciertos discursos y se dificulta también la promoción de ciertos otros porque no hay una igualdad de condiciones en acceso a internet y en acceso a plataformas.

Entonces, por ejemplo, otra justificación desproporcionada que hemos visto de esta criminalización desde el discurso oficial, en el caso de Chile, por ejemplo, con estos epítetos que se calificaba a los movimientos populares movilizados, el ministro Buñuel, por ejemplo, en algún momento habló de mejorar la inteligencia de la policía. Que básicamente es persecución y seguimiento, ¿no?

Y otros elementos que van ocurriendo en ese sentido, por ejemplo, son por supuesto el mayor presupuesto para Fuerzas Armadas durante la pandemia. Es el caso de mi país, se ha dado mayor presupuesto a fuerzas represivas, a compra de armamentos, más que a atención a temas de salud. En el caso de Chile vimos el uso de drones para aumentar la seguridad -o justificación para aumentar la seguridad- que eso de todas maneras vulnera el derecho de las personas a la manifestación.

Y también el sabido ya monitoreo de redes sociales. Como Manuel hace un momento lo decía, la falta de claridad en estos términos justamente deja demasiado a la interpretación de quienes van a hacer esa vigilancia, estos criterios que se deberían considerar.

En el caso de Bolivia, por ejemplo, en particular con los últimos movimientos durante este gobierno transitorio ha habido encarcelamientos, ha habido judicialización y ha habido persecución política a personas que solamente administraban grupos de Whatsapp porque no existe un marco normativo, porque la observación sobre este tipo de normas y este tipo de protecciones a la privacidad de las personas estaba muy ausente, ¿no?

Entonces, creo que es muy importante tener en cuenta estos escenarios porque hay claramente un viraje ideológico a nivel Latinoamérica que debemos considerar. No solamente se trata de establecer un marco quizá para aquellos escenarios donde hay claras vulneraciones, que es lo que han conversado justamente todos los estimados diputados que me han antecedido, pero también considerar que esta normativa puede por momentos ser desproporcionada con las personas que se movilizan por causas sociales, por causas políticas, por defender una línea política, una línea ideológica, que el hecho en sí no es ilegal.

Entonces, dicho esto, creo que es una buena antesala para empezar a conversar sobre el contexto de ciberseguridad en la región y para ello la primera invitada es Dayanni Olivo, de Directorio Legislativo, de Argentina.

Es directora de análisis político para Centroamérica y el Caribe en Directorio Legislativo. Comunicadora social y periodista especializada en el monitoreo y seguimiento de políticas públicas y regulatorias en los poderes Ejecutivos, Legislativos de América Latina y el Caribe. Es maestrante en Comunicación social y periodismo, de la UNLP de Argentina. Diplomada en Control social y gestión pública para la… distrital y corresponsal de guerra de las Fuerzas Militares de Colombia. Adelante, Dayanni. Dayanni, ¿está conectada? Hola, Dayanni, ¿estás conectada?

**La señora Dayanni Olivo:** Ahí estás, ¿ahora sí? Perfecto, okey. Bueno, arranco entonces de vuelta porque veo que hay un problema técnico de conexión. Raisa, gracias por la invitación. Gracias a la Cámara de Diputados de México, a los senadores y diputados presentes. Y a cada uno por la invitación y la participación a este evento.

Nosotros les vamos a compartir y vamos a hacer un breve recorrido por la región para analizar cómo está el panorama regulatorio. Vamos a ver el origen de algunos proyectos de ley que se han presentado y que están vigentes hoy en los congresos de América Latina y el Caribe. ¿Qué grado de avance tienen estos proyectos de ley? ¿Cuáles son los actores de referencia y los actores de incidencia? Y vamos a analizar un poco -y de manera breve porque el tiempo apremia- cuál es el contenido de esos proyectos de ley. Así que voy a compartirles pantalla para que podamos iniciar. ¿Me confirman que están viendo mi pantalla?

**La señora Raisa Valda Ampuero:** Sí, adelante.

¿Sí? ¿Estamos? Perfecto. Bueno, para empezar, contarles un poco cómo estamos hoy en la región porque venimos debatiendo bastante sobre el tema de ciberseguridad pero también es interesante ver a nivel del Poder Ejecutivo y a nivel del Poder Legislativo qué iniciativas están vigentes y cuál es el camino que hoy a nivel regulatorio se sigue desde el Poder Ejecutivo y desde el Poder Legislativo.

**La señora Dayanni Olivo:** Lo que nosotros hicimos para poder armar esta presentación, este breve panorama que les vamos a compartir es analizar 22 países de la región. Y lo que hicimos fue verificar si hay proyectos de ley o no vigentes en los congresos y analizar cuáles son las estrategias nacionales sobre defensa y ciberseguridad que se han presentado en cada uno de esos proyectos de ley.

Y encontramos algunos puntos que son interesantes. De los 22 países que revisamos… encontramos que actualmente tienen proyectos de ley vigentes sobre temas de ciberseguridad, como lo son Costa Rica, Honduras, Nicaragua, Colombia, Ecuador, Perú, Argentina, Chile, Uruguay, Bolivia, Paraguay, Brasil, El Salvador y México. Estos países tienen actualmente en sus congresos normativas que buscan de alguna manera regular el tema de ciberseguridad.

Obviamente aquí hay un debate al que no hemos entrado y por tiempo no podemos entrar a analizar el contenido de cada uno de esos proyectos de ley y quizás la pertinencia y la profundidad de esas iniciativas. Pero sí es importante que son congresos que actualmente tienen en sus agendas una iniciativa regulatoria para poder avanzar en una normativa sobre el tema.

También encontramos otro tipo de países, como lo son Jamaica, República Dominicana, Trinidad y Tobago, Panamá y Guatemala, que son países que actualmente no tienen en sus congresos proyectos de ley vigentes sobre temas de ciberseguridad, pero sí tienen una estrategia nacional de ciberseguridad.

Y por lo general lo que nosotros encontramos -y esto lo podemos manejar como una tendencia- es que desde el Poder Ejecutivo muchos de los países han avanzado en el desarrollo y en la implementación de estrategias nacionales. En algunos casos marcan como una hoja de ruta para que a partir de esas estrategias nacionales los congresos puedan empezar a emitir legislaciones específicas que puedan regular lo que se ha establecido desde el poder Ejecutivo.

Y hay otros países que están un poquito más avanzados. Son aquellos que ven en pantalla, que tienen una estrellita como indicador y son países que actualmente cuenta con una estrategia nacional de ciberseguridad. Y además de contar con esta estrategia nacional también tienen en sus congresos proyectos de ley para regular este tema. Entonces, este tercer grupo -si se quiere- son países que están quizás un paso más adelantado o más avanzado que algunos otros países en los cuales ni siquiera se tiene una estrategia nacional de ciberseguridad.

En este tercer grupo nosotros encontramos países como Colombia, Brasil, Paraguay y Chile. Eso para tener un panorama general de hoy cómo está la región en un tema normativo y cuáles países hoy tienen iniciativas vigentes sobre ciberseguridad. También es interesante analizar de dónde provienen esos proyectos de ley y esas iniciativas. En este gráfico tenemos dos partes, una primera parte que hace referencia al origen y una segunda parte que hace referencia al estado de esos proyectos de ley.

El origen en su gran mayoría de los proyectos de ley que hoy están vigentes corresponden al Poder Legislativo y ahora más adelante vamos a ver por qué corresponden al Poder Legislativo. Hay una razón que tiende a ser que sea mucho más fácil en algunos casos que desde los gobiernos se avance de manera más rápida en una normativa integral que dejar esta tarea al Poder Legislativo de cada uno de los países. Y en otros casos el origen proviene del Poder Legislativo.

Entonces, de este mundo de iniciativas que tenemos hoy vigentes en los congresos encontramos que en mayor medida son iniciativas que provienen directamente como una idea de los legisladores y en un segundo caso iniciativas que provienen directamente del Poder Ejecutivo.

Y por lo general aquí cuando hablamos de Poder Ejecutivo no se habla de proyectos de ley como tal, no son leyes marco sobre ciberseguridad donde se busque regular de manera integral el tema, sino son el algunos casos convenios internacionales que el país ha suscrito con otro país y es necesaria su ratificación y su aprobación  en el Congreso.

Entonces, algunos de estos -en el caso del Poder Ejecutivo- refieren a esto. Que no son de menor importancia; todo lo contrario, lo que el empezó, importante también, porque permite que a partir de la ratificación de esos convenios internacionales se avance en las mas específicas.

¿Cuál es el… de esos proyectos de ley hoy en la región? Tenemos tres estados, la gran mayoría de proyectos de ley están hoy en comisión, son proyectos que están quietos, hay intenciones fijas sin avanzar, en trabajar y en estudiar, pero están ahí, en comisión.

Hay un tanto más de proyectos, tres proyecto de los de este mundo, del que anunciábamos, del que les contaba eran 20 proyectos de ley en total, los encontrábamos en toda la región, encontramos que tres de ellos están hoy listos para ser votados en un plenario y acá en algunos casos obviamente, entra el matiz de que tenemos en la región congresos que son bicamerales y otros unicamerales, que en este caso, pueden permitir que la aprobación de estos proyectos de ley sea más rápida o menor, no es lo mismo un proyecto de ley que necesita la ratificación en una sola Cámara a un proyecto de ley que tiene que pasar a una Cámara revisora o a una segunda instancia donde ese proceso puede llegar a tardar o a retrasar más un tratamiento dentro del Congreso.

Y, tenemos otro grupo de proyectos que está actualmente sancionado y que está en espera de promulgación, uno de esos es en el caso de Colombia, es una ley especifica sobre ciberseguridad, pero sí es una ley que apañe a uno de los tantos temas que se derivan de ciberseguridad.

¿Cuáles son los factores que se toman como referencia?, y ¿cuáles son los factores que inciden en los proyectos de ley que hoy están presentados en la región. Tenemos distintos actores de referencia ¿no?, y una de las razones principales que hace que hoy haya una preocupación a nivel legislativo y a nivel ejecutivo en avanzar en estas iniciativas, obviamente, es el avance rápido de la tecnología de internet y la regulación siguiente ¿no?, esa es una de las principales razones que hace que se promuevan distintas normativas regionales, pero detrás de esto también hay actores de referencia que se toman como modelo para poder impulsar, sostener o fundamentar estas iniciativas –acá en la pantalla lo podrán ver– algunos… no son… todos… una enumeración exhaustiva, seguramente que hay muchos más y que por tiempo, obviamente, no podemos profundizar, pero los organismos sobre las ideas o planes que se toman como referencia son la Estrategia Interamericana Integral de Seguridad Cibernética.

La agenda sobre ciberseguridad global, también, que impulsa la Organización de las Naciones Unidas, acá en particular encontramos también la Agenda 20-30, para el Desarrollo Sostenible, el objetivo 9, es algo de los, es uno de los objetivos que más se cita.

Por ejemplo, en los proyectos de ley analizados, los convenios internacionales y acá quizá hacemos mención al convenio de Budapest, como uno de los tantos convenios a nivel nacional de los cuales 8 países, 6 de la región ya están adheridos a este convenio, otros están en proceso de adhesión, pero los convenios internacionales también son parte del fundamento que se toma y que toman los legisladores como referencia para poder impulsar este tipo de iniciativas y estudios de gobernanza pública de la OCDE, entre otros.

No es como le decía, exhaustivo, hay una lista muchísimo más grande, pero en los proyectos de ley que nosotros analizamos en este relevamiento encontramos que estos son algunos de los actores que… en los cuales se sustentan estas iniciativas.

¿Qué tipos de proyecto de ley encontramos? Y acá, vamos a ver un poco del contenido, ¿no?, de lo que hay hoy en la región a nivel legislativo y a nivel normativo. Por un lado, tenemos leyes marco, ¿no?, y en estas leyes marco encontramos que hay países como México, como Honduras o como Perú, que tienen actualmente vigente en sus congresos proyectos de ley que buscan oponer, crear una ley que dé un… general, que no se enfoque solamente en un tema específico sobre ciberseguridad, sino en general.

Obviamente que acá nosotros le compartimos acerca de los tipos de proyectos que hay, sin entrar en el contenido especifico de cada uno de ellos, porque dentro de esta ley es marcos, como les decía al comienzo, no podemos entrar a revisar ahora por tiempo la pertinencia o no, tomemos como referencia la intención para avanzar en este tipo de iniciativas.

Así que, bueno, encontramos, por un lado, leyes marco que es en menor medida. Por otro lado, encontramos normativas especificas y acá citas donde será la mayor cantidad de proyectos de ley que hoy tenemos en la región.

Son proyectos que buscan regular un tema específico, no abarcan como tal a la ciberseguridad, no toman un marco general, sino que, toman cuestiones especificas y… cómo es el caso de Chile y Colombia que actualmente tienen proyectos de ley en sus congresos para… en la tipificación, en la definición de lo que son los delitos informáticos.

Está, también, el tema de los datos personales y acá podemos hacer referencia en Nicaragua, en cuyo caso, además de proponer regulaciones especificas para datos personales, encontramos que hay países como Ecuador que van un poquitito más allá y buscan regular los datos personales, crediticios y de salud.

El acoso cibernético también es otro de los temas que está hoy en la agenda, en este caso podemos mencionar a Costa Rica, que tiene hoy un proyecto de ley vigente sobre este tema.

Proyectos de ley sobre defensa del consumidor, es otro de los temas que hay dentro de las normativas específicas y acá, a veces, se dan defensa del consumidor a nivel general, sin entrar específicamente a topar algún tema o se da defensa del consumidor en temas específicos como es el caso de Colombia, por ejemplo, lo que tiene que ver a comercio electrónico. Y, un punto más que encontramos en estas normativas analizadas es la discriminación en red, como es el caso de Honduras.

En un tercer nivel de equipos de proyectos de ley, encontramos que hay una actualización normativa, y en este grupo se encuentran países como México, Perú, Chile, Colombia, Costa Rica y Brasil y acá, se apunta más que a proponer un marco general, actualizar las normativas que hoy existen y quizás una de las razones por las cuales se apunta a esto es porque es más fácil en algunos caso y en algunas legislaturas avanzar de una manera mínima, actualizando la normativa que hoy existe, que lanzándose a regular de manera general e integral una normativa.

Y, encontramos un cuarto nivel que son otros tipos de proyecto de ley que hacen referencia a aquellos países que buscan crear institucionalidad y este tipo de proyectos de ley lo que proponen es específicamente crear organismos, algunos dependientes del Estado, otros sin trabajo con distintos sectores, sector público para avanzar en políticas públicas, en normativas o en distintas regulaciones.

Bien, sea desde el ámbito del Poder Ejecutivo, o bien sea desde el ámbito Legislativo o sea un trabajo mancomunado con distintos sectores, acá también le encontramos una gran cantidad de proyectos de ley en Argentina, México, por ejemplo, Costa Rica, Honduras, El Salvador, Ecuador, Perú y Colombia.

Así que, en términos generales ese es un poco el panorama donde estamos en la región y para cerrar algunas consideraciones finales, la primera es que presenciamos, estamos ante un escenario que nos ofrece un proceso insuficiente y… en materia de regulación, ineficiente, justamente por la disparidad que hay en América Latina y en cada uno de los países y los avances.

Lo veíamos al comienzo en la primera diapositiva, ¿no?, mientras algunos países ya tienen implementado o están avanzando hacía una estrategia… de ciberseguridad, hay algunos otros países que ni siquiera han dado en algunos de sus Congresos o si puede de sus Poderes Ejecutivos, están trabajando para desarrollar una estrategia nacional de ciberseguridad. Quizás esa es una de las primeras conclusiones que podemos dar a partir de este análisis.

Encontramos, también, que hay un avance reactivo y no proactivo en la legislación, tampoco lo veíamos, bloque número uno, nos compartían acerca de como distintos ataques se han dado en distintos países y que a partir de que sucede esto es que se activa la regulación por que quedan expuestas la debilidad y la fragilidad normativa en la que estamos muchos de los países. Entonces, eso hace que tengamos que salir a regular algo que se… y no estaba regulado.

Una tercera consideración es que, encontramos que hay un avance en… de iniciativas especificas y no integrales en los Congresos de la región y este responde, por un lado… es más fácil desde el proceso legislativo avanzar en lo específico que avanzar en lo integral, ¿no? Estoy por el consenso y la capacidad de negociación que sea a nivel interno entre las fuerzas cuando se necesita avanzar en algo, un tema específico y, por eso, aquí encontramos una cuarta consideración que va muy relacionada a la anterior y es que, ante la dificultad que a veces se presenta en los congresos de poder avanzar y las agendas tan distintas que tiene cada uno de los congresos. Los Poderes Ejecutivos deciden avanzar en un marco normativo más integral o deciden establecer una hoja de ruta general que después da paso y permite que los Poderes Legislativos puedan ir avanzando en iniciativas más específicas.

Y un último punto que podemos tomar como una consideración de este análisis es que el tema de ciberseguridad está en agenda, pero no en todos los países es un tema prioritario y en este último tiempo quizá un poco el tema de la pandemia nos ha podido. En poco meses hubo un avance progresivo y exponencial en muchos casos, antes las clases no eran digitales y de repente nos encontramos todos de alguna manera haciéndolo todo de manera digital.

Entonces, fue un salto muy elevado y eso de algún modo influyó para que se fueran poniendo en agenda este tema, pero no aún así logró ser un tema que sea hoy prioridad en todos los congresos de la región. Algunos de los países que han tenido…

**La moderadora Raisa Valda Ampuero:** Perdona que te interrumpa, pero hemos excedido el tiempo hace bastante ya. Te pediría que cerremos el punto para dar paso a la siguiente intervención.

**La ciudadana Dayanni Olivo:** Perfecto Raisa. Lo último, ya estábamos cerrando con esto. Un tema que está en agenda, pero es una prioridad y acá solamente para finalizar, alguno de los países que han tenido avances en esta son Nicaragua, Colombia, El Salvador, Perú, Uruguay, son países que en el último tiempo han tenido presentación de proyectos de ley sobre el tema o algún tratamiento en comisión o avance en concreto de sus proyectos de ley.

Para el caso de Paraguay, Colombia o Perú, también son países que van avanzando, quizá no con la misma celeridad que otros, pero son algunos de los países que hoy registran algún avance. Así que bueno, con eso estaríamos. Muchas gracias.

**La moderadora Raisa Valda Ampuero:** Gracias Dayani. Solamente recordar al resto de los panelistas invitados que el tiempo que tenemos es solamente de siete minutos para que podamos nadar la posibilidad de que todas y todos puedan exponer sus puntos.

A continuación está Susana Soto. Susana bienvenida. Ella es docente especializada en tecnologías digitales y procesos de generación de capacidades para la ciudadanía, es cofundadora y directora de proyectos de Abriendo Datos Costa Rica, organización de la sociedad civil dedicada a la promoción e implementación de iniciativas de apertura de información y datos públicos y la Red Ciudadana por un Gobierno Abierto.

Es también miembro de la Comisión Nacional de Datos Abiertos Costa Rica y el Consejo Constructivo de la Política Nacional de Ciberseguridad. Bienvenida Susana. Adelante, por favor.

**La ciudadana Susana Soto:** Buenas tardes, es un gusto estar acá. Muchísimas gracias Raisa, pero ante todo muchas gracias a las señoras y señores diputados. Esta iniciativa realmente es muy valiosa, es muy importante y me siento muy honrada por esta invitación, gracias por este espacio. Voy a procurar aterrizar y ser muy respetuosa del tiempo, así que si voy un poco rápido me disculpo, pero hay muchas cosas que ya las personas que me han antecedido han señalado y yo quizá voy a tomar algunas cosas para profundizarlas, pero hasta ahí.

Quiero comenzar con lo que señalaba Dayanni, con lo de la diversidad, de las leyes o de los proyectos de ley que en este momento, porque es un elemento más allá de las leyes, es un elemento que nos une como región y esas diversidad está a … de desarrollo en políticas, en estrategias, en leyes. Así es que cuando nos piden el reto de hablar de la región, pues nos enfrentamos a un marco muy difícil.

Yo me voy a supeditar a hablar un poco de la experiencia de Costa Rica y de algunos elementos muy generales a nivel de que nos puedan ayudar a todas y a todos en este tema. También recordar que esa diversidad incluye una gran cantidad de asimetrías y detrás de esas asimetrías, detrás de las leyes, detrás de la ciberseguridad están las personas. Ya Juan Manuel lo decía hace rato, tenemos que pensar y colocar a la persona en el centro y yo lo que voy a conversar voy en ese sentido.

Quiero hablar, desde mi punto de vista, de la ciberseguridad y desde una dimensión más política y humana, creo que como ya lo han señalado otras personas, este concepto … nos ha traído a la realidad en ese sentido. El quédate en casa ha traído también que haya llegado a la casa el riesgo de la ciberseguridad y que antes tal vez algunas poblaciones tenían más difuso, no les atañía tanto.

Al menos aquí en Costa Rica se ha desatado el temor a la ciberdelincuencia específica y más micro por decirlo así, más dirigida a la persona, al ciudadano y a la ciudadana común, a la persona de día a día ha luchado tanto a grandes ataques corporativos, sino que ha ido al menudeo, como decimos aquí en Costa Rica. Entonces, esto pone más énfasis en la necesidad de que vayamos y nos concentremos en eso, en la persona y en el enfoque de derechos.

El área de servicios digitales nos ha tenido que poner expuestos y desde los niños y las niñas que están expuestos al contacto diario, que ha acelerado y en cierto sentido ha sido positivo, porque ha acelerado, como dice por ahí un chiste que anda dando vueltas, ¿quien es el motor de la digitalización y de transformación digital en este momento? La pandemia. Entonces, en ese enfoque debemos de pensar en la ciberseguridad en algo más allá de los …, de los centros de respuesta, más allá de los grandes ciberataques y pensar en una estrategia más integral.

Costa Rica cuando creó la estrategia de ciberseguridad que tiene en este momento, que está llena de deficiencias y de áreas por mejorar, sí tuvimos esa oportunidad, apoyamos por la OEA, de generar a partir de un proceso con participación del actor, como señalaba también Juan Manuel, y un proceso … de mesas, de talleres, no tenemos nada a como comenzamos. Y de talleres, creo que era el señor Contreras quien lo mencionaba, que habían tenido una dinámica similar.

Eso le da gran riqueza porque la misión de todos los sectores y la misión de la persona que no tiene conocimiento tecnológico, pero que puede aportar su ciencia cotidiana con la tecnología es fundamental en este sentido. Lo escuchaba ahora que César señalaba y que ellos también han tenido un proceso muy construido, muy rico, muy alimentado y eso es fundamental. Es fundamental que nuestras leyes pasen por eres proceso y no se nos tiene que olvidar, pero ese es el tema que nos trae hoy.

Otro punto importante cuando vamos a hablar de ciberseguridad en el enfoque de derechos humanos es pensar en que nuestras legislaciones tienen que saber, o sea, la construcción de la legislación tiene que tener en cuenta que tenemos muchos vacíos de respaldo, como lo llamo yo, vacíos de fondos, que nuestra región tiene grandes vacíos. Entramos tarde en este juego tecnológico y el que entre tarde entra perdiendo.

Entonces, tenemos que saber qué hay capacidades instaladas y cuando hablamos de educación no solo la formación, que guíen lo decía también el maestro que habló sobre la educación y decía que hay que formar profesionales, pero también hay carencias de formación más atrás y más fundamentales. En esto tenemos brechas digitales, brechas de acceso que nos ponen en amplia ventaja o con … ventaja a poblaciones que son más sensibles a los ataques de toda índole.

Ya mencionaron la pornografía infantil, pero esa, ojalá, fuera la única amenaza que tenemos ahora en la población menores de edad. Ojalá fuera sola esa la única. Hay amenazas fuertísimas como el … y grandes riesgos que tenemos allí. El enfoque de género en el periódico, hay poblaciones más expuestas y hay poblaciones con menores capacidades para defenderse en este mundo y tenemos que tenerlas en cuenta.

Y algo muy importante que creo que también lo mencionaba Raisa al inicio, es saber que es tener esa visión y a la hora de hacer la ley, de pensar la ley, de conversarla, tener la visión de que a fin de cuentas sigue, el mundo virtual no es un mundo separado del análogo, no es un mundo separado del físico. La virtualidad es una dimensión en donde todo lo que existe en el mío no físico viene … también, es solamente un ámbito más en el que nos desenvolvemos. Eso tenemos que tenerlo en cuenta, porque muchas cosas se pueden facilitar , como lo mencionaba…, con adaptaciones a las leyes o cosas que ya están y ya están en los códigos penales, en los códigos civiles y poder traerlos acá.

Se me está acabando el tiempo, les voy a robar solamente un par de minutitos para un punto que no quiero que se me quede. En esto de los delitos, les decía, como hay grandes vacíos tenemos que pensar en que la legislación que se cree esté vinculada a otras legislaciones con protección de datos, que tengamos esa revisión, que tenga esa coherencia y ese armado de que podamos tener una red de respaldo, una Red Formativa de Respaldo, y que esté respaldada también por cosas de base.

Quiero sellar con el tema de recordar que las leyes también tienen que prever que el Estado, si hablamos de derechos humanos, el Estado es …, es un garante de los derechos humanos, entonces, eso le confiere un rol muy fuerte, en donde, no solo hay que prever sanciones para el que se imprime en la ley, sino que también hay que prever mecanismos de protección para las personas que son objeto de los derechos humanos.

Lo pueden hacer… cuando hablamos de empresas y la gente tiene y a veces del mismo Estado escuchamos el discurso de… pero a la gente no le importa darle los datos a equis empresa, a la gente no le importa dar el porqué nos reclaman a nosotros, porque reclaman por una recolección de arte. Es que es diferente.

Cuando yo entregó los datos o cuando me salgo o soy víctima a partir de una violación de los derechos desde una empresa, en primer lugar, yo di un consentimiento. Ahora, hay mucho tomado en juicio allá atrás y no voy a dejar… tienen que ser más informados, tienen que ser… pero hay diferente. Estoy en una relación diferente que en la que estoy con el Estado, en la que entrego mis datos para poder ejercer mi ciudadanía.

Yo entre con mis datos como un requisito obligatorio para ser una persona ciudadana y para ser persona que recibe servicios esenciales del Estado, además, el Estado tiene un… de garante que no puede infringir. Es algo que, son el toque que yo quisiera dejar sentado sobre la mesa a la hora de pensar en legislación, como bien, lo decía Clarisa, quienes puedan proteger y no exponer más hacía estas generaciones.

Hay mucho más de qué hablar y me encantaría poder tener sistema para siete minutos, pero espero que las cosas que estoy aquí dejando asentadas y parecer respetuosa al tiempo de las personas que están en esta mesa voy a dejar, espero que estos temas nos dejen ahí como espinitas para pensar más allá. Muchísimas gracias.

**La moderadora Raisa Valda Ampuero**: Muchas gracias, Susana. Gracias por tus apreciaciones y para dar continuidad ahora es el turno de Maricarmen Sequera, desde Paraguay. Maricarmen es abogada, con especialización en temas de tecnopolítica y ciberseguridad, también es directora ejecutiva de la UNGTEDIC, organización sin fines de lucro que defiende y promociona los derechos digitales en Paraguay.

Bienvenida Maricarmen, que gusto. Adelante, por favor. Siete minutos, también.

**La exponente Maricarmen Sequera Buzarquis:** Muchas gracias, Raiza. Muy contenta de ver a muchísima gente conocida acá. Bueno… ya en la Cámara de Diputados.

Bien, creo que voy a estar como casi repitiendo ya lo que en parte Susana, ya ha dicho, pero dando un contexto como más local, donde tiene que ver con que países como el nuestro, como Paraguay, como… un país pequeño, pero con pocos recursos hace que esto sea todo un… ¿no?

Entonces, me gustaría como contar un poco la experiencia que se va en todos los países con el apoyo de la OEA, comúnmente, donde nace en el año 2016, un poco más antiguas a todas las nuevas formas de creación de los planes en ciberseguridad y el proceso fue bastante interesante, pero, que también tuvo que tener varios desafíos para…

**El enlace técnico Daniel Ibarra:** Maricarmen, un favor. Casi no se te escucha.

**La exponente Maricarmen Sequera Buzarquis:** Déjame ver… salida…

**El enlace técnico Daniel Ibarra:** No sé si te puedas acercas más.

**La exponente Maricarmen Sequera Buzarquis:** Es que, no creo que pase por el… déjame ver, quizás tenga que ver con una configuración de… porque mi salida está… ahora. Ahí está. Hola…

**El enlace técnico Daniel Ibarra:** Ahí está perfecto.

**La exponente Maricarmen Sequera Buzarquis:** Ah, okey, perfecto. Sí era la salida de mi… un segundo. Bien, entonces, como contadora, ¿verdad?, de la experiencia que tenemos en Paraguay tiene que ver físicamente con, en apoyo de la OEA en el año 2016 con una agenda que recién empezaba en América Latina despues de Colombia, Paraguay había implementado y luego con una experiencia híbrida no con la metodología multitech holding, si ya tenía todos los actores multitech holding, hubo situaciones bastantes complejas, en el sentido, de que si bien agrupaba a todo el equipo o a toda la diversidad de parte interesada, lo que hacía era que la sociedad civil se juntaba con la sociedad civil y su genial Estado, o lo recomendaban el Estado en partes del ahorrador del plan.

Eso significo que gran parte de las partes no tuvieron un intercambio o no tuvimos un intercambio real para poder discutir cuáles realmente serían las prioridades. Por otro lado, también tiene que ver con casi encajonados ejes estratégicos que eso se repinta en todos los planes de ciberseguridad, uno que tiene que ver con una estandarización, pero también con fallas de aplicación en contextuales, ¿no?, que si bien, se agrupaban esos bloques, creemos que es desde un contexto local no se podía cumplir con… con relación a ciertos conceptos como que es conceptos culturales o vía digital y cultural, ¿no? Entonces, había cosas que se emitían antes…

Sin contar que el camino de ciberseguridad ha sido bastante controversial, aparte de la sociedad civil y técnica, también sugerida como eje temático cambiar la seguridad digital donde sí hay un concepto y claridad con relación a la aplicación. Pero, bueno, viendo esto, una tendencia global también, sin mucha definición se aplica un plan con estos términos, ¿no?

En parte también de algunas de las recomendaciones que se dieron, pero que no se pudieron tomar en cuenta por contextos bastantes complejos, tiene que ver con que el enfoque se sentó en la protección, obviamente, infraestructura de los… eso sí, en toda América Latina también y no necesariamente la protección de las personas, de las personas que están detrás de esos datos, verdad, eso ya lo dice Juan Manuel y también Susana y otras personas que anteceden, porque tiene una mirada bastante estructural y en algunos casos casi militarizados, como el caso de Colombia que en parte también forma parte de este tipo de mesas y liberadas por el Ministerio de Defensa.

Y, uno de los temas muy importantes en el momento de la aplicación o desarrollo de un plan nacional, es cuando se habla de educación no sé… era un plan específico para grupos específicos, estamos hablando de planes exclusivamente con enfoque de género, como ya decía Susana, muy importante trabajar con la mitad de una población que eran mujeres, por un lado y, por otro lado, un grupo en situación de vulnerabilidad, donde el acceso a internet y las formas de utilizar internet es muy distinta.

Significa que en ciberseguridad estamos hablando también de un ejercicio viendo no solamente el derecho a la privacidad con relación a un tratamiento de datos personales de un sector público, de un sector privado que muchas de ellas son muchas responsabilidades en cuanto a la aplicación de tratamiento de datos personales, sino también el ejercicio pleno de libertad de expresión.

Estamos hablando de un grupo vulnerable, comunidades LGTB o mujeres que cuando ingresan a internet no pueden hablar de otros temas, verdad, temas físicamente políticos, porque obviamente la agresividad y la violencia digital de género que se traslada, obviamente, a internet, implica que estas personas no puedan utilizar ni ejercer plenamente sus derechos. Estamos hablando de una ausencia de aplicación en temas de desenfoque en el plan de ciberseguridad.

Después de una… implementación, estamos hablando de 2016 ya 2020, casi cuatro años, de una etapa casi final de los primeros 3 años de aplicación del plan, se demostró que, bueno, muchas debilidades. En primer lugar, en la pantalla de recursos para la implementación del plan, el plan es ambicioso, pero, acá se encontraron varios problemas con relación a la implementación en cuanto a costos.

Por otro lado, también, siempre se centró –como decíamos–, en la infraestructura, entonces los ministerios o instituciones del Estado creían que solamente su equipo tecnológico tenían que estar en esas mesas de reunión para poder aprender sobre temas de seguridad, digital, de toda la administración pública y, por otro lado, en países como el nuestro, como hablaba, es un país pequeño con muchas desigualdades, eso significa que hay muy poca investigación académica con relación a el acceso, uso de internet más allá de los indicadores internacionales que existen.

Entonces, estamos hablando de que no hay evidencias locales, análisis sociales y jurídico con relación a cómo está población se está conectando y cuáles son las garantías que tiene como población para poder ejercer, plenamente es un derecho.

Y, por otro lado, cuando ya se estaba cerrando el plan también se mostró que no había realmente métricas reales para poder analizar sí había avances o no con relación al plan. Entonces, cuando llegó a la etapa de evaluación se evidenció el… de… por supuesto y, realmente, ante una ausencia de reglamentación de la implementación de manera transversal en todas las instituciones a nivel nacional, eso sí denunció y se dieron por sentados que una actividad o dos actividades o cinco actividades cumplían dentro de los compromisos, se daban por satisfecha, ¿verdad?, los compromisos que estaban dentro del plan.

Entonces, es muy importante trabajar en las métricas, también analizar cómo esa gente que estuvo participando de estas actividades realmente impacto a mediano y largo plazo este tipo de talleres y que fue el aprendizaje ¿no?

Por otro lado, como la… política de ciberseguridad, cuando hablamos de… Roy del Estado, que vino a regular los estándares para que un sector privado tenga las reglas claras de cómo trabajar y tratar los datos personales de sus clientes en este caso.

Entonces, es muy importante cuando hablamos de planes de ciberseguridad, el rol no debe caer en que el ciudadano debe conocerte más de cómo protegerse en internet que esa aplicación cumpla los estándares de tratamiento de datos personales y quien proteja mi privacidad y que yo tenga que aprender, no sé, a tener una capacidad de habilidades de estar a casi la última tecnología para proteger mis derechos en lugar de que realmente darle la responsabilidad a los creadores de estos tipos de servicios a través de tecnológicos, no tanto que sean del sector público o privado.

En estos momentos, el Ministerio de Tecnología en Paraguay, con un préstamo del BID, está aplicando, está implementando la agenda digital con 130 millones de dólares, está una implantación que se hará en los próximos cinco años, quizás con un poco más de prórroga. Eso significa que hay, en este momento, recursos como para pensar de manera más integral, ciertas soluciones con relación con el plan de ciberseguridad y que es muy interesante porque también lo plantea desde el lado de trabajo más de inclusión digital ¿no? que es un tema que también es transversal a temas de ciberseguridad.

En el marco de estas acciones creemos que es interesante ¿verdad? Como decía, ya para ir cerrando el enfoque de ciberseguridad también es de pensar que el enfoque de ciberseguridad debe estar  intrínsecamente temas de derechos, también temas de accesibilidad, apertura y múltiples interesadas en todo el proceso, no solamente en la creación del plan, sino también en la implementación y por supuesto, en definir los planes de definir los planes de evaluación y qué es lo que se va a estar evaluando dentro de los indicadores.

En ese sentido, también me gustaría resaltar la importancia de la Unesco en el desarrollo de los indicadores universales de internet que desarrolló justamente, no una suerte de *ranking*, pero sí una suerte de cómo visualizar desde dónde deben de ir las políticas públicas para que haya una mejor conexión entre los derechos y la tecnología basado en los estándares de… estamos hablando de derechos, economías, sociedad, cultura y medio ambiente.

Y para ir terminando, si bien hay demasiados esfuerzos a nivel nacional y también regional. Es muy importante que creo que con el tiempo también explicar que las políticas de ciberseguridad den ser políticas que todas las instituciones lo están planteando cuando… nuestras vidas, nuestros servicios de internet.

Entonces, sobre todo buscando soluciones no tecnosolucionistas, sino también como decíamos, siempre basados en la persona y de también en los contextos locales. Y en un caso que vamos a estar lanzando en el próximo mes de noviembre, junto al Ministerio de Salud Pública y al Ministerio de Tecnología de Paraguay… campaña sobre salud mental en internet en tiempos de pandemia.

Con eso, queremos evidenciar que, en temas de ciberseguridad, también se pueden plantear estos aspectos ¿verdad? Que son muy importante dejar en claro cuán expuesto y cuantas interconexiones estamos teniendo en internet y cómo esto implica en cuanto lo que es la salud, en cuanto lo que es un diseño de una tecnología que privacidad por diseño y otras como afectan para pensamientos psicológicos en el día a día.

Así que, creo que nos encontramos con estos desafíos justamente, permear estos discursos de ciberseguridad en políticas públicas que ya las instituciones lo tenían y no sabían, porque creen que simplemente está enfocado en sus departamentos de tecnología y de seguridad de infraestructura y aquí me quedo. Muchísimas gracias.

**La moderadora Raisa Valda Ampuero:** Muchas gracias, Maricarmen has dado puntos muy interesantes que ciertamente aportan bastante al debate. Ahora damos la palabra a Juan Manuel Aguilar, desde México con quien cerramos este segundo bloque.

Juan Manuel estudió Relaciones Internacionales en la Facultad Superior de Estudios Aragón 2008-2012. Es titulado por examen profesional con mención honorífica. Además, tienen dos maestrías una en Administración Pública y otra en Socioeconomía Estadística y Cómputo Aplicado.

Actualmente, es candidato a doctor en Ciencias Sociales, campo disciplinario Relaciones Internacionales en la FCPyS de la UNAM y desarrolla la tesis *Ciberseguridad con un enfoque teórico y analítico para la soberanía, seguridad nacional y la política exterior*. Bienvenido Juan Manuel, igual siete minutos para tu intervención.

**El ciudadano Juan Manuel Aguilar:** Muchas gracias… Voy a ser rápido para aprovechar el tiempo de todos y que…

Bueno, voy a hablarles un poco del contexto de ciberseguridad de México y también la parte de algunas nociones que deben ser claves para el desarrollo de ciber capacidades dentro de la región.

En el caso concreto de México, pues ya tenemos una gran cantidad de casos que han comprometido la seguridad nacional. Por ejemplo, han envuelto diversas esferas de la diplomática económica empresarial pública y privada, aspectos de ciber incidente o ciberataques… afectaciones.

Por ejemplo, el más activo recurrente que se tiene en mente siempre es el caso de Wikileaks este hackeo… activista en 2011 causó todo cuestiones diplomáticas entre el gobierno de México y el gobierno de Estados Unidos, por las implicaciones de ciertos comentarios que hacía el entonces embajador de Estados Unidos Carlos Pascual sobre la política de seguridad y, la administración del gobierno del presidente Felipe Calderón. Esto causa crisis diplomática y termina con una declaración del presidente Felipe Calderón al *The Washington Post* que practicante dice que es una persona no grata. Y Estados Unidos en el gobierno de Barack Obama lo tiene que sustituir con Anthony Wayne, a bueno, de alguna forma darle gusto al actual presidente en ese momento.

Hubo un ciberataque al SPEI en 2018 muy importantes, los cuales se calculan cada uno que fue exitoso y obtuvieron un saldo de 400 millones de pesos, uno en marzo- abril y otro en octubre que bueno, vulneraron la parte de este sistema de pagos interbancarios del Banco de México.

Lo interesante es que, se sospecha que fue una célula norcoreana que se introdujo a través del SPEI o las credenciales de una aseguradora francesa que se llama AXA. Entonces, así como que vemos la implicación tanto en situaciones de gobierno, como instituciones privadas.

… el ataque de Ramsoware a la paraestatal mexicana en 2019 que bueno, comprometió su capacidad de pago en un momento en el cual esta empresa buscaba renegociar su deuda y subir un grado de inversión para las calificadoras internacionales para presentarse con una institución de confianza. Y ciberataques a la red interna de la Secretaría de Economía el 24 de febrero de este año, que interrumpieron operaciones en esa institución por casi 14 días.

Lo principal, por ejemplo, con estos casos es que en el contexto de México no existen las capacidades de ciber disuasión sino de resiliencia. En ese sentido, como no hay estas capacidades, por ejemplo, en un sentido de poder detectar las amenazas y responder, no tenemos esta capacidad.

Primero, de tener los elementos mínimos y necesarios para hacer que los ciber agresores no intenten afectar las instituciones mexicanas y los sistemas informáticos de nuestro país y porque saben que van a tener una represalia en esas acciones. Y segundo, pues que no tenemos esa capacidad adaptativa a enfrentar los riesgos y amenazas que implica la ciberseguridad y, la evolución del ciberespacio.

Esto tiene que ver mucho con la primera Estrategia Nacional de Ciberseguridad 2017, que bueno, es una estrategia que ya a tres años de su publicación se… ambigua, no se ve que como en sintonía con las tendencias globales con la Agenda Global, por ejemplo, en ciberseguridad de la Unión Internacional de Telecomunicaciones que no responde a el contexto regional de ciber amenazas y mucho menos el contexto global.

Esto, por ejemplo, nos muestra un panorama de México que hay muchas iniciativas principalmente por la parte de la inversión privada, por la parte de la sociedad civil, por la parte, por ejemplo, estos debates que están haciendo desde la Comisión de Ciencia y Tecnología a quien México puede impulsar inversiones, debates, formación de capital humano en el tema de ciberseguridad.

Hay un fuerte flujo de inversiones. Por ejemplo, se estima que hay 621 mil millones de dólares en inversión en los últimos cinco años, lo que es algo bastante fuerte en el caso de México, porque todavía tiene que ser muy, muy focalizadas para mejorar las capacidades de nuestro país.

Aquí, por ejemplo, en el *National Cyber Segurity Index,* vemos que hay ciertas capacidades de México, como la atención de amenazas, como la… digital, la protección de… esenciales que no está totalmente cubiertos y que esta métrica de la… nos pone una cifra bastante severa que es una cifra de cero, todos nos están diciendo que no tenemos los instrumentos mínimos necesarios, para proteger nuestros sistemas informáticos de nuestra población y de nuestro gobierno.

Hemos visto que hay una gran oferta de estudios de entorno a ciberseguridad de empresas privadas, pero por ejemplo de las más importantes, es el caso de los dos reportes que ha hecho la OEA junto con el Banco Interamericano de Desarrollo. En el cual, a través de cinco dimensiones, analizan cómo en el contexto de ciberseguridad en la región y vemos que, en el estudio original que fue editado en 2016, había un conjunto de 17 países que estaban en una fase inicial que todavía eran los primeros pasos para introducir estrategias de ciberseguridad. Teníamos diez en nivel informativo y cinco ya con un fuerte nivel consolidado que estaban avanzando constantemente.

En una parte por ejemplo, con la métricas con los indicadores de *National Cyber Segurity Index* me puse a hacer análisis de cómo era el nivel de ciber capacidades de diferentes regiones del mundo y vemos claramente que México, está con una calificación de 27.7 en general, de los países de la región y bueno, está por debajo de la media global en casi 25 puntos y bueno, por muy debajo también de los países que se van a al vanguardia que en este caso, son los países que forman parte de la organización del atlántico norte.

Esto, por ejemplo, nos sirve para ver que estas dos métricas, el *Global Cybersegurity Index* de internacional de telecomunicaciones y el *National Cyber Segurity Index* nos sirven para guiar qué puntos hay que reforzar en la agenda de ciberseguridad de la región.

Y aquí vemos en qué pues todavía no hay ningún país en América Latina consolidado a un nivel estratégico o en un nivel… con base en estas métricas, con base en los estudios de la OEA respecto al desarrollo de ciber capacidades de defensa. No obstante, sí hemos tenido avances muy representativos en los últimos cuatro años y se hace un comparativo de la evolución y el crecimiento, vemos que hay países liderados por Uruguay, Colombia, Chile, México y Guyana que han avanzado más de 20 puntos en el desarrollo de su ciber capacidad, si comparamos las métricas de los dos informes de la UAE y el…, 2020 y el 2016.

Aquí vemos, por ejemplo, un panorama regional de ciberseguridad en América Latina con las dimensiones ya desglosadas. Vemos que tenemos dimensiones donde hay muy buen desarrollo como es política contra cibercrimen, desarrollo en educación a pesar de que no son suficientes y que se tiene que seguir avanzando en ese sentido, y hay otros que están muy, muy rezagados. Protección a servicios esenciales y protección a servicios digitales, por ejemplo, son las dos dimensiones en las cuales hemos avanzado en lo menos posible.

Por último, cierro con esa parte de que, dentro del centro de ciberdefensa, el centro cooperativo de ciberdefensa de Tallin de la organización del… Norte, hay un apartado de solamente legislaciones vinculadas a ciberseguridad en bastantes países del mundo.

Aproximadamente hay 80 países que han desarrollado documentos, declaraciones de derecho internacional, leyes, estrategias nacionales de ciberseguridad. En ese sentido, con un ejercicio que hice para un artículo que va a publicarse en España en esta diciembre, entorno a desarrollo y estrategias nacionales de ciberseguridad, vemos que pues los países, por ejemplo, que van a la vanguardia en el desarrollo de legislaciones y estrategias nacionales de ciberseguridad, llevan en promedio 3.8 documentos.

Entonces, por ejemplo, esta es una fase muy sumativa porque cambiar y renovar tu estrategia de ciberseguridad y tus legislaciones las hace cada vez más adaptables y las va complementando al reto de la ciberseguridad a nivel internacional. Seguirá Asia con 2.3, los países de América Latina con 1.12, y bueno, países de Medio Oriente con 1.11. Entonces en promedio son muy pocos los países de América Latina que tienen más de dos estrategias nacionales en ciberseguridad, y legislaciones. Y, bueno, en ese sentido esta evolución, esta renovación de estas estrategias y estas legislaciones nos hace más aptos y nos prepara más para enfrentar los contextos regionales y los contextos nacionales de ciberagresiones, amenazas e incidentes que pueden existir. Sería todo de mí parte. Muchas gracias.

**La moderadora Raisa Valda Ampuero**: Muchas gracias a ti, por haber dado, ilustrado tantos datos, tanta información tan pertinente para esto. Entiendo, si no estoy mal, diputada María Eugenia Hernández, que las preguntas las estamos trasladando hacia el final ¿correcto?

**La secretaria diputada María Eugenia Hernández Pérez:** Correcto.

**La moderadora Raisa Valda Ampuero:** Okey. Entonces con esto estaríamos cerrando este segundo bloque de ciberseguridad en la región. Muchas gracias a los panelistas, a las panelistas, al panelista invitado, y también yo reitero mi agradecimiento por este espacio.

**La secretaria diputada María Eugenia Hernández Pérez:** Muchas gracias Raisa Valda Ampuero, de Bolivia. Te agradecemos mucho la moderación en esta mesa, y también a todos los ponentes que nos dieron datos muy importantes sobre el tema de ciberseguridad. Muchísimas gracias y reciban un abrazo muy fuerte.

Y ahorita al final dejamos las preguntas y respuestas, si les parece bien, para pasar para la mesa número tres, en donde el moderador de este tercer bloque es al doctor Javier López Casarín ¿sí? Maestro en Dirección y Gestión Ambiental, reconocido con el doctorado Honoris Causa por la Academia de Derecho Internacional, de la cual es académico de número y presidente de la Comisión Internacional de Innovación. Asimismo fue galardonado por la presea de la Orden Mexicana del Derecho, la Cultura y la Paz.

Es fundador y director de Reinventando a México, grupo empresarial que basa su investigación, productos, soluciones y proyectos en la innovación y disrupción para asesorar a empresas, gobiernos e instituciones públicas, y probadas con la finalidad de mejorar la eficiencia de los procesos para el desarrollo e implementación de soluciones innovadoras a problemas sociales, con el objetivo de beneficiar y modificar su calidad de vida.

Es presidente de la Fundación Reinventando a México, enfocada a desarrollar nuevas ideas… en eventos internacionales que faciliten espacios de reflexión y análisis de nuestra realidad, así como de una plataforma de pensamiento nutrida con eventos de renombre para conseguir mejor los caminos en la construcción de un México mejor. Y vicepresidente del Comité de Ciberseguridad de la… y vicepresidente del Comité de Ciberseguridad. Adelante maestro Javier López Casarín.

**El moderador Javier López Casarín:** Hola, que tal, diputada que gusto saludarle diputada María Eugenia Hernández, secretaria de la Comisión de Ciencia y Tecnología, le agradezco muchísimo esta presentación, y ante todo, la creación y su propuesta para generar este foro. Agradecerle a su vez a la diputada María Marivel Solís, presidenta de la Comisión de Ciencia y Tecnología, a quien aprecio mucho y que me ha gustado mucho como a conducido esta comisión, generando estos paneles que a fin de cuentas de lo que tratan es de construir.

Saludo a todos mis compañeros panelistas, a todos los que están atendiendo, y compartirles que el fin de esta charla será platicar con Pablo Corona, con Bruno Bioni, Martín Portillo, Íñigo Solana y Gilberto Villegas, todos ellos expertos en diferentes temas, sobre todo, resaltando el tema, por supuesto, de lo que venimos hablando de ciberseguridad.

Si está de acuerdo, porque sé que venimos un poquito arrastrando tiempo, empezaré platicando con Pablo Corona, quien presento brevemente, y de ahí continuaría con los demás.

Pablo Corona es maestro en Administración de Tecnología de la Información; vicepresidente para ciberseguridad en la Asociación de Internet Mexicana; titular de la catedra de Buenas Prácticas de Seguridad de la Información en la maestría Gobierno de las Tecnologías de Información en la Universidad Iberoamericana. Autor del libro: “Guía práctica para la gestión de riesgos en la era de la ciberseguridad”; miembro del Comité Técnico, asesor para el programa de resultados electorales preliminares PREP, para el proceso electoral 2018, extraordinario 2019 y 2021 en el Instituto Nacional Electoral, INE.

Editor y redactor de iniciativas de cumplimiento para la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; y auditor líder certificado en Sistemas de Gestión de Seguridad de la Información, gestión de servicios, gobernabilidad de TI, gestión de riesgos y continuidad de negocios. Adelante, Pablo.

**El ciudadano Pablo Corona Fraga:** Muchísimas gracias por la invitación. Muchas gracias a la diputada María Eugenia Hernández, a la diputada Marivel Solís, a la senadora Beatriz Paredes, a Mercedes de los Santos y a ti Javier López Casarín, muchísimas gracias por la invitación a este panel.

Me gustaría compartir con ustedes, primero brevemente, el estado de cómo estamos actualmente en materia de ciberseguridad y protección de datos. Ya lo mencionaron en paneles anteriores, pero no debemos olvidar que el tema de la ciberseguridad no se trata solo de proteger computadoras o de proteger aplicaciones y software, estamos protegiendo a la vida misma, a las personas, y al proteger a las personas necesitamos proteger también las vías de comunicaciones, los derechos fundamentales de las personas, las posibilidades que tenemos de interactuar.

Por lo tanto, el panorama que tenemos actualmente, y en particular en México, en donde el internet tiene una alta penetración, arriba prácticamente del 70 por ciento de la población mexicana está conectada a internet. Pero al mismo tiempo todos los días vemos distintas vulneraciones, ataques y problemas relacionados con el uso de los datos personales y el uso de la tecnología. Y no es la excepción, por ejemplo, los engaños en internet, actualmente tienen, el año pasado hubo en México solamente 10.2 millones de engaños, y esto suma más de mil 200 millones de pesos en engaños, y solamente de los que son reportados a las autoridades, en este caso a la Profeco y a otras autoridades.

Entonces, el problema es grave por cómo utilizamos la tecnología y como los que tenemos más información podemos ayudar a aquellos que tienen necesidad del uso de la tecnología, pero no forzosamente son habidos tecnólogos. Entonces ¿Cuál serían para mí este panorama en general? Tenemos una falta general de capacitación y profesionalización en materia de ciberseguridad, un creciente uso de los servicios en línea; ahora con la contingencia cada vez hay una menor frontera entre donde empieza y acaba lo personal, lo profesional el uso de equipos que son propiedad del titular de la personas o de las organizaciones con pocos antecedentes, en algunos caso hasta nulos; aplicación de sanciones y ejecución de las sanciones en materias de vulneraciones de seguridad, en vulneraciones de datos personales hay muy pocos casos ya de ejecución de las multas, y cada vez un más alto número de transacciones.

Entonces ¿Qué derechos necesitamos proteger? Habría que entender que estos derechos fundamentales a la protección de datos y a la privacidad forman parte de la materia de la ciberseguridad, porque al final, como dijimos, estamos buscando proteger a las personas, y cualquier cosa que hoy tiene un impacto en el mundo digital tiene un impacto en el mundo físico y a la gente le afecta en su patrimonio, en su reputación o en su persona.

Entonces, uno de los puntos que me parece importantes ya como propuestas es: realizar adaptaciones en materia de las Leyes de Protección de Datos Personales en Posesión de Particulares, que ya quedaron de alguna manera retrasadas, tenemos una ley que si bien no es muy vieja, es de 2010, ya tiene 10 años, recientemente se publicó la Ley de Protección de Datos en Posesión de Sujetos Obligados, y en ella se hicieron nuevas consideraciones porque ha ido avanzando esta materia, y creo que habrá que adaptar la Ley de Protección de Datos Personales, por ejemplo, en materia de consentimiento.

En otros países y jurisdicciones, por ejemplo, en Europa que GDPR ha sido uno de los referentes fuertes, hay seis materia de cómo se puede hacer el consentimiento, más bien, la legitimación del tratamiento. En la ley mexicana pareciera que en posesión de particulares solo existe el consentimiento como vía de legitimación, hay varias otras.

Otro de los temas pendientes, me parece que es contar con incentivos adecuados para quien cumple o quien no cumple con estas regulaciones. Tener capacidades de profesionalización en materia de ciberseguridad y plataformas que permitan compartir y colaborar en esta información para, así, tener capacidades de reacción ante incidentes con órdenes como los… Cecyt y colaboraciones entre la administración pública y la iniciativa privada con la sociedad mediante el uso de estándares, por ejemplo, tenemos estándares internacionales como el ISO 27 mil 701, que habla de cómo proteger la seguridad de la información enfocada a la protección de datos personales y mayor monitoreo de las actividades delictivas y en la persecución de ellas, pero, esto significa un mayor monitoreo de la red y esto siempre deberá hacerse en cumplimiento de los principios y de los derechos humanos y de los derechos de privacidad que tenemos todos.

La invasión a la privacidad debe hacerse, más bien, debería considerarse está invasión a la privacidad en el momento en que monitoreamos la red para temas de ciberseguridad, no quiere decir que no podamos monitorear, lo que necesitamos es que se haga en conjunción con este tema de respeto a la privacidad de los derechos humanos. Fomentar el comercio electrónico, los servicios digitales, es fundamental y la libertad de expresión que es otro de los puntos relevantes.

Entonces, para mí, uno de los temas que hemos hecho desde la Asociación a Internet ha sido un análisis de cómo fortalecer el marco público de las leyes y regulaciones al respecto para tener nuevos cambios, por ejemplo, que permitan tipificar y perseguir adecuadamente la pornografía infantil, el fraude, que me parece una propuesta muy importante y puntual.

Ha habido varias propuestas de ley recientes, que de repente pareciera que buscan tipificar el uso de una herramienta en lugar de perseguir un comportamiento, lo cual, puede ser complicado, es importante no perseguir que alguien no use una herramienta, sino los comportamientos con los que se usa esa herramienta es uno de los puntos que necesitamos.

El fortalecimiento de las capacidades empresariales es otro de los relevantes y, actualmente, las habilidades digitales que tengamos todos. Entonces, como propuestas finales, tener cuidado en el monitoreo y la privacidad desde los puntos de vista de las fuerzas del hombre público, pero también respetando los derechos humanos y la privacidad, en particular con el uso de datos biométricos, cámaras de vigilancia en alta resolución que permitan identificar a gente en la vía pública, es uno de los puntos que hay que tomar cuidado en particular.

Otro, es el uso de mecanismos como la privacidad, por diseño y por defecto, en todos los desarrollos de sistemas informáticos que se lleven a cabo en los que se traten datos personales que, prácticamente, hoy son todos, porque todos los sistemas de alguna manera influyen, ya dijimos en la vida diaria de las personas. Y, el apego a los distintos elementos.

Ya lo mencionaban hace un momento en la presentación de la Secretaría de Comunicaciones, en alinearnos a estos elementos que se han hecho para una estrategia de ciberseguridad con los indicadores que el Unión Internacional de Telecomunicaciones hace a través de su estudio de madurez, de ciberseguridad, que lleven a México a adoptar esto y como último punto, también, pendiente llevamos varios años con el pendiente de la firma y la ratificación del convenio de Budapest para perseguir y tipificar delitos homologados con otras partes del mundo. Ha sido necesaria modificaciones y todavía tenemos varios pendientes y sería otro de los aspectos relevantes.

Hasta ahí mi participación y muchas gracias, nuevamente. Javier.

**El diputado Javier :** Muchísimas gracias, Pablo. Gracias por respetar el tiempo y les pediría lo mismo a nuestros panelistas para poder también tener una charla entre todos, donde podamos rebotar puntos de vista que, sin lugar a duda, van a contribuir de manera importante a eso.

Bruno Bioni, profesor y consultor legal en el área de Regulación y Tecnología, con énfasis en la… de protección de datos personales, en el campo académico es candidato a doctorado en derecho comercial, la Facultad de Derecho en la Universidad de Sao Pablo. Donde, también, obtuvo el título de maestría con honores en derecho civil, con un previo en investigación en el Centro de Tecnología en Derecho a Internet Sociedad, de la Universidad de Ottawa. Bruno, el micrófono es tuyo.

**El expositor Bruno Ricardo Bioni:** (Habla en su idioma portugués) Gracias, Javier. Ustedes disculpen… de estar aquí para participar en el Congreso… (Habla en lengua extranjera)

**El moderador Javier López Casarín:** Gracias, Bruno. Muchas gracias por tu punto de vista. Sin lugar a dudas, hablar desde un punto de región contribuye a temas donde se enmarca sin lugar a dudas la legislación, la regulación.

Y ante todo una reflexión para los que seguirán hablando, vendrá la parte que una legislación hay que enfatizar la parte punitiva, hay que acabar fortaleciendo el encarecer un delito, una acción. Ahí es donde trabajando conjuntamente tendríamos que enfatizar y esto lo dejo para poder ir ahondando en la plática porque efectivamente, si hablamos de legislación tenemos que también entrar a que haya un costo alto para aquellos que infrinjan la ley.

Cederé la palabra al ingeniero Martín Portillo Concha, maestro por el Instituto Nacional de Telecomunicaciones de Francia. El ingeniero Portillo es un profesional con más de 20 años de experiencia en el ámbito de las telecomunicaciones, desarrollándose en posiciones ejecutivas. Particularmente en el área de estrategias de negocios y planeación corporativa.

Graduado como ingeniero en Telecomunicaciones por la UNAM, con grado de maestría por Instituto Nacional de Telecomunicaciones de Francia, en los rubros de Redes de datos e ingeniería informática. Estudios de posgrado en la Thunderbird School of Global Management, en Estados Unidos, en Finanzas y desarrollo de negocios. Adelante, por favor, Martín. Bienvenido.

**El ciudadano Martín Portillo Concha:** Muchas gracias, Javier. ¿Me escuchan bien?

**El moderador Javier López Casarín:** Perfectamente.

**El ciudadano Martín Portillo Concha:** Muy bien. Voy a compartir mi pantalla, gracias por la invitación, muchas gracias por el tiempo. Voy a aprovechar esta oportunidad para introducir un tema que va muy de la mano con los temas de ciberseguridad que hemos estado tocando durante toda la jornada, durante toda la mañana. Y creo que es muy oportuno, dado las personalidades que tenemos hoy presentes y que nos están escuchando, llamar la atención en lo que nosotros estamos titulando en la presentación como La inteligencia artificial confiable.

Creo que estamos en un buen momento -ahora que estamos todos inmersos en este tema de desarrollos digitales, hablando de cómo poder crear un marco de control y operativo de la parte de ciberseguridad- para tomar de la mano también el desarrollo y la implementación de las plataformas de inteligencia artificial.

Para hacer un poco de contexto quiero explicar brevemente los cuatro temas que vamos a tocar en esta plática. ¿Por qué consideramos que la inteligencia artificial debería ser una plataforma confiable? ¿Cuáles son los impactos y riesgos de las tecnologías con inteligencia artificial? ¿Cómo podemos conseguir finalmente…? ¿A qué nos referimos con tener una plataforma confiable? Y finalmente, ¿qué podríamos hacer a partir de ahora?

Insisto, nosotros pensamos que estamos en un buen momento -aprovechando todas estas iniciativas de protección a la privacidad de la información y ciberseguridad- para sumar el eslabón final, que es el que nos permite tener los aplicativos y tener la funcionalidad social que ahora estamos teniendo con las plataformas.

Si lo vemos desde un punto de vista cronológico, nos damos cuenta de que cada vez que tenemos la aparición de alguna nueva tecnología se van a suscitar impactos positivos, impactos negativos. Y eventualmente lo que más nos vamos a dar cuenta serán los impactos o las reacciones  negativas por el buen o mal uso de la tecnología en cuestión.

Cronológicamente y para simplemente dar un dato, vemos aquí el famosísimo Proyecto Manhattan, de hace ya muchísimos años, siglo pasado, la década de los 40. La detonación de la energía atómica con una bomba. Bueno, esto claramente al final del día -de manera justificada- recibió la reacción negativa por parte de la sociedad y directamente hacia los científicos y técnicos que se encargaron del desarrollo de esta tecnología. Si bien la energía atómica tiene muchísimas aplicaciones positivas, desafortunadamente se nos queda en la mente y es más difundida la noción negativa de lo ocurrido durante ese hecho.

 De la misma manera, si analizamos temas ecológicos, temas ambientales, temas de biotecnología y recientemente la aparición del internet, el uso masivo de las redes sociales, claramente un impacto es justamente la justificación del foro en el que estamos ahora participando y es el tema de la ciberseguridad. Ahora el uso masivo de todas estas redes nos orilla, nos motiva, nos impulsa a tomar una atención especial en todos los marcos regulatorios, los estándares, las métricas que tenemos que cumplir para el tema de ciberseguridad.

De la mano y en paralelo estamos utilizando la inteligencia artificial. ¿Sería prudente ahora empezar a hacer algo? ¿Cuáles son los impactos? ¿Cuáles son los riesgos? ¿Qué es lo que tenemos que poner en la mesa para empezar a conversar al mismo tono que estamos haciendo con la ciberseguridad los temas de inteligencia artificial? Para tal efecto se ha hecho una serie de encuestas por compañías profesionales que se dedican exclusivamente a la evaluación de temas de esta índole y encontramos información muy interesante que queremos compartir aquí.

En general, de los cinco Estados que son países enteros en diferentes geografías, tenemos que ya encuentran un interés especial en el cómo estamos usando y cómo estamos incentivando el uso de las plataformas con inteligencia artificial. El principal problema que hemos capturado en el mundo entero de la gente que conscientemente ya está utilizando estas plataformas es…

Bueno, finalmente esta plataforma va a tomar una decisión de manera automática, ¿al final del día yo, ser humano, voy a tener la capacidad de tomar la última decisión o tendrá que ser la plataforma o el sistema mismo que lo haga por mi?

Por otro lado y en un gran porcentaje también, ya la gente empieza a preocuparse y empieza a demandar a las entidades reguladoras, a los gobiernos a pensar y establecer marcos que nos permita también trabajar de una manera consciente, confiable -como fue el título de esta plática- de la inteligencia artificial.

De la misma forma, encuestando a las compañías que nos dedicamos a la fabricación de plataformas de ciberseguridad, de protección de datos y de inteligencia artificial también las encuestas señalan que hay un gran interés por la reacción social hacia el uso de la tecnología con inteligencia artificial.

Más del 50 por ciento de los encuestados, incluso, que son estos grandes corporativos tecnológicos, no extraña una preocupación real de la reputación eventualmente que sus plantas, sus fábricas, sus productos vayan a tener, derivado de una percepción no necesariamente positiva o de un marco de acción no necesariamente regulado del uso de estas tecnologías.

De lado derecho presento brevemente un diagrama realizado en la Universidad de Oxford donde tabulan de 0 al 3 un poco el grado de importancia de algunos conceptos que están en la gráfica. Y vemos cómo, en su gran mayoría, la preocupación inicial en medio de todo esto sigue siendo la privacidad de la información o el manejo de los datos.

Para poder analizar esto de una manera más sencilla y respetando el tiempo que tenemos en esta participación, este tema de ciberseguridad asociado a la inteligencia artificial toca todos los segmentos productivos de la sociedad. Estamos hablando de la parte financiera, el transporte, la seguridad, la manufactura, los servicios y naturalmente los servicios de salud también.

Para poder analizar y explicar el contexto y cómo podríamos movernos en estos marcos regulatorios lo dividimos en cuatro rubros fundamentales de inteligencia artificial, analizando los niveles de aplicación, el nivel de datos -los algoritmos propiamente hablando- y la infraestructura de cómputo.

Vamos a ver brevemente cada uno de ellos. Vamos a empezar con la parte de sistemas o aplicaciones y vamos a tocar algunos ejemplos públicos, ejemplos que son del conocimiento probablemente de todos nosotros que estamos participando en este evento. Evento muy conocido, muy difundido. Incluso existen películas, series, etcétera. Aquél caso de Cambridge Analytica, en este caso de compañía social a Facebook, donde queremos resaltar que esta tecnología, ¿el uso de esta inteligencia artificial es un uso impropio, es un abuso de la tecnología?, ¿tendríamos que hacer algo en este contexto? Claramente está asociado también a la protección y a la privacidad de los datos.

El segundo ejemplo y creo que a todos con el uso de nuestras redes condales, con el uso de Twitter, con nuestras cuentas personales, incluso hacemos de alguna manera uso de manera cómica, chistosa lo que las plataformas nos permiten hoy hacer. Tomar una foto de una persona, tomar la foto de otra persona, combinarlas y hacer algún chiste de algún conocido.

Esto también permite utilizar figuras públicas, figuras de representación estatal y, eventualmente, generar noticias no veraces o falsas en concreto. Entonces, cómo estamos haciendo el uso de esta tecnología y cómo podemos cerrar el uso o qué tanto nos conviene cerrar el uso de esta tecnología para tratar de impedir estos impactos.

El otro ejemplo que es muy claro y muy verídico es que hoy la inteligencia artificial es un hecho, la estamos utilizando y claramente en algunos rubros vamos a tener algún problema de la desaparición de algunas capacidades de trabajo específicas. El ejemplo que ponemos está aquí en la página, en Francia el caso del sector financiero, del año 86 al año 2016 prácticamente en este lapso de 30 años se ha visto una disminución de la disponibilidad de fuerza de trabajo en el sector financiero de casi un 40 por ciento, incluso, se dice que probablemente en 25 años puestos tan comunes como son los contadores y gente contable tiendan a desaparecer. Entonces, esta tecnología también nos orilla a un tema de desempleo, es un tema que también queremos poner en la mesa.

La siguiente división es el uso de los datos, el uso de la privacidad de los mismos, es común y este ejemplo es muy conocido. Hoy estoy en una plataforma A, le comparto mi información, derivado de esto, ejemplo, estoy buscando un libro de ciencia ficción y de pronto una plataforma B a la cual no compartí mi información me genera también ofertas de las búsquedas que yo hice en la otra plataforma. ¿Cómo es que la plataforma B consiguió mis datos de esta manera? Está la … de uso de datos y está el uso de la inteligencia artificial y los límites que podríamos poner a este manejo.

El siguiente ejemplo, los famosos chatbots. Utilizamos un chatbot, generamos diálogos, la plataforma con cierta inteligencia aprende una palabra, aprende un adjetivo, una nomenclatura, no necesariamente se emplea alguien y de pronto se puede suscitar un lenguaje no aceptado socialmente, incluso, lenguaje peyorativo u ofensivo y esta también es una problemática que tenemos que atacar.

El siguiente son los algoritmos. El ejemplo que usamos aquí es el sector salud, esta descripción que aparece en la página es bastante genérica, pero nosotros tenemos, incluso, casos concretos en el caso de México, en el sector salud, donde ya nos dimos a la tarea de instalar y de utilizar sistemas con inteligencia artificial para la ayuda de los diagnósticos.

En caso concreto de la pandemia actual del Covid-19, en donde los doctores a pesar de que esta plataforma ofrece una respuesta prácticamente instantánea y muy acertada con respecto al diagnóstico de una persona afectada de esta pandemia, normalmente el médico tiende a no ser totalmente confiado del resultado de esta plataforma ligado a que nosotros le atribuimos a que no es los suficientemente transparente ni es lo suficientemente explicativo de cuales son los procesos o criterios que deberían tener. Entonces, habrá que pensar que tenemos que pedirle a estas plataformas o a estos instrumentos para que los profesionales realmente adopten la tecnología y la puedan utilizar dentro de un marco confiable, ético y moral.

Ejemplo de autos autónomos que, incluso, ya se han visto involucrados en accidentes y derivando en pérdidas de vida, también son problemas de algoritmos. ¿Cómo hacemos responsable a esta plataforma? Hacemos responsable al constructor, hacemos responsable al operador que se tiene que hacer en este contexto. Temas de reconocimiento, departamentos judiciales de cualquier país, hay información en esto de los sistemas inteligentes.

Eventualmente por la …, razas, estereotipos, normalmente y ya se está presentando que dependiendo de la información que capturemos el sistema automáticamente va a atender, a dar una calificación que no necesariamente sea la realidad, pero está afectada de información o de estereotipos como el ejemplo que estábamos mostrando en la página.

Finalmente algunos robots…

**EL moderador Javier López Casarín:** No, adelante Martin, podríamos empezar a cerrar para poder pasar la palabra y posteriormente con un diálogo entre todos.

**El ciudadano Martin Portillo:** Bueno, dame un minuto entonces, vámonos rápido.Esto es lo que estamos haciendo hoy, mencionar a organizaciones que ya se están ocupando activamente de cómo podemos normar o regular este marco del manejo de inteligencia artificial, mencionan esta organización europea. Hay recomendaciones, siete requerimientos básicos, podemos seguirla, compartiré la información y, por supuesto, ustedes lo puedan consultar.

Aspectos básicos que se están requiriendo: transparencia, justicia, equidad, plataformas no mal intencionadas, responsabilidad. ¿Qué se tiene que hacer? Tres componentes fundamentales: legalidad, ética, robustez. Hay aspectos éticos, autonomía humana, prevención del daño, equidad y transparencia. Finalmente otra organización que está haciendo lo propio en el mundo académico muy conocida, la …, dejo aquí la información también esperando que esto motive la curiosidad para poder entrar más al detalle. Un poco el proceso de lo que tendríamos que hacer.

¿Qué podemos hacer hoy? Hoy tenemos habilidades, tenemos conocimiento y tenemos generalmente algunas líneas o guías que podemos hacer para poder incluir dentro de nuestras pláticas de ciberseguridad, acciones contundentes sobre la ciberseguridad y por vanidad de datos, ya considerando la inteligencia artificial. Siendo, y simplemente con esto despido mi platica, la inteligencia artificial como la ciberseguridad es un hecho, la estamos utilizando y estamos conviviendo socialmente con ello. Muchas gracias Javier, aquí dejo mi platica.

**El moderador Javier López Casarín:** Gracias, Martin. Te tomo la palabra si así lo permites, hacernos llegar esa presentación para que la podamos compartir, porque realmente como lo presentas y todos los aspectos que tienen vienen perfectamente bien señala dios. Me gusta mucho no nada más el tema que abordas de la inteligencia artificial, sino que pone en la mesa el valor y la repercusión que habrá en las tecnologías exponenciales que ya son hoy un día a día, no solamente la inteligencia artificial, el internet de las cosas, la cantidad de sensores que hoy en día están en contacto con todas las actividades que generamos, lo que está sucediendo en la transaccionalidad.

Entonces, realmente empezamos a ver que esto no solamente quedamos en la inteligencia artificial, sino que hay que ir ahondando y a los sectores en los que estamos entrando, porque bien estamos hablando de manejos de datos, pero no hay que perder de vista que al fin de cuentas todo viene conectado y un ataque no solamente en ese sentido, sino también podríamos reflexionar en los temas aeroespaciales, en los temas de comunicación en donde todo está conectado y no viene siendo un manejo de datos, sino realmente ya estamos con una afectación.

Cómo está reflexión invitaría yo a participar a Íñigo Solana Riveroll, quien es licenciado en ciencia política y administración pública por la Universidad Iberoamericana, con especialidad en economía internacional. Trabajó como director de asuntos internacionales de la Cámara Internacional de la industria Electrónica de telecomunicaciones y tecnología de la información, director general de asuntos externos del American Chamber of Commerce Mexico, asesor del director general para Norteamérica, el Secretario de Hacienda Exteriores, y si directo de asunto legislativo del Consejo Nacional de Ciencia y Tecnología. Adelante, Íñigo.

No sé, no alcanzo a percibir. Íñigo tendrás el micrófono apagado, porque no alcanzo a ver. Bueno, respetando el tiempo, si estuviesen de acuerdo, y en lo que recibo mensaje de Íñigo le cedería la palabra a Gilberto Villegas Montoya, miembro de panelistas. Quien es socio fundador y director general de la empresa… Ya apareció, adelante Íñigo.

**El ciudadano Íñigo Solana Riveroll:** Una disculpa. Muchas gracias, buenas tardes a todos.

**El moderador Javier López Casarín:** Quieres … tu cámara, Íñigo.

**El ciudadano Íñigo Solana Riveroll:** Sí. Perdón, ya hay muchos perros en esta casa. Gracias, buenas tardes a todos. Muchísimas gracias por la invitación, a la Comisión de Ciencia y Tecnología, a la diputada Marivel Solís, a la diputada María Eugenia, gracias Javier por tu moderación y por este tema tan importante que yo creo que es súper valioso que se discuta aquí en la comisión.

Creo que el Congreso tiene un rol fundamental, yo quisiera enfocar mi plática más en el tema de gobernanza . Sabemos que el tema de ciberseguridad es un tema cambiante, que evoluciona con la tecnología constantemente, etcétera. Hemos visto los riesgos que implican, ya se ha comentado acá con los que me han antecedido en la palabra.

Y, bueno, la inteligencia artificial por supuesto es una tecnología fundamental para que la ciberseguridad sea habilitadora, digamos, de esta tecnología, ¿no? Y hemos visto ejemplos, ¿no? Justo quien me antecedió ahorita en la palabra hablaba de todos estos riesgos que puede haber.

En todo caso ya de alguna manera pues ya está bastante expuesto. Y yo lo que creo es que es super importante que en México ya podamos ir avanzando. Claro, es un proceso que lleva tiempo y, en ese sentido, pues, estos foros son super valiosos, pero siento que –con todo respeto para todos nosotros que formamos parte del ecosistema tecnológico– estamos yendo muy lento. Estamos yendo muy lento, porque seguimos en discusiones y en foros. Y yo siento que hay una… Obviamente el gobierno federal tiene que tomar un rol protagónico, ¿no?

A final de cuentas, todo el tema de ciberseguridad es obviamente un ecosistema y tiene que ser un acercamiento multi, multisectorial, digamos, ¿no?, eso queda claro, tiene que haber obviamente una participación del gobierno, tiene que haber una participación de la sociedad, de la industria, de la academia, etcétera.

Entonces, en ese sentido, bueno, pues, creo que tenemos una oportunidad de fortalecer o de estructurar un marco legal que le dé, o sea, que nos permita realmente tener un mejor sistema de ciberseguridad en este país, ¿no? Y, bueno, pues, hay avances. La industria, nuestra industria de tecnología pues ha hecho múltiples propuestas. Reconozco aquí a mi colega Pablo Corona, de la Asociación de Internet, que también pues yo represento de alguna manera también.

Entonces, yo creo que pue, como digo, es un acercamiento multisectorial y tenemos que avanzar en estas discusiones para que finalmente tengamos una, cómo queremos llamarle, una Ley Nacional de Ciberseguridad o como le queramos llamar, ¿no?, pero el tema es que el gobierno federal tiene que apropiarse de este tema, tiene que verlo como una prioridad y le tiene que invertir, sobre todo.

Entonces, hemos visto temas con esta administración, hay que decirlo con todas sus palabras, una descimbración, ¿no?, en el tema de tecnologías de información o una, digamos, quizás no una falta, a lo mejor hay una falta de priorización de la importancia que tiene, ¿no?, el tema de la tecnología y obviamente pues la ciberseguridad es crítica, ¿no?

Entonces, si no avanzamos en el tema de la ciberseguridad, pues no vamos a avanzar, por ejemplo, en temas de inteligencia artificial, ¿no?, o cualquier solución o algoritmo de inteligencia artificial, entonces, va a caer en todos estos sesgos que hemos comentado y de alguna manera va a ser todo hackeable. Yo, por ejemplo, imagínense subirse a un automóvil autónomo y que no haya una estructura de ciberseguridad.

No sé, por ahí hubo una política hace algunos años, como un hacker, a lo mejor un poquito exagerado, pero de alguna manera no creo que tan lejos de la realidad de lo que pudiera suceder, un hacker se mete al sistema del automóvil autónomo y hace que la persona equis, ¿no?, a la que quería atacar, por así decir, pues tenga un accidente, ¿no? Entonces, digo, eso es un pequeño ejemplo.

Yo ya terminaría mi participación nada más haciendo un llamamiento pues a todos nosotros que formamos parte de este ecosistema, a robustecer este diálogo. Repito, me da mucho gusto y gracias por la participación en este foro. Y a todos mis colegas que me han antecedido en la palabra. Y obviamente creo que la Cámara de Diputados, la Comisión de Ciencia, Tecnología tiene un rol protagónico, proactivo en ayudar a acelerar, digamos, esta necesidad tan apremiante que tenemos de tener un marco regulatorio de ciberseguridad lo más pronto posible y, sobre todo, una gobernanza, pero con este… o con este, perdón, acercamiento multisectorial, ¿no?

O sea, no es un rol del gobierno, no es exclusivamente del gobierno, no es un rol exclusivamente de los legisladores, no es un rol exclusivamente de la industria ni de la academia. O sea, todos tenemos que estar sentados en la misma mesa, porque esas tecnologías avanzan y primero tenemos que estructurar este sistema y establecerlo y quedarnos sentados todos en la mesa para que siga funcionando. Entonces pues muchas gracias.

**El moderador Javier López Casarín:** Gracias por tu intervención. Y rescato una palabra que señala Íñigo, que me parece que hay que poner peculiar atención y que se llama inversión. Hablaba de inversión por parte del gobierno y dejar aquí en la mesa la reflexión para el sector privado, puesto que hablar de ciberseguridad necesariamente nos lleva al tema de invertir, invertir en procesos, invertir en calidad, invertir en sistemas, invertir en preparación, para qué, para justamente, como bien lo mencionabas, robustecer y estar preparados. Asimismo, inversión también en el tema de no solamente ir evaluando los alcances, sino siempre estar yendo un paso adelante.

Y rescataría también una palabra que mencionaba Martín, que me parece verdaderamente importante y que podía dar también punto a uno de las propuestas, como bien Pablo iniciaba decir: precisemos con ciertas propuestas. Y es que él habla de la reputación de las empresas.

Al hablar de la reputación de las empresas, pues, bueno, nos debería llevar a un deber ser. Eso estamos viendo hoy en conductas de empresas trasnacionales, que vienen siendo más las maneras en las que se autorregulan que en sí la misma legislación, estas buenas prácticas que tendríamos que fortalecer para que puedan tener un esquema penetrante y, por qué no, llegar hasta a sugerir que todo esto siempre venga acompañado de un Comité de Bioética, esto pudiera funcionar, se los dejo en la mesa para que ustedes puedan dar su punto de vista.

Cedo la palabra a Gilberto Villegas Montoya, socio fundador y director general de la empresa Gimarc Consulting Services, SA de CV, Unidad de Verificación Aprobada por la ASEA, que es de seguridad energética y ambiental, y a la CRE, la Comisión Reguladora de Energía; socio fundador y presidente de la empresa Servicios Estratégicos en Inteligencia y Contrainteligencia; y socio y presidente de la empresa Airline Security Services; asesor de la Comisión Bicameral de Seguridad Nacional en el Senado de la República de octubre de 2014 a 2016; y es abogado del despacho jurídico Palomar Orozco y Asociados. Adelante, Gilberto. Bienvenido.

**El ciudadano Gilberto Villegas Montoya:** Hola. Qué tal. Buenas tardes. Gracias por la invitación. … Javier, Cámara de Diputados, Cámara de Senadores. Algo que me llamó mucho la atención en este sexenio fue el Plan Nacional de Desarrollo, yo venía trabajando en una investigación para mi grado de tesis de doctoral en 2013 al 2018.

En este Plan Nacional de Desarrollo veíamos en varios apartados la palabra de seguridad y ciberseguridad, que llegaba a mencionar. En este Plan Nacional de Desarrollo se menciona la palabra cambio de paradigma en seguridad, que será el único dedicado en todo el Plan Nacional de Desarrollo 2019-2024 a la seguridad.

Como puede suponerse, este inciso, no se mencionan aspectos relacionados con ciberseguridad, es por eso que yo encuentro el análisis, después de un estudio hasta marzo de 2019, cuando lanzan la Estrategia Nacional de Seguridad Pública.

Metiéndonos a todo esto, la seguridad depende del gobierno. Y, si no atacamos esto desde un inicio, con unas buenas bases, todo nos va a salir mal a lo largo y vamos a estar en un proceso largo y largo en llegar a unos mecanismos legislativos adecuados para México.

No podemos copiar a otros países con lo que ya existe, debemos tomar lo bueno, implementarlo en México, somos demasiados… que tenemos acceso a internet, algunos son nuevos, yo me he encontrado desde estafas en gestiones de… que te venden cosas por internet, para acelerar una sita o algo, y toda esa estafa. Y hay muchas formas que pueden cometer delitos en México. Entonces, esto debe ser legislado para poder ser castigado y prevenir y dar seguridad a todos los mexicanos que empiezan a navegar por internet.

Yo quiero retomar en qué es la ciberseguridad del ciberespacio. Todos nuestros compañeros lo han dicho. Estoy de acuerdo con el maestro Pablo, que acaba de hablar, de que todos debemos estar en la mesa y debemos de participar activamente en la creación de esta ley y las bases.

Quisiera mostrar la preocupación de por qué no existe en este Plan Nacional de Desarrollo, debemos meterle velocidad, a que podamos sentarnos, el sector privado, el sector público, a legislar esto, este cambio de paradigma que el presidente nos ha dicho, es un cambio totalmente. Debemos hacerlo visible en todos los aspectos, falta dinero para que podamos meterle todos los mecanismos para nivelar a México en este sector.

Me gustaría hablar sobre el plan, se basa en que la Guardia Nacional ahorita es la que tiene esta responsabilidad. Voy a permitirme leer un poco en lo que yo hago énfasis en mi investigación de por qué la Guardia Nacional va a terminar la estructura orgánica… llevará a cabo en la seguridad pública y formará la estrategia de seguridad pública.

Los respectivos programas políticos y acciones, la formación y el desempeño de los integrantes de la Guardia Nacional y demás instituciones policiales se deberán de regir por una doctrina policial fundada en… disciplina, respeto a los derechos humanos, imperio de la ley… perspectiva de género.

Es por eso que a este marco jurídico continúa en el diagnóstico en donde primeramente se reconoce que la seguridad es una garantía indispensable para la sociedad, así como por las razones principales en la existencia de la autoridad pública.

De las reflexiones anteriores en el fracaso manifiesto de las políticas que han incrementado los problemas que pretendían combatir se desprende la necesidad de formular nuevos paradigmas en seguridad nacional, interior, pública, que permitan sustentar estrategias de recuperación de la paz para el restablecimiento de la seguridad pública, en la prevención del delito, procuración e impartición de justicia, restablecer el Estado de derecho… a los infractores.

Tales estrategias deben ser multidimensionales, incluyentes y necesariamente radicales en el sentido de que deben de ir dirigidas a raíz a la aguda crisis que enfrenta el país en estos momentos.

Ahora bien, en cuanto a ciberseguridad, encontramos en el numeral 6 de esta estrategia nacional de seguridad pública nuevos criterios de distribución de recursos federales en materia de seguridad. Se hace mención a una interconexión tecnológica eficaz a los sistemas de información federal, estatal y municipal, la cual, a pesar de estar enfocada al sector financiero, abarca otros sectores informáticos en la administración pública, puesto que tiene falta de acuerdos en colaboración y coordinación interinstitucional de diversas instituciones a nivel federal, estatal y municipal, han invitado a la interconexión tecnológica.

La eficacia de los sistemas de información para combatir la criminalidad. Se requiere fortalecer la Plataforma México para contar con una interconexión tecnológica eficiente en todos los sistemas de información en los tres niveles: federal, estatal y municipal.

La inteligencia debe ser la base de un correcto desempeño de las fuerzas… en la medida del desempeño… el uso de la fuerza… la seguridad de la población los propios agentes.

Desarticular la raíz de los procedimientos delictivos. Se han establecido los primeros protocolos de intercambio de información y análisis… inteligencia… interior, pública y nacional.

Como ya vimos, la Guardia Nacional se va a encargar a hora de resolver las actividades de la Policía Federal y… es el referente para garantizar la seguridad, dependerá de la implementación de actividades en cuanto a la procuración de cultura y propagación de la cultura de la ciberseguridad…

Este es un tema prioritario para esta administración y se siguen desarrollando las políticas que se venían desarrollando en administraciones pasadas y no dejar morir todo el avance que ya existía.

Este es mi comentario. Me despido y agradezco…

**El moderador Javier López Casarín:** Muchísimas gracias. gracias, Gilberto. Gracias por tu participación. Quisiera yo en orden de cerrar pedirles que pudiéramos dar un breve mensaje de un minuto. Martín, por favor, si quisieras mandar un último mensaje, unas conclusiones y algo que podamos dejar en la mesa para que los diputados puedan retomar de ahí lo que, como bien se señala, esto es llegar aquí a proponer ciertas acciones que fortalezcan su labor.

**El ciudadano Martín Portillo:** Gracias, Javier. Un minuto. Bueno, simplemente diría que al mismo tiempo que temas de ciberseguridad ahora en nuestra región, América latina, en nuestro país, concretamente en México, estamos en este boom de tratar de generar los marcos, las leyes, etcétera, en paralelo también en algunos otros países donde empezaron mucho antes los temas de ciberseguridad ahora están también enfocados en los temas, en el caso que expusimos, de inteligencia artificial, entonces la invitación para que de manera paralela también empecemos a gestionar todos los procesos que nos ayuden al final del día a contar con sistemas con inteligencia artificial, vamos a usar la palabra regulados -no sé si necesariamente sea eso-, pero ese sería un poco mi conclusión de mi participación. Gracias.

**El moderador Javier López Casarín:** Martín, muchísimas gracias. Finalmente, Pablo, ¿quisieras dejarnos un mensaje de no más de un minuto, por favor, para que se quede aquí en la minuta con los diputados?

**El ciudadano Pablo Corona:** Con gusto. Es invitarlos a que hagamos una orquestación y hagamos equipo entre la iniciativa privada y la administración pública. La Constitución ya tiene en el apartado B del artículo 6 la elaboración de una política de inclusión digital.

Entonces, los temas de ciberseguridad deben surgir desde esta política de inclusión digital y no estamos haciendo otra cosa más que fomentar ese derecho humano al acceso a la información y al internet como un medio de acceso a esa información y poder tener entonces una persecución adecuada de los delitos, de perseguir las conductas antisociales y no el uso de las herramientas con políticas de prevención, de última razón, de poder no tipificar el uso de la herramienta, sino las conductas antisociales que ya mencioné y de alguna manera tener un internet seguro para todas y todos, en particular protegiendo a los grupos más vulnerables, a los adultos mayores, a las niñas y niños que de alguna manera son de los que más nos preocupan.

Y nada más para terminar: no olvidar que el tema de la ciberseguridad, todo aquello que en internet y en el ciberespacio tiene un impacto en el mundo físico lo tiene de regreso en el mundo digital. Y al revés también: las cosas que tenemos un impacto en el mundo digital tienen su correspondencia en el mundo físico. Por lo tanto, hoy las vulneraciones ya no es solamente decir: entró un virus y se perdió información. Hay en juego vidas humanas, hay en juego las comunicaciones, las cadenas de suministro, y por eso tenemos la responsabilidad de tomar esto con una nueva cultura y tomarlo más en serio. Muchas gracias.

**El moderador Javier López Casarín:** Muchísimas gracias, Pablo, y abonando a ese tema, pues yo les dejaría también un punto como pudiera ser Estonia. Estonia hoy maneja sus elecciones vía digital. Entonces, no solamente está de por medio el tema de la vida, el tema académico, el tema financiero, sino también hasta la misma estabilidad de un gobierno.

Pues agradecerles a todos el haber formado parte de este panel. Diputada María Eugenia Hernández, secretaria de la Comisión de Ciencia, Tecnología e Innovación, muchísimas gracias por haberlo permitido. A la diputada María Marivel Solís, presidenta de la comisión, que he visto que se está conectando. Pues agradecerles mucho a los señores diputados su tiempo, su presencia, y me parece que, al ir recolectando las diferentes aportaciones de todos, seguramente vendrá de ayuda para la labor que ustedes tienen que ejercer todos los días. Gracias por este espacio. Me despido de todos ustedes. Que tengan muy bonito día…

**La secretaria diputada María Eugenia Hernández Pérez:** Pues antes de pasar… buenas tardes. Antes de pasar a la conclusión, pues vamos nosotros a darle la palabra, si gustan, darnos un comentario final a la diputada Juanita Guerra Mena y a la diputada Marivel Solís. Si gustan darnos un comentario final o no. Alcen la mano.

**La presidenta diputada María Marivel Solís Barrera:** No, pues muchas gracias de verdad al doctor López Casarín, excelente, de verdad, su participación, su moderación. Muchísimas gracias. Esperamos pronto poderlo saludar porque él nos ha invitado para conocer todo el plan de trabajo. Muchísimas gracias. Y también, bueno, a todos los ponentes, a todos los que participaron en el foro, a las diputadas y diputados, de verdad agradecerles y en especial a la diputada María Eugenia Hernández felicitarla por todo su trabajo. Creo que ya con todos estos foros ya nos permiten muchísimo más tener clara la importancia que tiene el tema de ciberseguridad.

Muchas gracias a todos y continuaremos con eventos que tiene programada la comisión, haciéndoles la invitación y, bueno, en este tema de ciberseguridad continuaremos avanzando. Muchas gracias a todos. Un gusto.

**La secretaria diputada María Eugenia Hernández Pérez:** Diputada Juanita Guerra.

**La presidenta diputada Juanita Guerra Mena:** Gracias, diputada y compañera María Eugenia Hernández. Primero, reiterarle mi agradecimiento por invitarme a este su foro. Gracias por esa tenacidad. Usted es una de las que ha estado día con día, me ha preguntado casi a diario, le he dado la respuesta de que esto se presentó a la Secretaría de Seguridad y Protección Ciudadana…

También estamos en espera de que nos den la opinión de manera oficial del Poder Ejecutivo y por subsecuente también el análisis de cada uno de los compañeros legisladores que podamos en la Comisión de Seguridad Pública. Recordemos que somos 33 integrantes, todos ellos tienen opinión, todos ellos… tenemos que analizarlo y emitir el dictamen que se les va a dar por propuesta.

Y agradecerle infinitamente también a la diputada presidenta Marivel Solís. Presidenta, gracias por este apoyo y solidaridad que tiene con sus compañeros legisladores, primeramente, con María Eugenia. De verdad se ha visto el respaldo y en su Comisión de Ciencia y Tecnología y eso habla de una unidad, la requerimos todos para poder seguir avante.

Yo solamente sigo puntual y prudente en los tiempos. He tomado nota. Si se dan cuenta, he estado porque tenemos otras videoconferencias, el tema de seguridad, en otras también… pero ha estado mi personal muy atento tomando puntualmente de los panelistas invitados. A todos gracias. Son muy valiosas… toda la información que nos han… y, sobre todo, dotado de ella para poder tener una buena experiencia en el sentido de emitir un buen dictamen que sería en beneficio de las y los mexicanos y también, por qué no decirlo, las personas en todo el tema de ciberseguridad.

Así que les reitero mi compromiso, mi solidaridad, diputadas, diputados, también a los compañeros legisladores que están aquí, que estuvieron presentes, y también a la senadora que se dio el tiempo porque en las comisiones en que ella está, en este caso, la bicameral, les hago una sugerencia respetuosa: que también hay otros… como bien lo dijo, son tres diputados, tres senadores, que estén involucrados en ello. Ojalá en las próximas videoconferencias que tengamos estén presentes para darle la importancia que tiene. Muchísimas gracias a todos y felicidades por esta gran participación. Buenas tardes.

**La secretaria diputada María Eugenia Hernández Pérez:** Pues antes de proceder a la clausura, pues yo sí les quiero reiterar a todos, al diputado Alfonso Pérez Arroyo, que fue quien moderó la primera mesa, a… el segundo bloque y el tercer bloque al doctor Daniel López Casarín, excelentes en la moderación. Les agradecemos mucho su apoyo. Y también a todos los panelistas y asistentes a este primer foro latinoamericano por toda la información y experiencia que nos han compartido durante los bloques de trabajo.

Agradezco fundamentalmente a la presidenta Marivel Solís Barrera, quien nos ha respaldado ampliamente en este tema y que ya es el tema de la Comisión de Ciencia y Tecnología, el tema es ciberseguridad. Te agradezco mucho tu apoyo, presidenta Marivel.

Y al directorio legislativo por todo su apoyo para llevar a cabo este foro. A la senadora Beatriz Paredes Rangel por su mensaje de bienvenida y a la presidenta de la Comisión de Seguridad Pública, Juanita Guerra Mena por su apoyo en estos trabajos legislativos, así como a todos mis compañeros diputados que estuvieron presentes. A los medios de comunicación de la Cámara de Diputados que dieron cobertura a este foro virtual latinoamericano.

Hoy avanzamos, hoy avanzamos en este gran esfuerzo de compartir conocimientos sobre ciberseguridad en América latina que es lo que queríamos saber: cómo le hemos ido avanzando en la región latinoamericana, porque a ella pertenecemos, que compartiéramos experiencias a nivel también legislativo. Hoy sabemos que hay 20 iniciativas de ley sobre ciberseguridad. En América latina nos dijeron qué países eran los que estábamos avanzando, en qué ruta estábamos nosotros como México, por ejemplo. Entonces, eso es muy importante, porque a través del conocimiento y a través de estar interactuando con lo que se está haciendo en otros países vemos de qué manera nosotros podemos retroalimentar estas iniciativas.

Escuché también con mucha atención el tema que alguien, un ponente, comentó. Llegamos tarde al tema de ciberseguridad. Yo digo: no llegamos tan tarde, estamos en tiempo y forma para poder realizar iniciativas en el caso del Legislativo, poderlas apoyar, acompañar y que lleguen no nada más a que nos queden en las comisiones, sino que aterricen en los plenos para que se haga una realidad la cuestión de la ciberseguridad.

Y yo me quedo con muchas dudas, pero también muy contenta de que varios países y a nivel mundial se está dando atención a este fenómeno tan complejo que tenemos.

Y decirles que hubo preguntas de los ponentes. ¿A quién le compete?, ¿al Poder Ejecutivo, al Legislativo, la cuestión de la ciberseguridad? Y otro ponente también a su vez respondía: pues nos compete a todos. La ciberseguridad nos toca a todos, desde la trinchera en la que estemos.

Ahora, tenemos que seguir porque por ahí también mencionaban: es muy importante, bueno, pues estamos realizando foros. Sí, pero en la medida en que hagamos más foros, más conversatorios, sobre este tema, vamos a hacer visible este tema en diversos ámbitos.

Lo que queremos nosotros como legisladores en la propia comisión es hacer visible el tema, que sea un tema de la ciudadanía, que sea un tema que el propio ciudadano ejerza presión para que nosotros legislemos, para que a quien le competa podamos empujar estos temas porque ya vimos qué tan importante es la ciberseguridad, cómo estamos expuestos todos los ciudadanos. Dijeron: es que la ciberseguridad tiene que tener su enfoque en la persona, en la seguridad de las personas, en la seguridad también de las empresas, en la seguridad de los entes gubernamentales, en la seguridad de todos, pero fundamentalmente centremos la ciberseguridad en el ciudadano de a pie, en el ciudadano que todos los días estamos inmersos en las redes, en la telefonía celular, etcétera.

Yo les agradezco mucho a todas y a todos ustedes por lo que el día de hoy aprendimos, cada día se aprende más sobre el tema de ciberseguridad, y este gran esfuerzo que hoy se hizo, un esfuerzo de foro latinoamericano de ciberseguridad seguramente dará sus frutos.

Hoy quiero decirles que hubo algunos legisladores latinoamericanos que por cuestión de tiempos, de horarios -porque son de otros países- como que no alcanzaban a cubrir este foro latinoamericano, pero yo les agradezco infinitamente a todos los que estuvimos porque estamos caminando en la cultura del esfuerzo y en la cultura del conocimiento sobre ciberseguridad.

Sin más preámbulo, voy a ceder la palabra a mi compañero diputado Brasil Acosta… perdón… bueno, antes, quiere hablar doctor Javier López Casarín.

**El ciudadano Javier López Casarín:** Diputada, muchísimas gracias, ya que abrió usted la posibilidad de poder dar alguna reflexión. Yo simplemente dejaría en la mesa una reflexión importante para todos los que están asistentes y que ojalá podamos replicar. Estamos hablando de un tema de seguridad nacional. Estamos hablando de un tema de soberanía y hay que verlo de este tamaño de dimensión. No únicamente verlo como que podemos ser víctimas de un ataque cuando estamos hablando de ciberseguridad y seguridad, estamos hablando de ataques, y muchos de estos ataques, como hemos visto en diferentes ejemplos como los que mencionaban en el mundo, provienen de países o grupos externos al nuestro.

Entonces, hay que llevarla a una conversación de mucho más alto de nivel, no dejar de estar hablando de que es un tema de seguridad nacional y así lo deberíamos de estar tratando. Sería una reflexión que… me gustaría dejar en la mesa para darle realmente el peso que debe de llevar y que no sea visto únicamente como un tema de sector o un tema de vinculación de datos, sino que es un tema de seguridad nacional que debe de ser puesto en la agenda con esa seriedad. Sería mi aportación personal. Gracias por escucharme.

**La secretaria diputada María Eugenia Hernández Pérez:** Muchas gracias, doctor Javier López Casarín. Sin más preámbulo, pasamos a la clausura del evento a través de mi compañero diputado federal Brasil Acosta. Adelante, diputado.

**El secretario diputado Brasil Alberto Acosta Peña:** Gracias. Con el permiso de la diputada María Eugenia Hernández Pérez, que fue la organizadora de este evento, a quien felicito por su excelente trabajo. Al mismo tiempo, con el permiso de la presidenta de la Comisión de Ciencia, Tecnología e Innovación, la diputada María Marivel Solís. Diputada Juanita, también, presidenta de la Comisión de… Con el permiso, aunque ya no esté con nosotros, de la senadora Beatriz Paredes. Y con el permiso de los panelistas y de los responsables de llevar las mesas.

Me parece que lo que se ha hecho hoy es sentar precedentes de la importancia de un tema que efectivamente habla de la seguridad nacional. Y, por lo tanto, creo que sí es fundamental tomar en consideración que desde que nosotros abrimos una cuenta de correo electrónico o nos metemos a una red social damos nuestros datos y aceptamos en alguna medida, cuando no leemos el contrato, que los utilicen casi casi como quieran. Y esto ya rompe nuestra propia seguridad, pero nosotros la aceptamos.

Efectivamente, es necesaria una legislación al respecto y creo que los comentarios que se han hecho en estos foros, en estas mesas, en este foro latinoamericano de ciberseguridad, son fundamentales y tienen que ser escuchados, tomados en cuenta, y tienen que aparecer en las líneas de la ley que se vaya a establecer.

Por lo tanto, gracias a todos por su labor. Gracias a todos por su esfuerzo, por su tiempo, por sus conocimientos, y efectivamente en esta Comisión de Ciencia, Tecnología e Innovación somos plurales porque el problema es de la ciberseguridad… no le afecta a un individuo independientemente del partido al que pertenezca, sino que le afecta a todo ser humano de este país y por lo tanto estamos convencidos de que debemos trabajar unidos para tener un marco jurídico que sea lo suficientemente robusto para tener el tema de la ciberseguridad, para tener el tema de la ciberseguridad…

Pues, sin más, siendo las 14 horas con 58 minutos del día 29 de octubre del año en curso, declaramos clausurados los trabajos de este foro latinoamericano de ciberseguridad, agradeciendo a todos su participación para formar una ley que garantice que haya ciberseguridad en México. Es cuanto.

**---o0o---**