UNIÓN COLEGIADA DEL NOTARIADO COLOMBIANO "U.C.N.C."

MEMORANDO No. 3024 Bogotá D.C., 12 de abril de 2021

Tema : Artículos periodísticos sobre identidad digital, ciberseguridad, inteligencia artificial y biometría.

De : Prensa "U.C.N.C.".

Para : Notarios del País.

Respetados Señores Notarios:

Para su conocimiento, remitimos los siguientes artículos periodísticos de interés, publicados en el Diario El Tiempo, La República, Asuntos Legales y Revista Semana.

'La identidad digital debe tener altos niveles de seguridad'.
https://www.eltiempo.com/tecnosfera/novedades-tecnologia/entrevista-con-santiago-aldana-director-ejecutivo-de-la-plataforma-soy-yo-580178

Fraude, una amenaza para la ciberseguridad.
https://www.larepublica.co/internet-economy/fraude-una-amenaza-para-la-ciberseguridad-3151358

En el control de la inteligencia artificial nos jugamos el futuro.
https://theconversation.com/en-el-control-de-la-inteligencia-artificial-nos-jugamos-el-futuro-157019

Cordialmente,

VIVIANA ORTIZ CUENCA
Jefe de Prensa

Adjunto: Lo anunciado.
Elaboró: VOC

Tecnología

AMAZON, SIN SINDICATO

La idea de crear el primer sindicato de Amazon en EE. UU. fracasó, pues el recuento de votos mostró que una amplia mayoría de trabajadores de una planta de Alabama dijo no a la propuesta.

'Se debe buscar que la identidad digital tenga altos niveles de seguridad'

Santiago Aldana, director ejecutivo de Soy Yo, explica la importancia de proteger los datos y cómo se pueden reducir casos de suplantación de identidad en los trámites.

TECNÓSFERA | @TECNÓSFERA

Realizar trámites de manera virtual se volvió una práctica cada vez más usada, sobre todo en el último año, por el confinamiento a raíz de la pandemia de covid-19, que impulsó fuertemente el uso de canales digitales. En esto juega un papel muy relevante la protección de los datos personales que permiten establecer una identidad de manera digital.

Así lo señala Santiago Aldana, director ejecutivo de la plataforma Soy Yo, la cual ofrece la alternativa de que las personas a través de su celular puedan tener el control de la información que les permita ante una entidad o empresa comprobar quién son, contando con herramientas tecnológicas de punta, como reconocimiento biométrico, para la protección de los datos. Haciendo que los procesos sean sencillos y que cuenten con mecanismos de cifrado.

¿Qué es la identidad digital?

En la identidad digital hay varios factores. El primero responde a la pregunta de quién es la persona; la segunda es la autenticación, que esa persona pueda demostrar que es quien dice ser, esto se logra en el factor digital con biometría, ya sea facial, de voz o de iris, o con otros elementos más tradicionales como códigos por mensajes de texto o un *token*. Estos elementos permiten saber quién es la persona y se guardan desde el teléfono de forma segura.

La identidad digital contempla elementos muy fuertes de privacidad. Está volcada a que todo esto sea protegido y controlado por el individuo, que este sea el dueño de su identidad digital y cuente con herramientas tecnológicas disponibles para tal fin.

¿Por qué es importante ponerle atención a la identidad digital?

Con la identidad digital, uno puede guardar en un solo lugar la información que le permite a uno demostrar quién es. Actualmente, para diferentes trámites, uno tiene que identificarse y hacer el proceso con entidades distintas; termina uno con un montón de claves, al punto de que se volvió inmanejable. A ello se suman los riesgos de si esta información, por algún tipo de filtración o ataque, es robada y alguien puede violentar esa identidad al acceder a esos datos.

> **"Al relacionarnos con una empresa** o entidad, nos ponen a los individuos la carga de demostrar la identidad".
>
> **Santiago Aldana**
> DIRECTOR DE SOY YO

Por esto se debe buscar que la identidad digital tenga altos niveles de seguridad y privacidad, permitiendo interactuar con las empresas o entidades con las que se necesita hacer un proceso, pero de una forma al mismo tiempo fácil y rápida.

¿En qué consiste la plataforma Soy Yo y cómo se pueden hacer trámites?

Típicamente, cuando queremos relacionarnos con una empresa o entidad, ya sea para abrir un nuevo servicio o para ampliarlos, nos ponen a los individuos la carga de demostrar la identidad, tiene uno que anexar documentos, responder preguntas, hacer unos procesos largos, y eso se repite en cada uno de los lugares donde se necesita certificar la identidad.

Por eso, desde Soy Yo creemos que la carga de la prueba no debería ser sobre el individuo, debería ser fácil, rápido y con toda la seguridad y privacidad. Pero, además debería ser reutilizable, para todas las veces en las que tenga que comprobar quién soy. Lo que plantea la aplicación es que cada persona registre su identidad una sola vez y que cada vez que necesite comprobarla se vincula la plataforma con la entidad, para que el proceso sea sencillo y sin tantos pasos, pero al mismo tiempo seguro, ya que la aplicación guarda la identidad en el teléfono, a través de una llave única y no por una base de datos central manejada por la plataforma.

Cuando quiero hacer un trámite con cualquier entidad, sea para vincularme, para firmar electrónicamente, entre otros, la persona simplemente debe tomarse una selfi y ahí se realiza la certificación de la identidad.

¿Cómo nació la plataforma?

Este es un tema que en todo el mundo está surgiendo, es tecnología de punta y ha aparecido porque en el mundo digital nos falta confianza para poder hacer trámites de manera digital. Por esto, Bancolombia, Banco de Bogotá y Davivienda vieron la importancia de la identidad digital no solo en el sector financiero, sino en otros campos como el *retail*, el sector de las telecomunicaciones y de la salud. De ahí, en diciembre de 2019 se crea Soy Yo, que incorpora la mejor tecnología disponible globalmente, para que las personas puedan construir esa identidad digital, y en este momento estamos en la fase de escalarla y trabajar en los convenios con varias entidades para que cuenten con este servicio y se lo puedan ofrecer a sus usuarios.

¿Qué elementos integra la aplicación para garantizar la seguridad de los usuarios?

Lo que hacemos en Soy Yo es que nosotros no tenemos la información que permite realizar la identidad digital, cada persona es la que lo tiene y protege con elementos como factores de biometría; además, si a la persona se le pierde el celular, una persona externa no va a poder acceder a estos datos, y solo cuando la persona tenga un nuevo teléfono podrá restablecer su información. Acá lo que estamos haciendo es que cada usuario tenga una base de datos individual, la cual está cifrada.

¿La aplicación permite reducir los casos de fraude y suplantación de identidad?

Durante la pandemia hemos visto crecer de manera exponencial los casos de fraude y suplantación en las transacciones digitales, y de ahí es de donde sale con mayor relevancia todo el tema de Soy Yo; lo que buscamos es dar mecanismos que ayuden a mitigar todos estos delitos, dándoles al tiempo a las personas el control de sus datos, pero haciéndolo sencillo. Las personas tienen la identidad en su teléfono, pero protegida con los niveles más altos de seguridad tecnológica actual.

Santiago Aldana, director ejecutivo de Soy Yo, habla de la importancia de contar con mecanismos de seguridad para proteger la identidad digital. CORTESÍA SOY YO

LR LA REPÚBLICA

INTERNET ECONOMY

FIN DE SEMANA 10 - 11 DE ABRIL DE 2021

P11

TECNOLOGÍA

Fraude, una amenaza para la ciberseguridad

LOS DELINCUENTES SE APROVECHAN DE LOS FACTORES QUE GENERA EL PANORAMA ACTUAL, COMO EL MIEDO Y LA CONFUSIÓN PARA INCREMENTAR SUS ATAQUES, YA SEA HACIENDO USO DE 'MALWARE' O 'PHISHING'

DAVID LÓPEZ
Vp. de ventas para Latinoamérica de Appgate

La pandemia intensificó la dependencia de las personas por la tecnología y la forma cómo interactúan con las diferentes plataformas digitales. Sin embargo, esta realidad también potenció los ataques cibernéticos en las organizaciones.

El *Ministerio del Trabajo* informó que, en Colombia, la adopción del teletrabajo aumentó 80% durante la pandemia para finales de 2020. Según el organismo, más de tres millones de personas acogieron esta modalidad para realizar sus actividades laborales. Este es un crecimiento exponencial, más si tenemos en cuenta que, dos años atrás, esta cifra no llegaba a los 122.000 puestos.

Con la llegada de la virtualidad, las organizaciones expusieron de forma dramática la información. En el primer trimestre de 2020, los ciberdelitos aumentaron un 37% comparado con 2019. Diariamente, 240 millones de mensajes basura relacionados con el covid-19 y 18 millones de 'malware' y correos electrónicos de 'phishing' son enviados desde cuentas de gmail.

Ciberataques y sus enormes consecuencias

Ante esta realidad, los delincuentes se aprovechan de factores como el miedo y la confusión que genera el panorama actual para incrementar sus ataques. En nuestro informe 'Fraud Beat 2021: Adaptándose a los nuevos retos del fraude', identificamos las siguientes conclusiones sobre la ciberseguridad durante la pandemia.

Los atacantes utilizaron información relacionada con vacunas, curas y tratamientos contra el virus, para confundir a las personas y efectuar sus ataques. La *Organización Mundial de la Salud* (*OMS*), denunció que una vez se declaró la pandemia, se crearon 22.000 dominios ficticios ofreciendo servicios relacionados con la enfermedad.

El 'phishing' se convirtió en un enemigo letal que utiliza el engaño para robar información confidencial. Su impacto representó más de 80% de los incidentes de seguridad llevados a cabo en 2020 y, además, produjo un aumento de 345% de las estafas a personas.

Los ataques de 'malware', por su parte, aprovecharon la coyuntura y se camuflaron en las redes sociales de sus víctimas. Se identificó que producto de este comportamiento, los cibercriminales encriptaron datos en 73% de los casos.

Ante la dependencia en el uso de las plataformas para realizar reuniones virtuales, las empresas sufrieron ataques que afectaron 500.000 credenciales. El año pasado, ocurrieron 3.950 casos de filtración de datos y casi 80% fue producto de credenciales robadas. Según informó *IBM*, el costo promedio de esta vulneración es de US$3,86 millones.

Los mecanismos tradicionales de verificación mostraron su gran debilidad. La combinación de nombre de usuario y contraseña es un método poco efectivo para protegerse. En cambio, un modelo que contemple las biometrías de comportamiento con el análisis contextual, como pueden ser token, push, huella dactilar, QR y reconocimiento facial, tienen un 91% más de precisión.

Ante la poca seguridad que las empresas alcanzan ofrecer a sus entornos remotos, los ataques de 'ramsonware' y sus consecuencias no dejan de aumentar, ya que aprovechan estas vulnerabilidades para comprometer los equipos. Las organizaciones deberán anticiparse a las amenazas emergentes y puntos débiles encontrados en los dispositivos y las redes. Solamente así, el acceso estará en un ambiente protegido, seguro y con poca fricción.

Los avances en inteligencia artificial (IA) y en biotecnología, exacerbados en la imaginación popular por el discurso transhumanista, han propiciado que la gobernanza de la tecnología se haya convertido en un problema ineludible en la agenda política. Quizás ya no suene melodramático decir que se trata de un asunto en el que nos jugamos el futuro.

Seguimos, sin embargo, con instituciones y sistemas regulatorios que, a lo sumo, son funcionales en relación con la tecnología de la tercera revolución industrial (revolución digital e informacional), pero que resultan obsoletos para regular las tecnologías de la cuarta (unión de tecnologías digitales, particularmente la IA y las redes de sistemas inteligentes, la robótica, el internet de las cosas, las tecnologías de nuevos materiales, la nanotecnología y las biotecnologías). Esta revolución, a juicio de importantes analistas, ha comenzado ya.

Como bien explica el filósofo Luciano Floridi en su libro *The fourth revolution*, el reto que tenemos ante nosotros no es tanto el que puedan presentar las innovaciones tecnológicas como tales, sino el que plantea la propia gobernanza de lo digital. Sin embargo, buena parte de la sociedad parece no tomarse demasiado en serio este problema. Algunos legisladores y expertos son conscientes de la magnitud del desafío, pero hay dudas razonables de que puedan ejercer una influencia decisiva en el plano legal e institucional con la premura que sería exigible.

¿De verdad existe una inteligencia artificial?

Hasta el presente, todos los logros en el campo de la inteligencia artificial han sido en el desarrollo de lo que se conoce como "inteligencia artificial particular", específica o estrecha. Es decir, en la creación de sistemas computacionales que despliegan una gran capacidad, superior incluso a la humana, para realizar tareas muy específicas y bien definidas. Por ejemplo, jugar a un juego con reglas fijas (ajedrez, go, damas, videojuegos), responder a preguntas de cultura general, realizar diagnósticos médicos precisos (enfermedades infecciosas, tipos de cáncer, medicina personalizada), reconocer caras y otras imágenes, procesar e interpretar la voz humana, traducir de un idioma a otro.

En realidad, una parte sustancial de lo que hoy llamamos *inteligencia artificial* son sistemas de minería de datos, llamados así porque son capaces de analizar cantidades masivas de datos

y obtener de ellos patrones desconocidos y lo que podríamos considerar como conocimiento nuevo sobre esos datos.

Por impresionantes que sean estos logros, estas tecnologías no alcanzan la versatilidad y flexibilidad de la inteligencia humana. Los sistemas más inteligentes de los que disponemos en la actualidad no pueden ser utilizados con eficacia en tareas diferentes a aquellas para las que fueron programados. Hay quienes piensan que ni siquiera los deberíamos llamar inteligentes, puesto que la única inteligencia que aparece en ellos es la del programador humano o la de los seres humanos en cuyo contexto social estos sistemas cumplen alguna función.

Se suele decir que una máquina es inteligente cuando es capaz de realizar tareas tales que asumimos que requieren de inteligencia para ser llevadas a cabo. Esta es una definición operativa, puesto que considera que la inteligencia artificial se caracteriza como inteligente por sus resultados. No obstante, la propia caracterización de la inteligencia es un viejo problema cuya discusión continúa. No es fácil dirimir la cuestión, por lo que no es extraño que tampoco haya acuerdo sobre cómo definir la propia inteligencia artificial.

Aceptemos, sin embargo, que en un sentido no meramente metafórico podemos hablar de inteligencia artificial. ¿Debemos entonces temer la creación de una Inteligencia Artificial General (IAG)? ¿Tendremos máquinas superinteligentes que tomarán el control de todo el planeta o seremos capaces de controlarlas nosotros? Son preguntas que se repiten a menudo cuando se menciona el futuro de la IA en los medios de comunicación y en los libros de divulgación, y creo que merecen ser tomadas en serio.

La inteligencia artificial ya es un desafío

No conviene olvidar que, con independencia de si el desarrollo futuro de una inteligencia superior a la humana pudiera representar un peligro para la supervivencia de nuestra especie, lo que por el momento constituye un desafío desde el punto de vista de la salvaguarda de los derechos de las personas son ciertas aplicaciones de la IA cuyos efectos se están viendo ya, como es el caso del uso de nuestros datos personales por parte de sistemas de IA pertenecientes a las grandes empresas tecnológicas, cuyo poder a su vez se acrecienta aceleradamente, o los sesgos y opacidad de los algoritmos usados en la toma de decisiones importantes para la vida de las personas, como la contratación de personal en las empresas o la concesión de créditos bancarios.

Mención aparte merecen los peligros del uso de la IA en la identificación de rostros y en la búsqueda de delincuentes y prevención del delito, en la vigilancia y represión de disidentes políticos, en la creación de armas autónomas, o en la proliferación de los ciberataques, de las noticias falsas y de la desestabilización política mediante la desinformación.

Digamos también, para no dejar una imagen completamente negativa, que la IA está siendo un instrumento muy eficaz en la persecución de delitos financieros, en la protección de la seguridad de las personas, en la potenciación del progreso biomédico, en el logro de una mayor eficiencia energética y en la protección el medio ambiente.

Creo que, para analizar las consecuencias posibles de la inteligencia artificial, tanto favorables como desfavorables, discutir si se trata de inteligencia genuina, similar a la humana, con posibilidad de ser consciente o no, es desviar el foco del auténtico problema.

TECNOLOGÍA

El Gran Hermano sanitario

Las libertades fundamentales corren grandes riesgos en un mundo que implementa sistemas biométricos para monitorear a los ciudadanos en nombre de la lucha contra la pandemia de covid-19.

EN UN FUTURO NO MUY LEjano, los ciudadanos usarán mascarillas que monitorean la respiración, lentes de contacto que miden la presión ocular, anillos que evalúan la tensión arterial o ropa que calcula la temperatura del cuerpo y analiza la transpiración. El examen de los datos extraídos por esos aparatos permitirá a las autoridades de salud identificar una enfermedad, quizás contagiosa, y aislar al individuo.

Ese es el sueño orwelliano de las empresas que intentan comercializar tecnología biométrica para controlar la pandemia y prevenir epidemias futuras. Las innovaciones incluyen cámaras de reconocimiento facial con inteligencia artificial y también los llamados tecnoaccesorios (*wearables*, en inglés), prendas o instalaciones en el cuerpo que permiten monitorear la actividad de este en tiempo real.

▲ **Aunque no se puede negar el éxito de las tecnologías para controlar la pandemia, los defensores de los derechos fundamentales advierten graves riesgos para la vida privada.**

Una parte de esa tecnología ya existe y se implementa en varios países para luchar contra la covid-19. En Rusia se ha utilizado el reconocimiento facial para controlar la cuarentena, mientras que en China se usa para identificar a quienes no utilizan la mascarilla. Para monitorear a los nacionales que regresan del extranjero, el Parlamento israelí acaba de aprobar el porte de brazaletes electrónicos. Y en Estados Unidos, estudiantes del equipo de fútbol americano de la Universidad de Tennessee utilizan detectores de proximidad física en sus hombreras para que los médicos identifiquen situaciones de riesgo sanitario.

La lucha contra la pandemia aceleró la aparición de esas invenciones controversiales. Después de los atentados del 11 de septiembre de 2001, las grandes potencias empezaron a invertir en el desarrollo de todo tipo de tecnologías para identificar riesgos contra la seguridad. Por ejemplo, durante los seis años (2014-2020) del programa científico europeo Horizon 2020, alrededor de 2.000 millones de euros fueron destinados, entre otros, a la inteligencia artificial, drones a distancia, realidad aumentada, reconocimiento facial, de voces, iris o venas.

Aunque no se puede negar el éxito de las tecnologías para controlar la crisis sanitaria, los defensores de los derechos fundamentales señalan los riesgos para la vida privada. "La vigilancia tiene el potencial para mitigar la pandemia, pero también para producir prácticas y estructuras antidemocráticas y discriminatorias a una escala global. Las tecnologías y datos se pueden utilizar con objetivos diferentes a los iniciales", alertó Veena Dubal, profesora de Derecho en la Universidad de California Hastings, en una columna del diario británico *The Guardian* publicada en abril de 2020, cuando varios países empezaron a utilizar la biometría en nombre de la lucha contra la covid.

Los regímenes autoritarios ya han comenzado a instaurar esa tecnología para otros propósitos, como en China, donde la biometría es utilizada para vigilar a la etnia musulmana uigur. Pero en los sistemas democráticos la situación también conlleva riesgos. Por ejemplo, la Unión Europea ha financiado el proyecto iBorderCtrl, un detector de mentiras basado en la lectura de microgestos faciales que podría ser utilizado en el control de fronteras. Los activistas temen que se estigmaticen individuos identificados como no blancos por el dispositivo.

Además, esas innovaciones se están lanzando sin un marco legal que indique el uso de la información recolectada. ¿Quién puede exactamente acceder a los datos? ¿Las empresas privadas o la policía pueden tener acceso a ellos? ¿Podrán ser vendidos para objetivos publicitarios? ¿Durante cuánto tiempo pueden ser conservados? Por ahora, esas preguntas son ignoradas.

Aunque el planeta entero desea dejar atrás lo más rápido posible la crisis sanitaria, olvidar que el derecho a la vida privada es un fundamento de las democracias podría hacer que el mundo salga de la pesadilla de la covid-19 para entrar a la pesadilla de un sistema de vigilancia en el que hasta el corazón de las personas es controlado en cada latido. ■