Lima, 27 de abril de 2023

OFICIO Nº 558 -2022-2023 JCA-CR

INFORME DE VIAJE A LOS ESTADOS UNIDOS MEXICANOS

Asunto: Actividades de Representación.
Referencia: Viaje a ciudad de México.

Señor General(r)
José Daniel Williams Zapata
Presidente del Congreso de la República
Palacio Legislativo. Lima 1.
Presente. –

De mi especial consideración:

Me dirijo a usted con la finalidad de saludarle cordialmente y a la vez informar, cumpliendo con lo dispuesto por la norma legal aplicable[1], sobre las labores de representación oficial, efectuadas por el suscrito entre el 16 y 19 de abril de 2023, con ocasión del viaje vinculado a la invitación cursada para asistir al "Foro de Seguridad de las Américas" La Criminalización del Ciberespacio II, del que el suscrito formó parte integrante.

Sin otro particular es propicia la oportunidad para expresarle los sentimientos de mi especial consideración.

José Ernesto Cueto Aservi
Congresista de la República

[1] *Reglamento Congreso de la República / Art. 23, inc. "h" / Acuerdo Mesa.*

Congreso de la República

INFORME

FORO DE SEGURIDAD DE LAS AMERICAS

"La Criminalización del Ciberespacio II"

ALM. JOSE ERNESTO CUETO ASERVI

Congresista de la República

DESPACHO PARLAMENTARIO

"Año de la Unidad, la Paz y el desarrollo"

INFORME DE VIAJE A LOS ESTADOS UNIDOS MEXICANOS EN REPRESENTACION DEL PERÚ PARA EL "FORO DE SEGURIDAD DE LAS AMERICAS".

EVENTO

Con ocasión de este importante foro, se ha tenido la oportunidad de compartir experiencias entre representantes de diversas nacionalidades con el fin continuar lo mismo que con otros eventos similares, adquiriendo para el país la resultante de valiosas relaciones internacionales en las que se comparte experiencias y establece lineamientos críticos que sirven para analizar políticas de gobierno con las que se pueda combatir, en este caso la delincuencia a nivel de *ciberespacio*, en este caso en el marco de la "*ciberseguridad*", que como se sabe, es una amenaza latente en general para el mundo moderno y que, aumentó exponencialmente a partir de la Pandemia de la Covid-19, junto con el mayor uso de las redes en internet, lo que sumado a los efectos de la crisis económica resultante, más los conflictos sociales y guerra posteriores, obligan a los Estados a ponderar las vulnerabilidades que sufren tanto en la infraestructura digital como en la consecuente seguridad ciudadana.

En esta ocasión el evento se llevó a cabo en ciudad de México, donde se realizó el "***Foro de Seguridad de las Américas***", "*La criminalización del Ciberespacio II*", coorganizado por la Oficina Regional de "*Crime Stoppers*", el Parlamento Latinoamericano y Caribeño (*PARLATINO*), y la Fundación Konrad Adenauer, Programa Regional Alianzas para la Democracia y el desarrollo con Latino América (*KAS ADELA*). 1

MARGEN DE COBERTURA

Internacional, Institucional Público.

INFORME SOBRE LABORES DE REPRESENTACION

I. INFORMACION GENERAL

Sustento Normativo
Art. 23, inc. "f". Reglamento del Congreso de la República.

II. TIPO DE EVENTO

Internacional vinculado a Inteligencia y Seguridad.

III. LUGAR

País: México – ciudad de México[1].

[1] https://parlatino.org/news/foro-parlamentario-de-inteligencia-y-seguridad/

IV. FECHA

Periodo comprendido entre el 16 y 19 de abril de 2023.

V. ASISTENCIA

En representación del Perú como miembro integrante del Congreso de la República del Perú y presidente de la Comisión de Inteligencia del Congreso de la República.

VI. INFORMACION DETALLADA DEL DESARROLLO DEL EVENTO

Desarrollo del Programa de actividades del Foro Internacional entre los días 16y 19 de abril de 2023, en ciudad de México.

Como se ha señalado en los últimos años se ha producido un incremento exponencial en lo relacionado a la delincuencia en el ciberespacio; por ello, es necesario generar conciencia de las amenazas del mundo civilizado en especial en lo que corresponde al campo del ciberespacio y con mayor razón entorno del poder político que, impulsa a mejorar continuamente las legislaciones estatales, a la par de los adelantos que la ciencia y los cambiantes retos que impone el mundo moderno se generan.

Es importante resaltar dentro de este concepto la noción del "poder político" pues es precisamente a partir de el, que se puede transformar un país, sus instituciones, los grupos sociales y porque no, finalmente orientar *(para bien o para mal)* a las personas -cuando se menoscaba su libertad en un aspecto negativo, en la medida que se puede utilizar este (poder) para hacer cambios objetivos en las normas que rigen a las sociedades e influir en el pensamiento a través de las políticas de educación o culturales que, se desarrollan y aplican mediante políticas gubernamentales desde la niñez, durante y hasta la formación completa y compleja de la persona en su integridad.

El poder en si mismo sirve para hacer grandes cambios y suelen estos llevarse a cabo a partir de diversas fuentes como también la económica y la social; a nivel político, esos cambios suelen estar ligados al ejercicio de la función pública, generalmente vinculada a la representación delegada avalada democráticamente mediante la fuerza de los votos, sin embargo es indesligablemente necesario relacionar el poder político con la capacidad de generar cambios también a nivel económico y social con lo cual, se debe usar en principio para hacer frente a las amenazas que afectan a estas tres fuentes de poder -económico, político y social- lo que obliga a prepararse por ejemplo -en términos cibernéticos- para posibilidades de una paralización de sistemas informáticos, ciberataques ordenados por gobiernos foráneos, suplantación de identidades en línea, fraudes en redes, robos de identidad, accesos no autorizados a sistemas informáticos, piratería, amenazas a activos estratégicos, entre otros.

Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
www.congreso.gob.pe
jcueto@congreso.gob.pe

6.1 LA CRIMINALIZACION DEL CIBERESPACIO – CASO PERU

"EL CONTEXTO POLITICO"

José E. Cueto Aservi
Congresista de la República

¿En qué consiste la "Criminalización del Ciberespacio?

La criminalización del ciberespacio se refiere a la **aplicación de leyes penales y sanciones a las actividades delictivas que se llevan a cabo en el ámbito digital**, como el uso ilegal de la información, la piratería informática, el acoso en línea, el cibervandalismo, el *phishing*, el *spam* y el fraude en línea, entre otros.

La criminalización del ciberespacio tiene como objetivo combatir las actividades ilegales en línea y disuadir a los delincuentes de cometer delitos digitales, de la misma manera que se aplican sanciones penales a los delitos cometidos en el mundo físico.

Las leyes que rigen la criminalización del ciberespacio varían según el país y pueden incluir medidas para rastrear y perseguir a los delincuentes en línea, así como para prevenir y proteger a los usuarios del ciberespacio contra los delitos en línea. También pueden incluir medidas para garantizar la privacidad y la protección de los derechos de los usuarios en línea.

Sin embargo, algunos críticos argumentan que la criminalización del ciberespacio puede limitar la libertad de expresión y el acceso a la información en línea, y que puede ser difícil de aplicar debido a la naturaleza global y descentralizada del ciberespacio. Por lo tanto, es importante encontrar un equilibrio adecuado entre la protección de los derechos en línea y la necesidad de combatir el delito digital.

En este sentido, la Criminalización del Ciberespacio es un tema que forma parte de la agenda política regional (*Hemisferio Occidental*), orientada principalmente hacia Latinoamérica. Esta fomentada por los gobiernos de los países desarrollados a través de sus funcionarios de gobierno y de la red de ONGs de seguridad como parte de la llamada "sociedad civil global".

En este evento participan funcionarios de gobiernos que tienen por objetivo "sensibilizar" y "socializar" la agenda de la "criminalización del ciberespacio".

Este es asunto de actualidad que no se puede soslayar y la participación en estos foros proyecta el interés y compromiso de los actores políticos que participan en ella sobre el tema.

¿En qué consiste el "programa *Crime Stoppers*"?

El programa *Crime Stoppers* es un programa de seguridad pública que se utiliza en varios países para combatir el crimen y la delincuencia. El objetivo del programa es fomentar la participación ciudadana en la lucha contra el crimen, ofreciendo un medio seguro y anónimo para que las personas puedan proporcionar información sobre delitos.

El programa funciona a través de un sistema de recompensas para las personas que proporcionan información útil que conduce a la captura y condena de delincuentes. Los ciudadanos pueden proporcionar información sobre delitos y sospechosos a través de un número de teléfono o un sitio web.

La información proporcionada se mantiene en estricta confidencialidad y los ciudadanos no tienen que proporcionar su nombre o información personal.

La información recibida es luego transmitida a la policía, que investiga el delito y busca arrestar a los delincuentes. Si la información proporcionada conduce a un arresto y condena, el informante puede recibir una recompensa en efectivo.

El programa *Crime Stoppers* se ha utilizado con éxito para resolver muchos tipos de delitos, incluyendo asesinatos, robos, violencia doméstica, tráfico de drogas y otros delitos. El programa ha sido ampliamente adoptado en varios países y ha demostrado ser una herramienta eficaz para involucrar a la comunidad en la lucha contra el crimen.

Este programa tiene alcance internacional, es un programa global. En la región están sumamente activos con una serie de eventos y actividades tanto en México, cómo en Panamá. Una de sus principales áreas de acción es "el cibercrimen", y también desarrolla otras áreas cómo: medio ambiente, vida animal salvaje, fugitivos internacionales, tráfico humano, tráfico ilícito, y crimen financiero. Toda una red de informaciones globales en las que el anonimato es la base.

¿Qué es el Parlatino?

El Parlamento Latinoamericano y Caribeño, conocido como Parlatino, es una organización intergubernamental compuesta por representantes de los parlamentos nacionales de los países de América Latina y el Caribe. Fue fundada en 1964 y tiene su sede en la ciudad de Panamá.

El objetivo del Parlatino es fomentar la integración y la cooperación entre los países de la región a través del diálogo político y la promoción de políticas públicas comunes. Entre sus funciones se incluyen la promoción de la democracia, el desarrollo económico y social, la defensa de los derechos humanos y la protección del medio ambiente.

El Parlatino está compuesto por cinco comisiones permanentes que se encargan de temas específicos:

Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
jcueto@congreso.gob.pe

Política, Seguridad y Derechos Humanos; Asuntos Económicos, Financieros y Comerciales; Educación, Cultura, Ciencia, Tecnología y Comunicaciones; Medio Ambiente, Turismo y Desarrollo Sostenible; Familia, Niñez y Juventud.

Cada país miembro tiene derecho a enviar un número determinado de representantes al Parlatino, dependiendo de su población. El presidente del Parlatino es elegido por un período de dos años y es responsable de dirigir las reuniones y representar a la organización en eventos internacionales.

Es un "*partner*" (asociado, socio) promotor usual de las actividades de *Crime Stoppers*.

CONSIDERACIONES ESPECIALES

El uso eficiente de las Tecnologías digitales es un elemento transversal en la definición de políticas públicas relacionadas con la gobernabilidad democrática, la transparencia y el desarrollo equitativo y sostenible de una sociedad con **confianza digital**. Al mismo tiempo representan una oportunidad para garantizar los servicios digitales mediante mecanismos de seguridad.

Como parte de un país seguro digitalmente, se hace imperativa la voluntad de gobernar este proceso de adopción con una Estrategia Nacional de Seguridad y Confianza Digital (ENSC), que facilite las condiciones para aprovechar las oportunidades y mitigar los riesgos digitales derivados de este proceso; debido a que toda Sociedad se ha digitalizado en casi todos sus frentes, impulsando una nueva economía digital cuyo activo principal es la información.

Crear valor con estos activos es un imperativo no sólo para el sector privado, sino también para el sector público que debe atender, además, nuevas demandas de una ciudadanía digital.

En este contexto, las naciones más avanzadas han desplegado esfuerzos durante los últimos 5 años para manifestar sus intenciones de gobernar un proceso que convierta a la **Seguridad y Confianza Digital** en una herramienta para la gobernanza y protección de los datos. Es importante señalar que en el continente se habla de conceptos como ciberseguridad, seguridad cibernética y seguridad digital **para delinear los procesos de mejora en la gestión de la seguridad digital de cada país.**

Ese ha sido el principal propósito, con el que se han propuesto diversas manifestaciones, que van desde Políticas, Estrategias, Planes y Agendas Nacionales, que en sus primeras etapas contienen **diagnósticos del punto de partida y aspiraciones para fines de esta década**, pasando por recomendaciones de políticas públicas, fortalecimiento de algunos sectores y priorización de iniciativas público-privadas que garanticen los primeros pasos hacia una Estrategia Nacional de Seguridad y Confianza Digital.

Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
jcueto@congreso.gob.pe

LOS RETOS DE LA CIBERSEGURIDAD EN EL PERÚ

El Perú es el tercer país con mayor número de ataques cibernéticos en la región, siendo la falta de presupuesto de los emprendimientos la principal limitación para adoptar medidas de seguridad informática.

Ciberseguridad, cibercrimen y ciberguerra son términos que han cobrado importancia en el mundo de la seguridad en general. Ello, debido a la evolución tecnológica, pero, principalmente, producto del incremento de las trasgresiones de seguridad, actos criminales y la presencia de herramientas de manipulación basadas en desinformación.

A finales del 2020, en Latinoamérica, **la principal barrera para adoptar mecanismos de ciberseguridad dentro de las empresas era la falta de presupuesto** (34%), seguida por la ausencia de integración en la estrategia (18%) y la dificultad técnica de implementación (14%).

El Perú, según un estudio de ciberseguridad realizado por Fortinet, fue el tercer país de Latinoamérica con mayor número de ataques cibernéticos durante el 2021, después de México y Brasil.

En ese sentido, **el principal reto de la ciberseguridad en el país es enfrentar desafíos tales como la creación de un marco regulatorio integrado**, de manera que, al no estar fraccionado, sea más eficiente su cumplimiento e implementación. Asimismo, por parte de las organizaciones es importante reconocer **el rol del oficial de seguridad de la información o director de seguridad de la información** de una empresa (en inglés, *CISO*), además de contar con técnicos especializados en ciberseguridad y asignar un presupuesto adecuado.

No obstante ello, **el Perú no cuenta con una estrategia de ciberseguridad, sino diversas normas relacionadas a este tema.** Sobre el particular, pueden nombrarse la Ley N° 30999 de Ciberdefensa, que tuvo como objeto establecer el marco normativo en esta materia; la Ley N° 27269, de Firmas y Certificados Digitales; la Ley N° 28493, que regula el uso del correo electrónico comercial no solicitado (spam); la Ley N° 29733, de Protección de Datos Personales; entre otras.

NECESIDAD DE CONVERTIR AL PERÚ EN UN PAÍS MÁS PREVISOR Y MENOS REACTIVO

El Perú, en materia de ciberseguridad, es un país más reactivo que previsor. Falta mucho aún para alcanzar los estándares regionales en seguridad digital, ya que, entre otros aspectos, las empresas e instituciones públicas no están acostumbradas a tomar todas las líneas de seguridad que le sean atribuibles dado el riesgo que enfrentan. "*Bank of America*" tiene, por ejemplo, un presupuesto en términos de ciberseguridad ilimitado y *Microsoft* de alrededor de un billón de dólares.

Según la Encuesta "*Global Digital Trust Insights de PwC 2022*", la mayoría de las empresas no controlan los riesgos cibernéticos de terceros, riesgos que se oscurecen por la complejidad de sus relaciones comerciales y sus redes de proveedores. Los hallazgos son una señal de alerta en un entorno en el que el 60% de los encuestados de la alta dirección anticipan un aumento de los delitos cibernéticos en 2023.

También reflejan los desatinos que enfrentan las organizaciones para generar confianza en sus datos, asegurándose de que sean precisos, verificados y seguros, para que los clientes y otras partes interesadas puedan confiar en que su información estará protegida.

EL CASO DE LOS "*FAKE NEWS*"

Los peruanos vivimos rodeados de "*fake news*", de noticias falsas, muchas veces malintensionadas, que se difunden muy rápido y se viralizan. A pesar de ello, todavía no sabemos reconocerlas y, peor aún, estamos expuestos a ciberdelincuentes que se aprovechan de esta vulnerabilidad.

Según un estudio de *Kaspersky*[2], casi el 80% de los peruanos no sabe reconocer lo que es una "*fake news*". Esto ha llevado a que la empresa en ciberseguridad bloquee un promedio de 123 ataques de *malware* por minuto entre enero y agosto del 2022, lo que nos coloca en el tercer país con más ataques en la región, detrás de Brasil y México.

CIBERATAQUES MÁS COMUNES

Según la compañía de ciberseguridad CANVIA[3], los ciberataques más comunes en los que caen los usuarios en el Perú son los siguientes:

1. ***Ransomware***
   Se trata de un *software* malicioso que, al infectar el equipo, otorga al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota, encriptando y secuestrando los archivos.

2. ***Zoom-bombing***
   Es la posibilidad de irrumpir en una videoconferencia en *Zoom* sin el permiso de la persona que creó la reunión. Puede resultar sencillo interrumpir en este tipo de videoconferencias porque muchas veces las URL para acceder a los encuentros se rastrean haciendo una búsqueda digital o bien si alguien, por error, la comparte o deja publicada en algún sitio.

[2] refer.- https://latam.kaspersky.com/
[3] refer.- https://www.canvia.com/

3. ***Phishing***
Se relaciona con el envío de correos electrónicos que tienen la apariencia de proceder de fuentes confiables (bancos, tiendas, entre otras), pero que en realidad buscan manipular a la persona que lo recibe para robar información confidencial.

4. ***Spyware***
Este *software* sigue las actividades del colaborador en línea, tanto en equipos como en dispositivos móviles. Puede supervisar y copiar todo lo que se escribe, carga, descarga y almacena, en forma de troyano, virus, virus gusano, entre otros.

Finalmente, cabe destacar que el Perú no cuenta con una Política Nacional de Ciberseguridad, por lo que no se han elaborado ni informes, ni reportes ni rendiciones que detallen presupuesto para su implementación. Su rectoría debería recaer en la Presidencia del Consejo de Ministros.

FORO DE SEGURIDAD DE LAS AMÉRICAS

6.2 Resumen de algunas de las ponencias, tiempos de debate y participación llevados a cabo durante el primer día del Foro, registrado con fecha lunes 17 de abril de 2023.

"**Diplomacia digital y cibernética, Ministerio de Asuntos Exteriores de Estonia, anteriormente Global Digital Governance Fellow at Stanford**.
OSULA, Anna María

Entre las múltiples experiencias internacionales en torno a la ciberseguridad compartidas durante este importante evento están por ejemplo los casos de Estonia; la república báltica, es considerada como el primer 'país digital' del mundo, entre sus actividades resaltantes se observa que exporta su experiencia de Administración '*online*' a Kenia, Nigeria, Tanzania y Benín; entre otros países Estonia, participa en numerosos proyectos de digitalización en África, explotando su propia experiencia, pero también reivindicando una trayectoria que le acerca a las realidades del continente bajo el modelo de "*e-administration*" (administración electrónica) principalmente a países africanos.

Estonia en el marco de su independencia, era un país pobre y el Gobierno debía ofrecer los servicios básicos, que los ciudadanos esperaban. Empezamos introduciendo internet en todos los colegios en 1996 y dando alfabetización digital a los mayores. Estonia se independizó en 1990, pero la Unión Soviética no lo aceptó (en medio de su propia descomposición) hasta el año siguiente, sin embargo, también es en Estonia que se registran

cada día múltiples ataques electrónicos principalmente a la infraestructura critica.

Con relación a la seguridad, muchos ataques están patrocinados por Estados o grupos políticos con activismo criminal. Muchos ataques se dan en diferentes campos en Letonia (identificación electrónica, firmas digitales y más o menos tres mil (3,000) sistemas que afectan en el campo digital y más del 90% de los residentes usan estos sistemas.

Se trata del primer país en implementar el "voto electrónico"; pero todo esto lo hace a la vez altamente vulnerable (habiendo tenido p.e. su primer ataque cibernético en 2007, hubieron otros ataques a los *ID Card* en 2017 y 2018), en términos generales sobre bancos, centros comerciales, sitios web del gobierno, entre otros y precisamente a partir de ese año se inicio en Estonia la "ciberguerra" que hizo "despertar" a Estonia y hoy se constituyen en uno de los mejores sitios de ciberseguridad, desarrollando estrategias de ciberseguridad.

Entre estas "estrategias", Estonia ha desarrollado ya la tercera de ellas, debido principalmente a la recepción de mas de 25 mil ataques por año la han llevado a mejorar también los actos legales y estructuras e infraestructuras tecnológicas diseñadas para funcionar entorno a una "sociedad digital" donde se concentran también los principales esfuerzos del Estado.

Existen tres niveles de comprensión del sistema de ciberseguridad (domestico, regional e internacional) gracias a un enfoque multisectorial con parte del sector empresarial.

Principales temas desarrollados

Intercambio de información;
Coordinación de política legal aplicada;
Ciberseguridad como parte de las relaciones exteriores;
Medidas de ciberseguridad a compartir;

Queda claro que a este respecto debe tenerse un enfoque responsable frente a esta guerra cibernética, junto con un necesario aumento del conocimiento con políticas de protección de nuestro ciberespacio con las siguientes consideraciones:

- Existe un intercambio de actividades de ciberseguridad;
- Debe implementarse geopolíticas orientadas a la guerra cibernética;
- Deben poder determinarse nuestras vulnerabilidades – ACN;

Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
www.congreso.gob.pe
jcueto@congreso.gob.pe

- Debe poder determinarse los principales actores (privados);
- Debe propenderse a Campañas en todos los niveles (importante), sobre todo en torno a una verdadera voluntad política de nutrir esta educación;
- Se debe asegurar la confianza en el Estado como un modo de vida;

"**Ciberseguridad - KAS**".
GEHRINGER, Ferdinand Alexander

Existen motivaciones geopolíticas inmersas en el desarrollo de los ataques a la ciberseguridad de las naciones (Geo politización del ciberespacio); existen más de 34,000 ataques anuales de *malware* en Alemania. En particular en Alemania los ataques en el ciberespacio iniciaron en 2015; con este motivo se desarrollo consciencia de la importancia del rol del Estado, especialmente a través del rol del Parlamento, las afectaciones a los ordenadores de gobierno como usuario.

Con el tiempo se ha ido desarrollando la ciber inteligencia en el ciberespacio sobre lo que aun hay poco conocimiento a nivel usuario, pero es a partir de esta plataforma que se agudizan los ataques de los *Hackers* que han superado los requisitos de ingreso establecidos por las instalaciones muchas veces incluso militares. En 2016 se permitían ingresar incluso a la red de datos del gobierno federal (Alemania). Hacia el 2016 ya se tenían ataques que infectaban los ordenadores del parlamento. La seguridad sobre estos escenarios ha mejorado, pero siguen siendo en algún ángulo vulnerables.

A modo de conclusión hay que orientar esfuerzos hacia una legislación de lineamiento general internacional que ayude a todos a tener una base de datos a modo de una "embajada de datos" fuera de los sistemas nacionales a modo de un "*Back Up*" independiente.

"**Cibercrimen en Guatemala**".
CUSTODIO, David

En términos de política criminal; el ciberacoso en Guatemala llegó a cifras alarmantes del 45% con volúmenes en aumento; en este campo los estudios han llevado a considerar la necesidad de tener una "Unidad de investigación de ciberdelitos".

Durante el desarrollo de esta ponencia se mencionaron algunos casos de afectaciones que llegan a la Contraloría, al propio Ministerio de Relaciones exteriores entre otros, delitos como estafas y diversos tipos de ciberdelitos.

"**Cibercrimen caso: Costa Rica**".
BRENES, Paula

La ciberseguridad busca neutralizar la relevancia negativa que tiene un ataque en el ciberespacio "en el momento indicado" (o menos oportuno); esto hace que, en términos de política criminal; se prevean por ejemplo ataques en el preciso momento en el que se produce un "cambio político" (Elecciones por ejemplo para un cambio de gobierno), que podría tratarse de ataques que tienen muchas consecuencias negativas para el ordenamiento de un país.

En el caso de Costa Rica esto fue el motivo de la guerra cibernética a la que no se le dio suficiente importancia. En el caso de Costa Rica, lo mismo que en otros países de la región comparativamente con el rápido desarrollo de la ciberdelincuencia, en el caso de los gobiernos demora mucho informar y activar las defensas a estos ataques cuando deberían por el contrario los gobiernos ir a la cabeza del desarrollo e implementación de ciberseguridad, estos ataques suelen afectar el seguro social, la hacienda, este tipo de ataques específicos fueron hechos por un mismo grupo ("*Ransomware Conti*") igualmente en el Perú.

En términos económicos, las paralizaciones en Costa Rica durante el año 2017 a raíz de los ciberataques significaron un promedio de 30 millones de dólares diarios, literalmente "detuvieron al país".

"**Centro de Ciberseguridad: República Dominicana**".
GAUTREAUX, Juan G.

Para Republica Dominicana, la "Agenda Digital 2030" debe desarrollar aspectos de ciberseguridad de manera transversal en todos los campos. En este país se desarrolla un modelo de gobernanza en dicho aspecto junto con el Ministerio de la Presidencia (PCM para el Perú), e involucra a casi todos los Ministerios (Defensa, Hacienda, Relaciones Exteriores -ciber diplomacia- Educación, Judicial, entre otros), con el fin de elaborar estrategias de ciberseguridad nacional e internacional, entre las que se contemplan estrategias contra ciberdelitos, ciber terrorismo, ciber educación, ciber diplomacia, entre otros.

"**Uso de la Inteligencia Artificial (IA)**".
ULLOA, Mario

Hoy en día los datos se obtienen casi en tiempo real, esta nueva realidad debe usarse también para usar e integrar esos datos e información para su uso contra la criminalidad.

Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
jcueto@congreso.gob.pe

Con relación al uso de la Inteligencia Artificial (IA) existen en USA centros de fusión (Inteligencia con intercambio de datos) que obtienen y procesan toda la información de Centros u Oficinas en tiempos mínimos.

También se utiliza Inteligencia Artificial Analítica donde se usan toda la información de personas o instituciones para fines de seguridad, del mismo modo se utilizan datos de IA en temas judiciales, entre otros con un uso incuestionablemente útil, pero siempre en el límite de la "privacidad".

En estos aspectos se busca darle "calidad a los datos", ya el uso dependerá de quien lo requiere, desde que ámbito y con que móvil, lo que obviamente siempre será igualmente muy controversial desde el aspecto legal.

RESUMEN DE LA ESTACIÓN DE DEBATES

Resulta ser un aspecto importante el concebir un concepto de "*ciberresiliencia*" entendida como la capacidad de una organización, sistema o país de "resistir" los ataques de ciberdelincuencia, pero además de recuperarse de forma rápida y efectiva; esto resulta vital para la soberanía de los Estados en aspectos de cibernética, preservar documentos sensibles y generar confianza en las sociedades y entre los propios Estados.

Desde esta perspectiva, cabe preguntarse ¿Cuáles son las estrategias a implementar en la estrategia de ciberseguridad? Debe analizarse el como mejorar lo que hay en cada país y para ello se debe contar con la cooperación internacional; en este aspecto es necesario convenir en que resulta altamente importante aprender constantemente y sobre todo desde la base de las "lecciones aprendidas" lo que, sin duda es diferente en cada país pero, será siempre necesario que en la diversidad de casos se esté desde el ámbito de todos los Estados, atento a las experiencias compartidas con el fin de advertir y precaver en el propio territorio las variantes que pudieran tener ciberataques registrados en otros Estados y en las empresas, instituciones internas por su parte la permanente coordinación y colaboración entre cada Estado y sus respectivas organizaciones internas, público-privadas, entre otras.

RESUMEN DE LA PARTICIPACIÓN DEL CONGRESISTA ALM. JOSÉ CUETO ASERVI

Esta fue una especial oportunidad para desarrollar el manejo de la Resiliencia en nuestro país, como un proceso por el cual nuestro pueblo ha desarrollado gracias a que se enfrenta casi constantemente a innumerables adversidades que le han llevado a enriquecer su fortaleza mediante ese

enfrentamiento a la realidad compleja que, producto de su multiculturalidad y de su rico pero también desafiante territorio y en el marco de su complejidad histórica, no lo es hoy diferente desde el ámbito de los eventos y retos que el mundo moderno impone, en especial desde la óptica de la ciberseguridad, enfrentando modernamente como sociedad la complejidad de los ciberataques, lo que sin embargo ha servido igualmente para desarrollar organizaciones que tanto a nivel de gobierno (p.e. Secretaria de gobierno y transformación digital) como de gobernanza en colaboración con el sector privado, en muchos casos, vienen sirviendo para salir adelante, analizando las perspectivas de superación hacia futuro, para lo que se evalúa no solo las estrategias a seguir cuanto por demás, la regulación del marco de enfrentamiento entre la tecnología y la ética, lo que ha llevado en múltiples -aunque no suficientes- normas producto de la legislación peruana que promueven el análisis de casos en concordancia con la legislación en desarrollo concordante con una constante evaluación que utiliza mecanismos de transparencia que pretenden respetar y cuidar de no trasgredir los límites de la ética y la dignidad de la persona, y que en sucesivos parlamentos dentro de un ordenamiento constitucional estable se va trasladando paulatinamente en determinados casos a la legislación a nivel de políticas como de geopolíticas de gobierno.

6.3 Resumen de algunas de las ponencias, tiempos de debate y participación llevados a cabo durante el segundo día del Foro, registrado con fecha martes 18 de abril de 2023.

"**El Metaverso**".
ESTRADA, Mónica

El Metaverso es un nuevo concepto que nos remite a un "universo paralelo" de modelo 3D, en el que podemos encontrar espacios y tiempos distintos a los reales; se trata de una versión (una nueva) diferente del "*internet*" que permitiría a los usuarios virtualmente hacer o llevar su vida (una vida distinta) a través del *internet*, propiamente inicio a través de los video-juegos y se proyectaría a un escenario (o vida) por la que se pueda interactuar, trabajar, inclusive adquirir propiedad y adquirir o transaccionar riqueza.

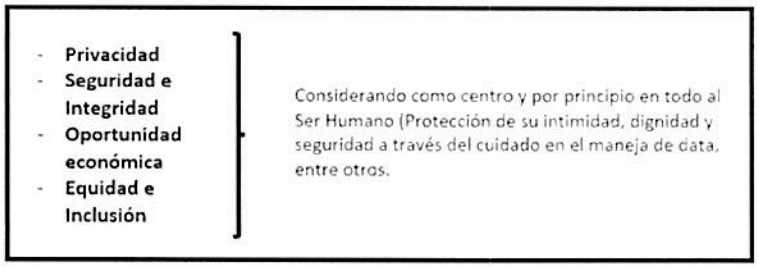
Este es un concepto deducido y visto a través de la propia percepción luego de las exposiciones y debates durante el Foro y sobre esto se agregan las observaciones de Mónica Estrada por las que describe todo lo digital que se maneja hoy de manera social e interconectada.

Estrada señala además que, el Metaverso concentra desde ya todo lo que existe actualmente como el "*whatsapp*", "*Facebook*", "*Instagram*", entre otros

(desde experiencias inmersivas); es aquí que se habla de conceptos como "realidad virtual" o "realidad aumentada" que son espacios en los que se van a reducir las limitaciones físicas como los casos del trabajo (remoto) y la colaboración (p.e. tratamientos médicos remotos) o en aspectos de educación, el "aprendizaje inmersivo" por el que los alumnos puedan estudiar "junto a otros" pero "sin estar juntos físicamente".

Este es el universo de los cambios incluso de sentidos, entre ellos se puede citar las "sensaciones" como la de precisamente estar junto a otro mediante el uso de cámaras, todo lo que permitirá incluir y desarrollarse también a ciertos grupos con determinadas discapacidades físicas.

Innovación responsable; implica la idea de aprender del pasado y sentar las bases para el futuro.



No obstante lo señalado, es difícil para los Estados desarrollar una efectiva interoperabilidad, en la medida en que existen muchas empresas dedicadas a ello, sin embargo la forma de hacerlo podría ser a través de la generación de "políticas públicas" y el modo de propender a ellas es mediante la constante observación de las acciones de la comunidad en cada región, por ejemplo, en el desarrollo de Foros como este es que eso se lleva a cabo, advirtiendo de las amenazas que afectan la ciberseguridad comparando los aspectos comunes en la generación de confianza mediante la cual sea posible una eficiente colaboración entre Estados con el fin de propender a la ayuda mutua en este nuevo mundo digital.

"**Los desafíos de la seguridad frente a la Inteligencia Artificial**".
GUTIERREZ, Juan Raúl

Existen muchas formas de analizar el desarrollo de la inteligencia artificial (IA) en el marco de una verdadera "revolución" moderna, una de ellas es la que se sustenta en los algoritmos inteligentes que sirven para apoyar todo tipo de escenarios sociales (toma de decisiones a nivel económico, social y preferencial a nivel especifico); se utilizan para ello diferentes métodos de

desarrollo de dichos algoritmos y cada uno de ellos con cada vez menor intervención humana.
Sucede esto también en algunos casos en el campo jurídico, sin embargo, ¿es procedente dejar al ámbito de la lógica matemática, la generación de una decisión sobre la libertad de las personas o sobre determinados derechos u obligaciones de estas?

En este campo (el jurídico) por ejemplo, la IA tiene dos lados uno luminoso que sirve para ayudar en la consolidación de los derechos de las personas y otro oscuro en el que el ser humano pierde el control sobre sus derechos que es cuando se generan derechos dispares (muchas otras necesidades y muchas otras diferencias) que generan desarrollo asimétrico porque muchos no tienen siquiera internet.

En el campo privado se ha visto que las propias empresas han tenido que crear sus propias defensas para evitar inequidades y en el ámbito político grandes son los desafíos que enfrentan los parlamentos para proteger a los ciudadanos de forma tal que siempre se facilite el desarrollo de la IA pero sin que ello afecte directamente los derechos de las personas; para ello se propugna una "dignidad digital" con el objetivo de prevenir y precaver las conductas humanas antes de la generación del daño.

"**Aplicaciones especiales de ciberseguridad**".
ZAMORA ACEVEDO, Pilar

Los efectos de la actividad humana en el medio ambiente son indiscutiblemente graves; el campo de la cibernética es obvio que no esta aislado de este tipo de actividades y concurrentemente existen altos riesgos de afectar el medio ambiente desde la propia "gestión de riesgos" en los aspectos variables de predicción en aspectos meteorológicos entre otros.

En este aspecto, la tecnología se orienta por ejemplo al control y apoyo mediante observación satelital, análisis de data y flujo de información, sistemas y estructuras, que generan diversos proyectos en diferentes organismos estatales para contener posibles ataques de ciberseguridad.

6.4 A MODO DE CONCLUSIONES DEL FORO DE SEGURIDAD DE LAS AMÉRICAS

Como se ha hecho notar y apreciado, modernamente el *internet* y junto a el desarrollo de la Inteligencia Artificial, no obstante esta ultima un producto de la inteligencia humana, han traído aparejados altos riesgos y consecuentes daños principalmente producidos también por la inconducta humana

mediante la cual se utiliza también el "lado oscuro de la IA" para generar por medio de *malwares* daños a terceros en provecho de quienes ilícitamente, lo mismo que en el mundo real aprovechan la virtualidad de un mundo paralelo (también conocido como *Metaverso*) para afectar el orden establecido en provecho propio de forma ilegal.

Es responsabilidad de los Estados mantenerse en constante interconexión, conocimiento, desarrollo y colaboración inter pares para estar en condiciones de combatir el llamado *cibercrimen* en el marco de lo que conocemos también modernamente como una nueva aspiración llamada "*ciberseguridad*".

Si bien la inteligencia humana da origen a los algoritmos que desarrollan la (IA), es esta ultima la que está empezando a dar mayores beneficios en múltiples campos del quehacer humano, lo que es fácil apreciar modernamente especialmente en la salud, el transporte, la seguridad en la producción de múltiples bienes y servicios, pero principalmente en la administración y gestión de la llamada "*big data*" y en general del conocimiento asequible mejorando las condiciones de la educación y de la formación en sus nuevas plataformas de acceso.

Hay mucho por desarrollar en el campo de la IA, pero también grandes son los retos que paralelamente tienen los Estados a través de sus parlamentos por los que lograr implementar paralelamente los niveles de seguridad necesarios para hacer frente a los acelerados avances de la IA y de la seguridad en el *Metaverso* que siendo aspectos que coexisten pueden tener injerencia y convertirse en amenazas per se, independientemente de la *ciberdelincuencia* por ejemplo en campos como el jurídico en el que, la IA tiene dos lados uno luminoso que sirve para ayudar en la consolidación de los derechos de las personas y otro oscuro en el que el ser humano pierde el control sobre sus derechos que es cuando se generan derechos dispares (muchas otras necesidades y muchas otras diferencias) que generan desarrollo asimétrico en un mundo en el que todavía el internet resulta ser un "recurso" escaso para determinadas realidades, inexistente.

6.5 A MODO DE RECOMENDACIONES DEL FORO DE CIBERCRIMINALIZACION DEL CIBERESPACIO "Foro Americano de Seguridad"

Conjuntamente con el "Proyecto de Ley Modelo sobre Delitos Informáticos" que viene trabajando el "Foro Americano de Seguridad" sobre la regulación de los mecanismos dirigidos a prevenir, investigar y sancionar los actos considerados como "cibercrimen" que sirvan para establecer las bases

generales normativas para promover la educación de los usuarios y consumidores del servicios informáticos en el marco de la cooperación y asistencia multisectorial intergubernamental internacional se acordaron dentro de las principales, las siguientes recomendaciones:

- Trabajar para la actualización de la Ley Modelo aprobada por el PARLATINO antes referida;
- Trabajar en conjunto con el Programa de Ciberseguridad del CICTE, de la Organización de los Estados Americanos (OEA);
- Emitir desde el PARLATINO recomendaciones a los países miembros sobre la urgente necesidad de incluir temas de ciberseguridad en el currículo nacional de la educación publica y privada con los fines preventivos correspondientes;
- Discutir en los Parlamentos de los países integrantes del PARLATINO las conclusiones y recomendaciones a que arriban estos programas;
- Promover en los Congresos de América Latina y el Caribe, la urgente necesidad de asignar recursos en el presupuesto nacional con el fin de prevención, control y combate de la criminalidad en el ciberespacio; creando un fondo para la capacitación continua en ciberseguridad dada la permanente actualización del tema;
- Creación de un *Networking* público-privado entre los países que permita compartir recursos técnicos, lecciones aprendidas y experiencias exitosas;
- Creación por parte del PARLATINO, del "Dia Latinoamericano de la Ciberseguridad" para ser adoptado por los países de la región;
- Promover la suscripción y/o ratificación del Protocolo de Budapest en los países miembros del PARLATINO;
- Realizar Foros con ejercicios y juegos de ciberseguridad;
- Elaboración de un diccionario común / tesauro sobre los temas de ciberseguridad y ciberespacio que contribuya a la armonización legislativa y de políticas publicas en América Latina y el Caribe, incluyendo programas de capacitación para adultos mayores y profesores de centros educativos;
- Realización de eventos regionales que permitan que el Ciberbulling, el acoso sexual, la suplantación de identidad sean considerados como tipos penales en las legislaciones nacionales;
- Elaboración de un diagnostico regional de ciberseguridad en lo publico y en lo privado que sustente la toma de decisiones y la creación de una "Agencia común para mitigar los riesgos;
- Realización de mapeos regionales de legislación en materia de ciberseguridad y ciberespacio como insumo para la labor legislativa promoviéndolo en los países de América Latina y el Caribe;

Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
jcueto@congreso.gob.pe

www.congreso.gob.pe

- Promover la prevención y combate de la ciberdelincuencia organizada en el marco de ciberespacio y uso de aplicación para detección temprana de riesgos en el comercio;
- Introducir en las agendas públicas y privadas los temas relacionados a los crímenes digitales cometidos entre Estados;
- Creación de un observatorio regional sobre uso del ciberespacio;
- Fortalecer las unidades de inteligencia e investigación de los países y promover su trabajo regional para compartir información y recursos;

De acuerdo con las recomendaciones antes expuestas y debido a la existencia en nuestra legislación de normas relacionadas a "delitos informáticos", existe en nuestro ordenamiento un conjunto de normas disgregadas que no necesariamente forman parte de una estrategia, por lo que podría decirse que el Perú, no cuenta propiamente con un sistema ni menos una "política" de ciberseguridad que formen parte de un Plan que vaya más allá de las diversas normas relacionadas a este tema disgregadas entre conductas sancionables en el Código Penal y actos ilícitos descritos a manera de prevención propendiendo a una mayor seguridad tanto de la información o data como del espacio (ciberespacio) establecido para su desarrollo, como la Ley N° 30096 de delitos informáticos, la Ley N° 30999 de Ciberdefensa, que tuvo como objeto establecer el marco normativo en esta materia; la Ley N° 27269, de firmas y certificados digitales; la Ley N° 28493, que regula el uso del correo electrónico comercial no solicitado (spam); y la Ley N° 29733, de Protección de Datos Personales.

Por las razones antes expuestas y de conformidad con lo observado a través del presente Informe, se cumple asimismo con referir los avances correspondientes al trabajo que sobre el particular viene realizando el PARLATINO en lo relacionado a la ciberseguridad en el ciberespacio, con el objeto de plantear ante las comisiones parlamentarias por cuya competencia se tenga vinculación con los temas materia de desarrollo e informe por medio del presente instrumento para que, de conformidad con las conclusiones y recomendaciones observadas, se proceda según corresponda en sede parlamentaria.

SB /JC

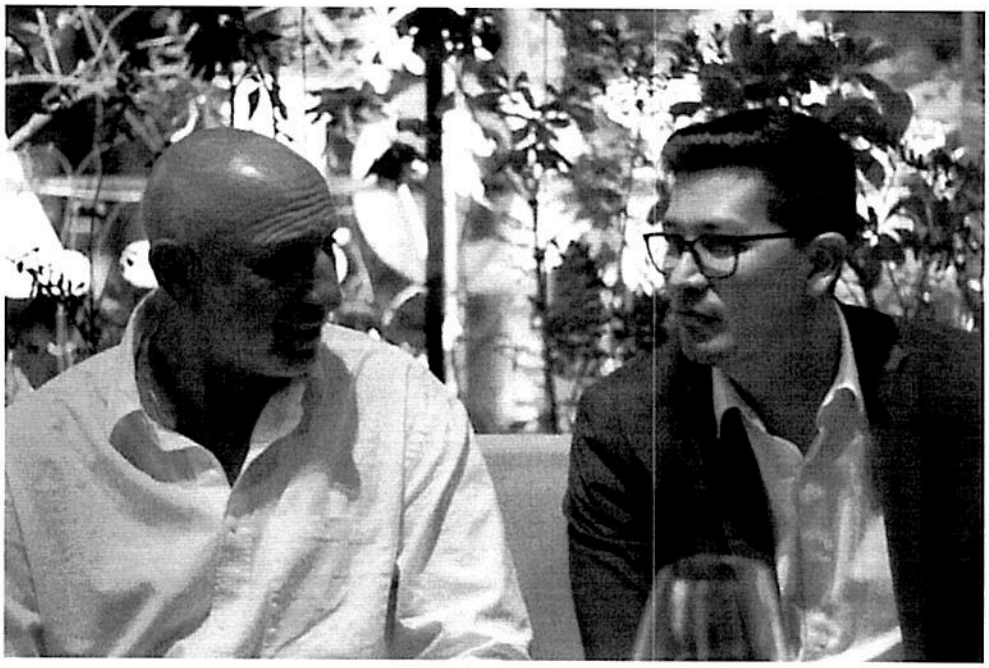
Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
jcueto@congreso.gob.pe

VII. GALERIA FOTOGRAFICA DEL INFORME

"Foro de Seguridad de las Américas" – La Criminalización del Ciberespacio II - Organización. Sesiones de Trabajo – Ciudad de México, abril de 2023.

Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
jcueto@congreso.gob.pe

www.congreso.gob.pe



"Foro de Seguridad de las Américas" – La Criminalización del Ciberespacio II - Organización, Sesiones de Trabajo – Ciudad de México, abril de 2023.

Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
jcueto@congreso.gob.pe

www.congreso.gob.pe

"Foro de Seguridad de las Américas" – La Criminalización del Ciberespacio II - Organización. Sesiones de Trabajo – Ciudad de México. abril de 2023.

Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
jcueto@congreso.gob.pe

"Foro de Seguridad de las Américas" – La Criminalización del Ciberespacio II - Organización. Sesiones de Trabajo – Ciudad de México, abril de 2023.

SB /JC

Edificio José Faustino Sánchez Carrión.
Jr. Azángaro N°468, Oficina 908. Lima - Perú.
Teléfono 01-3117172
jcueto@congreso.gob.pe

www.congreso.gob.pe