WORLD LEGAL SUMMIT

CAPÍTULO MÉXICO 2019

LAWIT
Law + Innovation & Technology

WLS
WORLD LEGAL SUMMIT

FORO JURÍDICO

THOMSON REUTERS

Lawgistic

genius soft

Sistemas

Microsoft

Tecnológico de Monterrey

World Legal Summit es un proyecto que engloba a distintas organizaciones locales. El primer día de agosto se llevó a cabo un evento de análisis al mismo tiempo en más de 40 ciudades de 20 países, en donde expertos locales se sentaron a discutir la problemática nacional y a proponer soluciones. Entre los panelistas se encontraban expertos de los sectores legal, académico, profesional y gubernamental.

La integración de los temas fue consensuada a nivel global, para determinar en qué aspectos prioritarios se debe fijar el alcance de su análisis a través de expertos en las materias de seguridad cibernética, privacidad de datos, máquinas autónomas e identidad y regulación. El diseño que se implementó en todos los países que se sumaron a este importante esfuerzo, fue de apertura en la discusión y diagnósticos en paneles de expertos, con una muy activa participación de los demás invitados a participar en el evento.

La organización del WLS Capitulo México fue encomendada a la firma Lawgistic, a través de su brazo de innovación legal LAWIT, y de la mano con *partners* estratégicos de gran influencia como *Foro Jurídico*, Microsoft, GeniusSoft y LB Sistemas.
Los esfuerzos derivados de esta primera fase del World Legal Summit continuarán con otras actividades para seguir avanzando hacia una mejor regulación de las transformaciones e impactos que generan las nuevas tecnologías. Los contenidos locales, fruto de las discusiones que se tuvieron durante el evento, serán consensados por la sede del World Legal Summit en la oficina de Canadá y se trabajará para crear lineamientos que sean útiles y prácticos, para continuar la discusión de estos temas a la luz de una mayor plataforma que comparta las realidades internacionales, sus retos y oportunidades, y que sumen al esfuerzo de implementar guías que promuevan las mejores prácticas, condiciones, reglas y apoyos, para que los avances tecnológicos en estas áreas se den en un marco que proteja los derechos de las personas, incentive los esfuerzos de desarrollo de reglas y marcos legales que promuevan la equidad, transparencia y legalidad en su implementación.

En breve se estarán dando a conocer los resultados por país y los resultados mundiales.

En México, los paneles estuvieron integrados por los siguientes expertos:

SEGURIDAD CIBERNÉTICA Y PROTECCIÓN DE DATOS PERSONALES

SEGURIDAD CIBERNÉTICA Y PROTECCIÓN DE DATOS

Panelistas

- Adriana Servín Villada - Relaciones Gubernamentales y Asuntos Corporativos SAP.Julio Téllez Valdés - Catedrático investigador.
- Oscar Manuel Lira Arteaga - JusTIC´s Peritos en Ciberdelitos.
- Joel A. Gómez Treviño - Lex Informática Abogados.
- Moderador: Marco V. Herrera - Revista Foro Jurídico.
- Relatora: Karen Guadalupe Castillo Acosta - Thomson Reuters.

Ejes Temáticos

- Analizar y discutir lo que las diferentes jurisdicciones están haciendo para administrar y proteger los datos personales en general y los de los usuarios que realizan operaciones en línea en México.
- Centrarnos en descubrir cómo se protegen estos datos y los diversos mecanismos que se utilizan para administrar la seguridad en línea.
- Analizar los marcos legales y ofrecer ideas a los programadores de diferentes aplicaciones para que tengan en cuenta estos requerimientos con el fin de que desarrollen mejor sus tecnologías.
- Definir cómo puede ayudarnos la tecnología a resolver los problemas actuales.

→ DIAGNÓSTICO

El panel fue moderado por Marco V. Herrera, director de la revista Foro Jurídico. El moderador planteó como pregunta inicial: ¿cuáles son la problemática actual y los riesgos de la ciberseguridad que tenemos en México?

Inició el panel Adriana Servín Villada, de Relaciones Gubernamentales y Asuntos Corporativos SAP, señalando que el reto principal de México es el tema de gobernanza. Destacó que aún existe cierta percepción de que la ciberseguridad es un tema únicamente de empresas, toda vez que se considera que las empresas son las que se encuentran frecuentemente en riesgo y, por ende, deben asumir la responsabilidad de crear sus propias normas para regular el delito. Enfatizó que, en la mayoría de las jurisdicciones del mundo, la ciberseguridad forma parte principal de las agendas de políticas públicas como un tema integral y transversal hacia todos los sectores: público, privado, social y académico. Lo

anterior se debe a que los sistemas de información y comunicaciones operan por igual en todos los sectores y, en consecuencia, estos tienen la misma susceptibilidad de sufrir ciberataques o incidentes de seguridad en su información o sus sistemas. Recalcó que en México falta posicionar a la ciberseguridad como premisa en la agenda pública, toda vez que es uno de los aspectos de política pública transversal más críticos de nuestro tiempo. Por último, manifestó que difícilmente a través de las leyes se pueda cambiar una realidad, por lo que no necesariamente se requiere de una regulación, sino de la construcción y ejecución de un mecanismo de gobernanza e interacción de todos los sectores de la sociedad, liderados bajo una coordinación de política pública.

El Dr. Julio Téllez Valdés hizo alusión a que en México se tiene un retraso de legislación en materia de tecnología. Consideró que una ley no necesariamente limita o restringe, sino que busca emplear una extensión de las políticas públicas con la finalidad de estimular acciones que enriquezcan el sector. Estableció que la tecnología debe verse bajo dos perspectivas: como instrumento o como objeto de estudio para una regulación. En el caso en que la tecnología brinde beneficios sustanciales colectivos, se debe usar la ley como instrumento para incentivar su buen uso; y en el caso de que la tecnología sea empleada para provocar daños o vulnerar los derechos de las personas, sirve para erradicar dichas conductas. Recalcó que nuestro país tiene una regulación tardía e incompleta en los temas de protección de datos personales y ciberseguridad. Manifestó que no existe claridad en saber si, al crear una legislación, no quieren hacer las cosas o no quieren hacerlas bien, o una ineptitud ante la problemática. Destacó lo tardío de la legislación federal, toda vez que a nivel estatal y municipal se reguló primero el tema de protección de datos personales. Por último, mencionó que México pidió formar parte del Convenio 108, Consejo de Europa del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos personales; del Reglamento General de Protección de Datos y del Convenio sobre la Ciberdelincuencia suscrito en Budapest el 23 de noviembre de 2001, del que México pidió ser parte hace muchos años y no fue adherido.

El abogado e ingeniero Oscar Manuel Lira Arteaga destacó que no existe la ciberseguridad, toda vez que hoy en día es un modismo para los ingenieros. Sustentó lo anterior al considerar que la ciberseguridad se busca “solucionar” con herramientas, las cuales son adquiridas buscando un mecanismo de defensa. Al presentarse un incidente sobre ciberseguridad, los ingenieros y abogados se encuentran en una dualidad. Comentó que los ingenieros saben recuperar sistemas; sin embargo, no saben cómo identificar, fijar y preservar evidencia para ser presentada ante las autoridades. Por lo que el trabajo del abogado compete en el Ministerio Público, éste debe recabar todas las evidencias del incidente; y al existir un desconocimiento

de ciberseguridad, genera una lentitud en los procedimientos jurídicos y en la clarificación de delitos. Manifestó que la ciberseguridad no funciona en México porque se han copiado estandartes de otros países que no funcionan en el país. Expresó que es importante la autorregulación y sugirió la creación de un artículo 190 bis en la Ley Federal de Telecomunicaciones y Radiodifusión, relacionado con los datos que se deben preservar en comunicaciones digitales, como son la dirección IP, hora y fecha. En México no existe legislación, ya que hay vacíos legislativos importantes que no obligan a los proveedores de internet a almacenar los datos de conexión que permitan a las autoridades rastrear lo generado a través de la web.

Joel A. Gómez Treviño, de Lex Informática Abogados, señaló que existe un desconocimiento por parte de los operadores jurídicos sobre el tema de delitos informáticos. Asimismo, mencionó que en México se cuenta con más de 20 años de legislación sobre la materia y destacó que, a pesar de ello, ningún operador jurídico conoce sobre el tema ni cómo manejarlo ante las instancias judiciales. Destacó que es un problema de sectorización, el cual consiste en dejar a la industria que busque su propia regulación o se regule con sus propios Códigos. Mencionó todas las leyes federales que regulan la protección de datos por medio del secreto profesional e industrial, por lo que manifestó que se deben unificar criterios en un tipo de cuerpo colegiado, ley o norma, con la finalidad de homologar criterios y que en cualquier lugar se pueda entender qué se debe proteger, qué se debe considerar como información confidencial, qué debe considerarse como ciberseguridad.

→ ANÁLISIS

El precio de los datos personales en aplicaciones es desconocido por los consumidores, así como el uso de estos; por lo que resultan ser la materia prima para dirigir anuncios, guiar el comportamiento en línea y capacitar el sistema de inteligencia artificial. Ahora bien, se tiene que crear conciencia en México para la protección de los datos personales, toda vez que en algún momento los usuarios se sentirán vulnerables ante el sistema y, por lo general, desconocen cómo actuar ante dicha situación, así como ante quién apoyarse. Se debe crear una cultura de protección de datos personales a través de las Cámaras, organizaciones e instituciones educativas con la finalidad de abarcar mayormente a la población que tenga acceso al uso de internet. Se consideró que una cultura de protección es más fiable que invertir en tecnología, toda vez que en México ya se cuenta con la suficiente tecnología, por lo que hay que enseñar el buen uso de esta.

La autorregulación en las empresas e industrias puede ayudar a que el gobierno ponga como premisa los temas de ciberseguridad y protección de datos personales en la agenda pública, por

lo que es necesario que la autoridad sea consciente del aporte que el sector industrial y empresarial genera. Es importante que el Plan de Desarrollo contenga los temas de ciberseguridad y protección de datos; la agenda de México debe contemplarlos responsablemente en conjunto con el sector privado, el público y la academia. La ignorancia en el tema dentro del país se muestra cuando, en los eventos en los cuales se intercambian ideas con especialistas de otros países, se denota que México no cuenta con la infraestructura para combatir dichos delitos. Asimismo, la ciberseguridad cuesta más dinero, por lo que las empresas, al no contar con políticas adecuadas que establezcan qué necesitan, qué tienen y cómo se van a proteger, generan una incertidumbre de hacia dónde se debe dirigir el sector para protegerse. Mediante la unión se puede llegar a mejores cosas; las empresas deben ver a los consumidores como coadyuvantes para hacer mejoras y exigir al gobierno mecanismo idóneos para la protección.

Por otro lado, en cuestiones educativas, las facultades de Derecho e Ingeniería deben contemplar los temas de ciberseguridad y protección de datos, toda vez que en la Facultad de Ingeniería no se encuentran generando ingenieros que cuenten con la capacidad de actuación en los temas; así como en la Facultad de Derecho no se encuentran enseñando sobre el tema de ciberseguridad ni protección de datos. Existe una arrogancia del conocimiento en los temas, por lo que hay un rezago en los temarios de dichas profesiones en México. Las generaciones venideras no tienen la cultura en el uso de la tecnología, debido a que se encuentran en un desconocimiento, lo cual genera que los jóvenes pueden caer en trata de personas y/o tráfico de órganos. Se debe trascender para mejorar la base de México en los temas. Mediante la creación de perfiles híbridos, con la finalidad de que existan más ingenieros que cuenten también con estudios de derechos y viceversa, con la finalidad de que puedan abarcar el área técnica y legal.

Por último, por parte de la función pública se refirió que el tema de ciberseguridad se encuentra reestructurando su infraestructura, con la finalidad de garantizar a la población mejor protección y fortalecer al grupo de ciberseguridad. Destacó que la reforma a la Ley de Telecomunicaciones y Radiodifusión fue un éxito al ser apoyada por los sectores y actores políticos; sin embargo, a la hora del litigio saltan diferencias por causa de intereses de los operadores de las marcas y empresas. Asimismo, se atienden las consultas que se plantean en el Poder Legislativo; mediante ellas se busca la armonización constitucional con el tema. Manifestaron que se encuentran realizando una reforma dentro de la Secretaría con la finalidad de que exista un área encargada del tema de ciberseguridad.

→ PROPUESTAS

El régimen se debe basar en dos puntos importantes como son los usuarios y

las nuevas tecnologías, toda vez que el avance de la transformación digital nos va a sobrepasar.

Para legislar se debe tener conceptos precisos y claros, tener a la sociedad como parte fundamental de la legislación, y la actividad a regular debe tener una perspectiva de desarrollo e innovación.

Se debe partir de la política pública y las leyes deben ser tildadas, acotadas y sancionadoras. Al coadyuvarse deben estimular el buen uso de las tecnologías y sancionar el uso indebido para solucionar los problemas que aquejan a la sociedad. Para la creación de un Código moderno se le debe agregar a todos los artículos "por cualquier medio", así como homologar criterios.

El uso del Protocolo IPv6 podrá hacer que cada ciudadano mexicano cuente con su propia cuenta de Internet, con la finalidad de navegar con seguridad.

Se debe tener un ecosistema de ciberseguridad, el cual consiste en una industria local fuerte, que tenga profesionales que puedan asesorar a los sectores públicos y privados para proteger la industria digital; estadísticas confiables (neutras); tecnología para el monitoreo de protección y defensa para el entorno digital; medidas de seguridad físicas, técnicas y administrativas establecidas en la Ley Federal de Protección de Datos Personales; un conjunto de leyes y políticas públicas estrictas en materia de ciberseguridad; desde una perspectiva transversal, unificar criterios y cuerpos normativos para que sea más fácil su aplicación; y contar con autoridades y abogados capacitados y conscientes en la materia para garantizar una labor eficaz de persecución.

Por último, mediante la educación se debe generar una cultura del buen uso de internet a los más jóvenes con la finalidad de protegerlos de delitos y de llegar a ser vulnerables con los datos que arrojan a Internet.

MÁQUINAS AUTÓNOMAS

En un esfuerzo por concientizar a especialistas en diversas áreas del conocimiento, sobre los grandes retos y oportunidades que se presentan ante el acelerado auge que ha representado el desarrollo de las tecnologías relacionadas con la inteligencia artificial, el pasado 1 de agosto de 2019 se llevó a cabo el World Legal Summit, capítulo México.

Este evento contó con la participación de ingenieros, abogados, empresarios y otros expertos, quienes conformaron tres paneles de discusión en los que se abordaron temas como Ciberseguridad, Identidad y Gobernanza, y Máquinas Autónomas.

MÁQUINAS AUTÓNOMAS

Panelistas

- Adi Corrales Magallanes - Director de Sistemas Automatizados del Centro de Ingeniería y Desarrollo Industrial.
- Christian Palacios - Manager en el área de Strategy, Analytics & Cognitive and M&A de Deloitte.
- Luis Gerardo Fonseca - Exdirector General de Aeronáutica Civil en la Secretaría de Comunicaciones y Transportes y actual consultor en Inteligencia Futura.
- Moderador: Daniel Santiago Acevedo Sánchez - Gerente de Proyectos Estratégicos en Galicia Abogados S. C. y Founder/ Host en Legaltech en español.
- Relatora: Karla Capetillo Núñez - Thomson Reuters.

Ejes Temáticos

- ¿Qué son las máquinas autónomas?
- ¿Cuál es el impacto que tendrá la tecnología en el campo laboral y cuál deberá ser la participación del Estado para atender este fenómeno?
- ¿Cuáles son los retos aparejados al desarrollo tecnológico?, desde el punto de vista legal y de políticas públicas.

→ CUARTA REVOLUCIÓN INDUSTRIAL

Al inaugurar el panel, el moderador Daniel Acevedo hizo referencia a Klaus Schwab —fundador y presidente del Foro Económico Mundial—; quien en un interesante artículo publicado en 2015, explica el inicio de una nueva etapa dentro del desarrollo de la humanidad, siendo éste un fenómeno de cambio al que Schwab denominó cuarta revolución industrial o revolución de la información.

Así, el exponente destacó que estos cambios, resultado de la crisis económica de 2008, hay que considerarlos como una nueva etapa dentro de las revoluciones naturales de la evolución humana, que, a diferencia de las anteriores, se está desarrollando a mayor velocidad, razón por la cual la humanidad pudiera no estarse preparando adecuadamente; lo que nos hace cuestionar, ¿a qué se refiere Schwab al indicar que la humanidad pudiera no estar preparada?

En otro de los trabajos de Schwab, The Fourth Industrial Revolution, (2016), nos habla de este nuevo paradigma, además de presentar algunas teorías de expertos en la Universidad de Oxford, con las cuales ofrece datos interesantes con respecto de la posible transformación en la fuerza laboral a nivel mundial, debido a la desaparición de empleos caracterizados por ejecutarse mediante actividades repetitivas y de fácil automatización.

Dicha automatización de la experiencia humana se realiza por medio de: sistemas que tratan de pensar por nosotros, es decir, "inteligencia artificial" y de máquinas que hacen cosas por la humanidad.

Bajo esta perspectiva, el moderador invitó al ponente Adi Corrales a responder dos sencillas preguntas, ¿qué es una máquina autónoma?, y, para el caso de México, ¿cuáles considera ya se encuentran implementadas?

→ ¿QUÉ ENTENDER POR MÁQUINA AUTÓNOMA?

El tema es considerado complejo y aunque no hay una definición exacta, si se analiza un poco de la historia de la evolución del hombre es posible determinar de dónde viene el término y a partir de cuándo puede considerarse que las máquinas autónomas empezaron a formar parte del desarrollo de nuestra sociedad.

En este sentido, el ponente explica las siguientes etapas:

- **Primera revolución industrial:** Se crea la máquina de vapor y el hombre descubre que puede transformar la energía para hacer un trabajo. En esta etapa empiezan a suplantarse trabajos humanos por los que los nuevos instrumentos son capaces de generar.
- **Segunda revolución industrial:** Inician las producciones en masa, si bien las máquinas permiten líneas continuas de producción, éstas requieren de amplias líneas de empleados que las operen.
- **Tercera revolución industrial:** Se da en 1959 con el invento del primer controlador lógico programable o PLC, considerado como la primera máquina autónoma o computadora en la que se programa un set de instrucciones y ya no es necesaria la intervención humana.
- **Cuarta revolución industrial:** Se da en el año 2000 con la revolución de la información, destacando la necesidad de la obtención de datos.

De lo anterior se desprende el concepto universal de máquina autónoma, es decir, es aquella que desarrolla tareas sin intervención humana, sin embargo, esta definición se puede quedar corta, si se toma en consideración que las máquinas de la cuarta revolución industrial ya son sistemas capaces de reproducir tareas y que gracias a los parámetros internos que el desarrollador implementa son capaces de auto medirse, reaccionar ante el ambiente que les rodea, poseer movilidad propia

y, sobre todo, actuar en consecuencia de decisiones propias.

Las máquinas autónomas pueden dividirse en dos categorías: software (por ej. máquinas que hacen big data o de protección de datos) y hardware, siendo este último el que se destina a crear productos para el consumidor y al uso industrial.

En México, los sistemas automatizados han penetrado el ramo automotriz ante la necesidad de mejorar los tiempos de producción, así como de abaratar sus costos. Se estima que las empresas que deciden invertir en tecnología autónoma tienen retornos de inversión de dos a tres años y una disminución de su fuerza de trabajo operativa de cinco a uno.

Lo que nos lleva a preguntarnos, ¿cuál va a ser el rol de los empleados desplazados y de aquellos que por las características propias de su formación profesional sean susceptibles de ser sustituidos por algún tipo de tecnología?

¡Al respecto, Christian Palacios hizo énfasis en los amplios desarrollos de software que ya realizan algunas tareas de manera más eficiente que cualquier empleado y a un menor costo, es decir, los robots hoy "aprenden" a replicar lo que una persona hace con un teclado y un mouse, por ejemplo, revisiones menores de contratos, emisión de pagos, conciliaciones contables, solo por mencionar algunas.

Lo anterior, debe ser entendido como un reto de adaptación para la sociedad, pues si bien este tipo de cambios genera resistencia en los equipos de trabajo, las empresas deben acompañar a sus empleados con una correcta gestión de esos cambios y apoyarles en la adaptación de esta nueva "cultura tecnológica", así se podrá entender que la automatización, además de permitir la reducción de errores, mejorar la calidad en los procesos y disminuye los costos; abre opciones para desarrollar nuevas habilidades, por ejemplo, se vuelve necesario que haya quien se encargue de que los robots realicen o desempeñen las actividades para las que se les programó y desde el punto de vista técnico debe haber un responsable, capaz de dar soporte si algo sale mal.

Así, en la medida en que las industrias, las organizaciones y los gobiernos conozcan las capacidades de la tecnología, eventualmente generarán una evolución del perfil y las capacidades que hoy poseen las personas, lo que permitirá soportar la coexistencia entre humanos y máquinas.

Para que esta evolución del perfil sea una realidad, es necesario considerar cambios en la preparación académica de la sociedad, tanto de la que ya está teniendo dificultades para convivir con las nuevas tecnologías, como de las generaciones futuras. De ahí surgen las siguientes interrogantes, ¿se tendrá el tiempo suficiente para formar a los obreros y/o profesionales desplazados por ese sistema automatizado a efecto de que se adapten al nuevo paradigma laboral en el corto plazo?, ¿cómo se vislumbra la transformación del mercado a 20 años?

→ RETOS Y EXPECTATIVAS DE LA IMPLEMENTACIÓN DE MÁQUINAS AUTÓNOMAS EN EL ENTORNO LABORAL

Al abordar este tema, expertos y público consideraron que la sociedad sigue sin estar preparada, por ello urge hacer conciencia del enorme reto que ya se está viviendo.

Acerca de este reto, Luis Gerardo Fonseca opina que debe formarse a la sociedad a través de conceptos que le permitan entender la aplicación y los alcances de la inteligencia artificial, es decir, se debe invitar a la población a ser interdisciplinaria lo que le permitirá involucrase activamente en el desarrollo de las nuevas tecnologías.
Como se dijo anteriormente, este no es el primer proceso de automatización e innovación tecnológica de la historia, y se sabe que todos han provocado cierto desplazamiento laboral debido al incremento de la producción, el tema es que a medida que esos cambios se hacen más rápidos la sociedad tiene menos tiempo de absorber esto de manera natural por lo que requiere la intervención del Estado para facilitar la transición a esta condición, al generar las competencias necesarias, apoyar la reconversión de la fuerza laboral y promoviendo que la nueva industria surja de una manera más sencilla.

Para concluir este punto, Luis Gerardo Fonseca indicó que la automatización de las máquinas que dependen de la inteligencia artificial y del aprendizaje, tienen tres efectos en el mercado laboral:

- El desplazamiento;
- La transformación de los roles de los trabajadores, y
- El incremento de la capacidad de desarrollar nuevas tareas de mayor valor.

En el largo plazo se vislumbra un mercado laboral transformado, en el que para que exista un correcto funcionamiento de las máquinas autónomas, será fundamental la intervención del ser humano transformado y adaptado al nuevo cambio, pues sólo así se podrá alcanzar el máximo potencial de la inteligencia artificial.

Entonces, si el desplazamiento del ser humano en el mercado laboral es un fenómeno inevitable derivado de la cuarta transformación industrial, ¿qué papel debe jugar el Estado en relación con la generación de políticas públicas para atender ese fenómeno?

→ POLÍTICAS PÚBLICAS EN MATERIA LABORAL

A decir de Luis Gerardo, lo primero que debe hacer el Estado es un diagnóstico de la situación en el que se identifiquen las industrias que estarán participando en esos procesos de cambio, esto permitirá reconocer el tipo de afectación que se tendrá en el mercado laboral; además se debe detectar el perfil que tienen esas fuerzas laborales sujetas a desplazamiento,

a efecto de planear adecuadamente la reconversión de sus roles y funciones.

Asimismo, las instituciones públicas deberán identificar las oportunidades que representan la adopción de procesos de automatización, ya sea con la creación de empresas mexicanas que participen en el diseño, construcción, despliegue y operación de máquinas autónomas o de agentes inteligentes, o apoyando a las nuevas industrias en su implementación.

También se espera que el Estado intervenga en la formación de competencias, es decir, que participe como agente de cambio en el desarrollo del capital humano, ya que actualmente la rigidez de nuestro sistema educativo hace aún más compleja la incorporación de la sociedad al mundo tecnológico. Para ello, se sugiere:

- Fomentar en los jóvenes estudiantes el interés por las áreas de la tecnología, la ciencia, las ingenierías y, por supuesto, las matemáticas, esto a través de mayores oportunidades de ingreso a carreras orientadas a dichos temas.
- Generar mayor oferta académica en cuanto a diplomados, especialidades, maestrías, seminarios y cursos de actualización para quienes tienen una carrera y necesitan adquirir competencias para desenvolverse en el nuevo entorno.
- Flexibilidad del Estado en los procesos de reconocimiento de competencias adquiridas a través de vías no tradicionales, es decir, estudios hechos en plataformas digitales.

→ RESPONSABILIDAD POR EL USO DE MÁQUINAS AUTÓNOMAS Y BREVE ANÁLISIS DEL CASO TESLA

Una vez desarrollado el diagnóstico, los ponentes analizaron la responsabilidad frente al mal funcionamiento de una máquina, considerando los diversos componentes y factores que se involucran en su desempeño.

Para algunos, la delimitación de responsabilidades suele ser ambigua, ya que actualmente los desarrollos en materia de aeronáutica son los únicos que pueden considerarse capaces de tomar decisiones acertadas, con escasas probabilidades de falla; el resto de los desarrollos, incluso los automotrices, aún dependen en gran medida del soporte y la intervención humana.

Al respecto, Luis Gerardo Fonseca refiere que la mayor carga de responsabilidad frente a la falla de una máquina autónoma, llámese software o hardware, recae principalmente en el usuario, toda vez que él es quien decide adquirir el bien, otorgándole a éste la potestad de actuar por cuenta propia.

En ese sentido, el ponente destaca que el verdadero problema radica en que no hay reglas claras, ni criterios formales que puedan determinar si a una máquina se le

da el funcionamiento adecuado, así como tampoco existen reglas de revelación que le permitan al usuario conocer los alcances de su responsabilidad, aunado a la ausencia de autoridades preparadas para hacer juicios de valor sobre el tema.

Claro ejemplo de esto es el ya conocido caso de un ingeniero de Apple quien falleció a bordo de su coche Tesla hace algunos meses y que no ha podido resolverse por la falta de claridad respecto de si la falla provino del piloto automático incluido en el modelo del vehículo, o fue responsabilidad del conductor quien, según se sabe, reportó ante su concesionario repetidas fallas del sistema en la misma zona en la que ocurrió el accidente e inclusive recibió algunas alertas sonoras y visuales del sistema de navegación, y aun así siguió haciendo uso del vehículo.

Por lo anterior, los panelistas coincidieron en que es importante que el usuario que decide adoptar alguna tecnología autónoma, esté siempre consciente e informado de las implicaciones y los alcances de su adquisición, pues al no existir reglas claras y límites perfectamente delimitados de lo que puede hacer un robot y/o una máquina inteligente, hay pocas posibilidades de deslindarse de cualquier tipo de responsabilidad, además de que se vuelve una obligación estar al pendiente de las decisiones y el correcto desempeño de la máquina.

Durante su intervención, Christian Palacios mencionó que delegar la responsabilidad a la máquina autónoma no es un comportamiento que se debe asumir de manera inmediata pues sólo hay que considerarla como un asistente de la actividad humana para realizar acciones de manera autómata y no tomarla como la desvinculación del humano de dicha actividad.

Retomando el caso de Tesla, uno de los abogados asistentes puso en contexto que la norma que regula la responsabilidad de las máquinas es mucho más basta que la simple responsabilidad extracontractual, pues si bien existe la teoría del riesgo creado, por la que debemos entender que si se usa una máquina que por su naturaleza es peligrosa, te vuelves responsable del daño que cause, también es cierto que existe la responsabilidad contractual para las empresas especializadas que asesoran a sus clientes para adoptar cierta tecnología, por lo que no les es posible alegar que no tienen los datos suficientes ante cualquier tipo de incidente o daño, cuando sí los tuvieron para brindar el servicio de asesoría. Cabe señalar que quienes asesoran, ya sean abogados o ingenieros, tienen responsabilidad civil contractual por su asesoría e incluso por su negligencia o “no saber”.

Aunado a lo anterior, se debe considerar la responsabilidad por incumplimiento legal, es decir, si se incumple una disposición legal porque alguien usó una máquina, por ejemplo: una persona utiliza un software que sirve para contratar personal, sin embargo,

éste falla y no contrata a alguien por su condición de transgénero, es decir, el software discrimina a la persona, y al respecto, existe una ley que prohíbe la discriminación; es claro que se está incumpliendo una norma y la responsabilidad recae, en ese caso, en la persona que decidió utilizar la tecnología en su proceso de contratación; pero ¿qué hay de un posible incumplimiento por falla en el diseño?, lamentablemente, en México no hay disposiciones legales que obliguen a los desarrolladores a incorporar como tal la legislación del país en el que comercializan sus desarrollos, no obstante, podría ser un buen momento para que los legisladores consideren incluir en la ley mexicana un capítulo de cumplimiento por diseño.

Posterior al tema de responsabilidad por mal funcionamiento, los panelistas abordaron el tema de la regulación, desde el punto de vista de si la existencia de un marco regulatorio restringe o no las posibilidades de desarrollo de la inteligencia artificial y con ello el avance de las máquinas autónomas.

→ EL ESTADO Y LA REGULACIÓN PENDIENTE

Todo proceso de innovación genera disrupciones y al final la sociedad los asimila y adopta a favor de su vida cotidiana, sin embargo, la incertidumbre se hace presente cuando el cambio implica delegar la facultad de toma de decisiones a una máquina de la cual se desconoce o no se tiene la seguridad de cómo fue creada y de en qué basará su funcionamiento.

Se sabe que la función de estas máquinas depende de un "agente inteligente" que actuará según la función/objetivo que le sea programada a través de una serie de datos y la recepción de insumos que le permitan "tomar la mejor decisión".

De los elementos que conforman al agente inteligente, se debe tener en cuenta que:

- En la recepción de insumos. Se debe asegurar que los datos utilizados para el aprendizaje automático del agente estén libres de sesgos y de criterios discriminatorios, esto con el fin de reducir los sesgos sociales y de no transmitirlos o mantenerlos.
- Impacto de las decisiones. La toma de decisiones a cargo de las máquinas autónomas debe coincidir con las reglas para su interacción con los seres humanos y establecer medidas especiales para su utilización por parte del gobierno o de una autoridad.

Para Luis Gerardo Fonseca no se trata de regular la tecnología, sin embargo, sí considera que al tener un agente inteligente actuando en el entorno social se deben tener las reglas para que todo el mecanismo con el que fue creado asegure un comportamiento aceptable dentro de la sociedad.

Cabe señalar que en México existe una pequeña, aunque ignorada, regulación de los agentes inteligentes, esto se debe a que

no hay forma de implementarla ya que fue tomada de la Directiva 95 de la Unión Europea.

El artículo 112 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, denominado Tratamiento de datos personales en decisiones sin intervención humana valorativa, establece que cuando un agente inteligente ocupa una decisión tomando en cuenta datos personales, esa persona debe ser informada para saber cómo se puede revertir dicha decisión.

→ SUGERENCIAS AL PLAN NACIONAL DE DESARROLLO TECNOLÓGICO

En México, el Consejo Nacional de Ciencia y Tecnología (CONACYT) es el organismo público encargado de articular las políticas públicas del gobierno federal y promover el desarrollo en materia de investigación científica, desarrollo tecnológico e innovación a fin de impulsar la modernización tecnológica del país.

Durante la gestión del Dr. Enrique Cabrero Mendoza, en el CONACYT se mantuvo una dirección altamente tecnificada, además se implementaron diversas prácticas relacionadas con la industria 4.0, lo cual permitió al Consejo estar a la vanguardia en materia de tecnología, sin embargo, las políticas del gobierno actual han decidido dar un enfoque distinto a las políticas públicas del país.

Al respecto, los panelistas señalaron que no se deben abandonar los avances en el desarrollo tecnológico, por el contrario, se debe aprovechar e involucrar a la industria, al gobierno, a la academia, a la sociedad civil, incluso a los agentes de cambio en el ambiente, lo que permitiría darle un enfoque social para avanzar en conjunto a una industria 5.0.

Aunado a esto, debe invertirse en el fortalecimiento de las carreras técnicas y en la creación de programas flexibles que permitan el reconocimiento de habilidades, que posteriormente podrán ser aprovechadas en beneficio de la transformación del Estado.

→ CONCLUSIONES

- Las máquinas autónomas son el componente principal de la cuarta revolución industrial, que no es más que una nueva etapa de la evolución de la humanidad.
- Una máquina autónoma es aquella que desarrolla tareas sin la intervención humana, esto a través de los parámetros internos que el desarrollador le ha proporcionado, es capaz de auto medirse, de reaccionar ante el ambiente que le rodea, de poseer movilidad y, sobre todo, es capaz de tomar decisiones propias. Actualmente estas máquinas tienen aplicaciones de servicio e industriales y se dividen en software y hardware.
- Si bien la implementación de

tecnología en el ámbito laboral aporta a la industria mejoras en la calidad de sus procesos, disminuye considerablemente los errores humanos, así como los costos de producción, es importante acompañar e instruir a los empleados en este proceso de cambio para que la coexistencia entre máquinas autónomas y de recursos humanos implique una evolución del personal y no su desplazamiento del proceso productivo de la sociedad.

- Por lo que respecta a la imputabilidad de la responsabilidad legal por el mal funcionamiento de una máquina y el perjuicio que éste puede causar aún hay mucho por definir, sin embargo, una realidad es que el sujeto que decide incorporar a su vida una máquina o un sistema capaz de "tomar decisiones por sí mismo", nunca debe dejarlo o permitirle actuar sin supervisión. Por ello es importante:

    - Generar conciencia en el usuario de los alcances y capacidades que tiene la tecnología que está adquiriendo.
    - Se debe exigir al fabricante que implemente en su tecnología la capacidad de auto diagnosticarse, para disminuir así posibles fallas en su uso.
    - Deben implementarse reglas y existir registros que faciliten la investigación de cualquier incidente que haya sido provocado por el uso de una máquina autónoma.
    - Exigir a los fabricantes que tengan niveles regulatorios de calidad.

- El caso de Tesla es un claro ejemplo de la necesidad que tiene la sociedad, así como la industria tecnológica, de contar con reglas claras y eficientes que faciliten la investigación de las autoridades y les permita llegar a conclusiones concretas con respecto a los hechos en los que las máquinas con autonomía de actuación están involucradas.
- Sin evidencias irrefutables de que las fallas en la tecnología se deben a errores de programación o defectos del fabricante, no será posible deslindar al usuario final de ninguna responsabilidad, pues al adquirir el bien se adquiere también la responsabilidad de su uso.
- La creación de un marco normativo no necesariamente frena ni restringe las posibilidades de desarrollo de los sistemas autónomos, por el contrario, su implementación permitiría eliminar algunos prejuicios que la sociedad todavía tiene contra el uso de máquinas autónomas. Se debe concebir la implementación de regulación en ese ámbito como una necesidad, no para limitar la innovación, sino para establecer condiciones que transparenten los criterios de toma de decisión.
- El CONACYT debe hacer ciencia y vincularse con las empresas, asimismo debe impulsar la creación de oferta académica para que haya competencia y ésta se aproveche por la industria mexicana.

IDENTIDAD Y GOBERNANZA

IDENTIDAD Y GOBERNANZA

Panelistas

- Moderador: Marilú López - DAMA Capítulo México.
- Baltazar Rodríguez - IBM.
- Carlos Valderrama - Legal Paradox.
- Marco Antonio Ruiz Aguirre - Presidente del Consejo del Colegio de Notarios de la Ciudad de México.
- Relatora: Teresa Ganado - Thomson Reuters.

Ejes Temáticos

- La identidad en el ámbito digital y los aspectos que deben considerarse para gestionar las identidades digitales.
- Cómo las tecnologías emergentes facilitan la descentralización de sistemas de identidad, así como en los distintos modelos de identidad digital dentro del contexto legal.
- Cómo los especialistas en tecnología deben considerar estos modelos de identidad en las soluciones tecnológicas, considerando las facilidades que las nuevas tecnologías brindan.

El panel “Identidad y Gobernanza” fue moderado por Marilú López, presidenta de Data Management Association (DAMA Capítulo México), quien presentó a los panelistas y dio la bienvenida a los participantes.

En su participación, la moderadora destacó la importancia de difundir y mejorar las prácticas en la gestión de datos. En ese sentido, comentó que si bien estamos familiarizados con los “Avisos de Privacidad”, detrás de éstos debe existir una “cimentación” con la que debe contar cualquier organización, para que realmente se puedan respaldar y resguardar los datos y, en términos de seguridad, se pueda garantizar el adecuado tratamiento de la información.

Asimismo, Marilú López al destacar la importancia de ese evento, enfatizó que el ejercicio de ese panel era explorar los temas que de forma simultánea se discuten en 24 ciudades de 20 países, para que al final se puedan concentrar las conclusiones

a las que se lleguen y se pueda realizar un análisis a nivel global, dijo.

Partiendo de este punto, dio inicio a la sesión, centrada en el tema de la identidad y la gobernanza. Para ello, en primer término se realizó un diagnóstico de la materia, para identificar: (i) qué retos supone la protección de identidad ante los cambios de comportamiento y la tendencia de incremento en fraudes cibernéticos; (ii) si se cuenta con un marco normativo entendible, eficaz, aplicable, y (iii) qué tan adecuado es ese marco, conforme va avanzando la tecnología. Ello, a efecto de analizar los desafíos que representan y obtener propuestas para su mejora.

→ DIAGNÓSTICO

Retos que supone la protección de identidad ante los cambios de comportamiento y la tendencia de incremento en fraudes cibernéticos.
El ingeniero Baltazar Rodríguez, durante su participación, destacó que el uso de las Tecnologías de la Información y Comunicación (TIC) están presentes en casi todos los procesos. Por ello, enfatizó que éstas han permitido desarrollar nuevos modelos de interacción para expresar nuestra voluntad en medios digitales, creando –por así decirlo– un "símil digital" de nosotros mismos. Si bien esto ha permitido la optimización de recursos, también supone desafíos importantes en cuanto a la seguridad de la información y la protección de ese aspecto íntimo de quiénes somos.

Asimismo, señaló el panelista que hoy en día se habla de que los datos son el nuevo "recurso natural", y es que las plataformas digitales tienen a su alcance los incentivos para deducir comportamientos, asociaciones, afinidades, preferencias, dando a nuestra identidad un valor económico, el cual es factible comercializar y explotar.

De igual manera –indicó Rodríguez– en México uno de los mayores retos es que estamos ante un "vacío jurídico", sobre todo porque tenemos normatividad que habla acerca de la identidad, de la protección de datos y, sin embargo, no hay normatividad en el tema de suplantación de identidad en medios digitales. Y es que existen temas similares en el mundo físico, como falsificación de documentos, pero se está ante un vacío normativo frente a ese ejercicio digital, aseveró.

Esto es, se ve el robo de identidad como un acto criminal, no obstante, de que existe también una utilización comercial y jurídicamente válida de esos datos de identidad, que las personas por su propia voluntad entregan a cambio de una aplicación (APP) o de algún mecanismo digital, y que no necesariamente cae en robo de identidad, pero sin embargo resulta ser igual o más peligroso debido al uso poco ético que se le da a esa información.

Por su parte, el notario Marco Antonio Ruiz Aguirre señaló que el derecho a la identidad de las personas físicas o naturales está íntimamente ligado a la

obligación que tiene cualquier Estado de otorgar certeza y seguridad jurídica a su población.

Destacó que, al hablar de identidad por medios electrónicos, se ve involucrada necesariamente la participación del gobierno, y la manera en la cual la persona se identifica frente al Estado, pues a partir de la certeza de esa identificación es como migra esa identidad en el mundo digital. Enfatizó durante su ponencia, el hecho de que no se puede hablar de una prevención de suplantación de identidad digital, si no existe una certeza de inicio en la identidad de las personas.

Es así que, por ejemplo, para obtener los medios de identificación expedidos por el gobierno (credencial del INE o pasaporte) éstos se pueden solicitar mediante la presentación de documentos apócrifos, por lo que se tiene un documento de identidad válido, pero que está viciado desde su origen.

Por tanto, señaló Ruiz Aguirre, una de las problemáticas que gira en torno a este tema se da desde el marco normativo en cuanto a su aplicación. En primer término, el artículo 4 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) establece el derecho a la identidad como un Derecho Humano. Por su parte, la Ley General de Población (LGP) establece la creación de una Cédula de Identidad Ciudadana, sin embargo, no existe un documento de identidad para efectos de acreditar la ciudadanía, por lo que hay un vacío en cuanto a la obligación estatal de emitir esa cédula de identidad.

En este sentido, la facilidad con la que se consiguen documentos apócrifos para obtener medios de identificación legal, aunado a que no existe la certeza jurídica de que el documento de identidad expedido por las autoridades sea plenamente seguro y que representa la persona que se ostenta, acrecienta los retos para tratar a la suplantación de identidad. Bajo esta perspectiva, aseveró Ruiz Aguirre, la suplantación de identidad también implica un problema cultural, en el sentido de que se debe concientizar a las personas respecto al cuidado de sus datos e información, pues los primeros en cuidar los datos de nuestra identidad debemos ser nosotros mismos.

Por su parte, el abogado de Legal Paradox, Carlos Valderrama, indicó que los avances que se han dado en cuanto a la posibilidad de almacenar datos de una manera barata, y esa facultad de procesarlos para tener información específica y usarla de acuerdo con el tipo de modelo de negocio que se adopte, redunda en temas éticos, en los cuales la ponderación del bien jurídico tutelado no se tiene claro, debido a que no existe un marco regulatorio propicio para esos esquemas.

Asimismo, Valderrama mencionó que desde la perspectiva de las Tecnologías de Institución Financiera (Fintech), sí existen disposiciones relativas a la suplantación de identidad, tanto de las propias instituciones autorizadas para operar estos marcos innovadores, como desde

la perspectiva del usuario, por lo que, si se proporciona información falsa a esas Instituciones, es considerado un delito, y como tal, punible, aseveró.

Destacó el expositor que en términos de regulación, si bien es cierto que las entidades Fintech tienen un marco normativo importante en materia de protección de datos personales en posesión de particulares, es decir, sí cuentan con estas herramientas normativas, debe analizarse el campo de su aplicación.

Asimismo, dijo que para efectos de la Ley Fintech, ese tipo de datos es catalogado como "información sensible", debido a que no sólo se trata del conjunto de datos personales, sino de datos financieros y patrimoniales, por lo que la ley obliga a las entidades a clasificarla como información crítica, y con base en eso, desarrollar un marco de temas de ciber security para su protección. Es por ello por lo que esos terceros que manejen y tienen acceso a ese tipo de información –por ejemplo, alguien que procesa la contabilidad–, tendrá que pasar por el registro y validación previa de la Comisión Nacional Bancaria y de Valores, en donde es necesario que esos proveedores manifiesten en dónde se encuentran ubicados sus servidores; su principal lugar de negocios; entre otros aspectos, dijo el abogado.

En otro tema, el ponente señaló que para que una identidad sea suplantada, primero se debe tenerla, es decir, analizar cuáles fueron las fuentes que dieron origen a ella. Y es donde radica el gran problema: por un lado, se han desarrollado motores de inteligencia artificial los cuales permiten la creación de imágenes de personas inexistentes, de las cuales se puede crear todo un perfil para realizar transacciones electrónicas y, por otro, existe la desconfianza ante nuestras propias autoridades, que no expiden un documento de identidad con base en un proceso estandarizado, sino que existen varios medios de identificaciones emitidos por diversas autoridades, lo cual provoca que los procesos sean complejos y difíciles de unificar, y finalmente, no se tiene la certeza jurídica de que la personas es quien dice ser, concluyó.

→ ANÁLISIS

Cambios que se han dado en la legislación para favorecer la protección de la identidad.

Al abordar este tema, Marilú López recapitula un poco y señala que si bien se tiene desde el marco legal a la Ley General de Población, la Ley General de Protección de Datos Personales en Posesión de Particulares, la Ley Fintech, la Ley de Notarios para la Ciudad de México, entonces qué otros avances –desde el marco normativo– se podrían hacer para ayudar a proteger la identidad.
Al respecto, Baltazar Rodríguez señaló que existen aproximaciones parciales normativas para la protección de la identidad, como es la aparición de la Firma Electrónica Avanzada, así como otras normativas en materia de salud,

por ejemplo, la creación de un certificado electrónico de nacimiento. Éstos podrían señalarse como los primeros puntos dentro de una generación de regulación en el ejercicio de la identidad, sin embargo, afirma, existe ese marco regulatorio, pero no el ámbito de su aplicación; es decir, no existe un ejercicio continuo, debido a que existen limitantes para su implementación.

Asimismo, destacó Rodríguez, existen iniciativas regulatorias y tecnológicas, las cuales buscan proteger la identidad, como por ejemplo normatividades como el GDRP en Europa e iniciativas tecnológicas como SOVRIN, las cuales tienen como objetivo evitar una comercialización y explotación indiscriminada de la identidad.

Por su parte, Marco Antonio Ruiz Aguirre señaló que en el caso del Registro Nacional de Población o Renapo, se prevé la creación de una medida de verificación de la identidad conformada por todas las bases que lo identifican (Secretaría de Salud, Seguro Social), así como una base de datos compartida, pues con la implementación de la CURP, se cuenta ya con esa base, a efecto de que se pueda verificar la identidad de las personas, en tanto que este problema de identidad puede ser considerado como un tema de seguridad nacional. Finalmente, Carlos Valderrama añadió que, para efectos de la Ley Fintech, existe lo referente al openfinance, aplicable a los clientes de servicios financieros, en el cual se contempla que mediante el uso de aplicaciones se puedan acceder a distintos datos, siempre que se esté autorizado. Por ello se espera para marzo de 2020, el desarrollar un cuerpo normativo que prevea el uso de esas plataformas, y tener certeza jurídica de que los datos se utilicen conforme el usuario haya dado su consentimiento.

Aplicación de las normas de protección de identidad ¿qué tan accesibles y efectivas son? En este tema, la presidenta de DAMA Capítulo México, Marilú López, pidió a los asistentes que compartieran su perspectiva con respecto al marco legislativo de las normas de protección de identidad. En ese sentido, los asistentes abordaron lo tocante a la dificultad que representa la validación e identificación de la información de las personas morales, derivado de la poca transparencia que existe en el Registro Públicos de Comercio. Por ello, se les cuestionó a los panelistas cómo debe manejarse esa línea delgada entre la protección de datos y el acceso a la información, que es pública.

Por otra parte, el notario Marco Antonio Ruiz Aguirre, consideró que el problema debe ser atacado desde su origen, debido a que el tema de la suplantación de identidad va de la mano con la presentación de documentos apócrifos.

Además, urgió a utilizar la tecnología al señalar que es necesaria la interacción con las entidades gubernamentales y empresas, para implementar y hacer uso de la tecnología; para adaptar herramientas las cuales permitan automatizar los procesos y dar una mayor certeza y simplificación en el trabajo diario.
Finalmente mencionó la necesidad de incorporar elementos biométricos a la firma electrónica no solamente en el

momento de su obrención sino también al momento de su uso para evitar la suplantación que se realiza cuando se comparte con una persona diferente.

También, entre lo que se comentó se dijo que existe una falta de procesamiento de la información por parte de las autoridades, pues para que ésta sea funcional, debe haber una labor de concentración.

Asimismo, los asistentes consideraron que existe la normatividad en la materia, sin embargo, falta vincular y trabajar para que se dé su cumplimiento, en este caso con los organismos garantes, como lo es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el que debe vigilar que así sea; por tanto, se debe hacer valer y cumplir la ley que se tiene para mitigar esos riesgos, se aseveró.

→ PROPUESTAS

- Impulsar la incorporación de elementos biométricos al momento del uso de la Firma Electrónica Avanzada.
- Creación de un documento o sistema de verificación de identidad único a nivel nacional.
- Apalancar los distintos documentos que hoy ya existen y que se pueden utilizar para validar la identidad a través de un esquema colegiado, basado en tecnologías como la de blockchain y la de identidad autosoberana, solicitando los cambios normativos que validen este esquema.
- Crear campañas de concientización a la ciudadanía en general, para alertar sobre el impacto de otorgar nuestros datos, conscientes en que somos los primeros responsables de proteger nuestra identidad.
- Buscar agilizar la normatividad sobre la validación de identidad basada en principios más que en reglas, como complemento al cumplimiento de las leyes ya existentes
- Promover educación y cultura en las personas para proteger sus propios datos personales y datos de identificación.
- Promover mecanismos de vinculación, normatividad compatible y armónica con lo definido por organismos globales o regionales.
- Promover que haya controles y consecuencias por la no aplicación de las Políticas públicas a nivel población, para impactar en el esquema obligatorio de protección de datos y ejercerlo efectivamente.
- Fortalecer la Cultura de prevención. Quien utilice los medios electrónicos de contratación, deberá conocer la importancia, alcances y consecuencias de esos actos, así como la certeza sobre la identidad y verificación de la autonomía de la voluntad de la persona a la que se le contrata.
- Difundir ampliamente el mensaje de que el uso tecnológico debe estar basado en principios éticos, los cuales protejan ese valor íntimo que es la identidad de cualquier forma de abuso, y derivado de esos principios, generar un marco regulatorio adecuado.