EDI

Revista Digital -Agosto 2021

en memoria de
Alvaro Andrade Sejas

ElDerechoInformatico.com

El presente será Tech

Edición n° 38 - Distribución gratuita

librería | hammurabi

Talcahuano 440 - C1013AAI
CABA - Argentina
Tel.: (54-11) 4371-8179
info@libreriahammurabi.com.ar

en preparación

Colección «elderechoinformático.com»

11 volúmenes

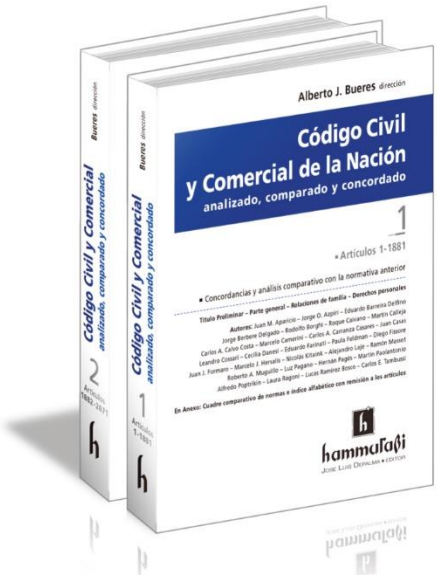
Guillermo M. Zamora dirección

1 — La prueba informática
2 — Negocios jurídicos en tiempos de Internet
3 — Delitos informáticos
4 — Propiedad intelectual en la era de la información
5 — Gobierno digital y gobierno abierto
6 — Datos personales, su protección
7 — ODR, Resolución de Disputas Online
8 — Firma digital
9 — Régimen jurídico de nombres de dominio
10 — Teletrabajo
11 — Aspectos jurídicos del *cloud computing*

Novedad

Código Civil y Comercial de la Nación

analizado, comparado y concordado



Alberto J. Bueres dirección

2 tomos | Artículos 1 - 2671

Análisis complementario de las principales normas que inciden en el «Derecho del trabajo» al cuidado de Juan J. Formaro

Contiene: Cuadro comparativo de normas. Indice alfabético de voces

• **Tomo 1. Arts. 1 a 1429.** **Autores:** Juan M. Aparicio – Jorge O. Azpiri – Eduardo Barreira Delfino – Jorge Berbere Delgado – Rodolfo Borghi – Martín Calleja – Marcelo Camerini – Carlos A. Carranza Casares – Rubén Compagnucci de Caso – Leandro Cossari – Cecilia Danesi – Paula Feldman – Diego Fissore – Juan J. Formaro – Marcelo J. Hersalis – Germán Hiralde Vega – Nicolás Kitainik – Alejandro Laje – Sabrina Luini – Ramón Massot – Luz Pagano – Hernán Pagés – Alfredo Popritkin – Laura Ragoni – Lucas Ramírez Bosco – Carlos E. Tambussi.

• **Tomo 2. Arts. 1430 a 2671.** **Autores:** Liliana Abreut de Begher – Beatriz Areán – Jorge O. Azpiri – Eduardo Barreira Delfino María I. Benavente – Gabriela Boquin – Roque Caivano – Carlos Calvo Costa – Marcelo Camerini – Juan Casas – Federico Causse Rubén Compagnucci de Caso – Leandro Cossari – Nelson Cossari – José Fajre – Eduardo N. Farinati – Juan J. Formaro – Andrés Fraga – Alberto Gabás Lidia Garrido Cordobera – Marcelo J. Hersalis – Gabriela Iturbide – Jorge Juliá – Alejandro Laje – Ricardo Nissen – Martín Paolantonio Christian R. Pettis – Lucas Ramírez Bosco – Javier Rosembrock Lambois – Luciana Scotti – Gabriel Ventura – Luis M. Vives.

EDICIÓN N° 38
AGOSTO 2021

ÍNDICE

SOMOS EDI LA RED

EL CENTRO DE INFORMACIÓN

y contenidos
más grande iberoamerica

TWITTER: ELDERECHOINF

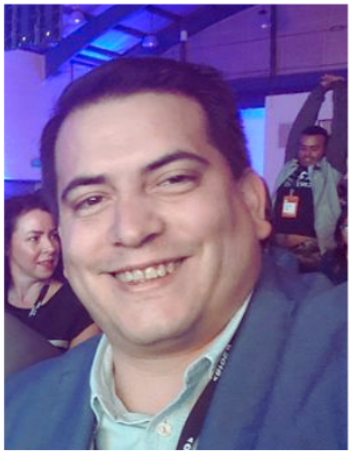
EDITORIAL

Hace unos días falleció un amigo, no voy a decir que se fue, solo se alejó un tiempo, una persona generosa con los demás, leal a sus amores, honesto, divertido, resumiendo un gran tipo, la noticia nos llegó por sorpresa, como todo lo inmerecido y acá estamos los que tuvimos la suerte de conocerlo, intentando procesar la pena.

Quisiera poder expresar mejor la tristeza que tengo y que nos llena el alma a los integrantes de La Red EDI, pero como siempre, las palabras faltan cuando más las necesitamos.

Hace unos días falleció **Alvaro Andrade Sejas,** un amigo, no hace falta decir que siempre va a estar cerca de nuestros corazones, en el de su amada familia y el de su querida Bolivia.

Buen viaje Alvaro, te vamos a extrañar (bah, ya lo estamos haciendo)



#MIS DATOS SOY YO

Está en tus manos aceptar o rechazar ceder el uso de tus datos

Tu privacidad hace tu libertad

EDI

ElDerechoInformatico.com

EDI

LA RED QUE VA MÁS ALLÁ DE
LO QUE PODÉS VER

SONRÍA, LO ESTAMOS FILMANDO

Camaras de seguridad y datos personales, una relación tirante

María José Quintana

[1]

Hace unos cuantos años atrás empezamos a ver carteles dentro de los negocios que, con cierto humor nos indicaban: “Sonría lo estamos filmando”, como una advertencia en son de broma. En la actualidad, es tan común que una gran parte de la sociedad tiene cámaras en su propia casa, a la que incluso monitorean en tiempo real a través de una aplicación en el celular.

Sin dudas el uso de estos dispositivos, otorga cierta seguridad y sensación del control. Lo que resulta paradójico, porque vivimos en una sociedad cada vez más incierta y cambiante, con pandemia, cambio climático e inseguridad debido al incremento de los delitos contra la propiedad.

En ese contexto de desazón, las cámaras parecen venir a traer un poco de seguridad o sensación de control, de ubicuidad, de poder estar

[1] **Por María José Quintana Dourado**, Abogada, Argentina.

en dos lugares a la vez y saber qué está pasando.

Podríamos decir que somos un poco nuestro propio Big Brother. Incluso se venden objetos que simulan ser cámaras pero que no filman nada, y sólo sirven como elemento disuasivo, tanto para prevenir los hurtos en comercios como para ahuyentar amigos de lo ajeno de los domicilios particulares.

Paralelamente, el propio Estado ha ido instalando estos dispositivos en la vía pública, que abastecen de imágenes los centros de monitoreo, pudiendo hacerse prevención y respuesta rápida frente al delito, u otras cuestiones que hacen a la seguridad pública, como incendios, accidentes, etc. Con ojos que todo lo miran 24/7 parece que algunas ciudades le han encontrado la vuelta al asunto echando mano a esta tecnología.

Países del extranjero como el Reino Unido llevan la delantera con una cámara cada trece habitantes. A lo cual se suman Inteligencia Artificial y big data para procesar datos y cruzar información, lo cual permite – por ejemplo- identificar personas que tienen pedido de captura, a través de sus datos biométricos (en este caso el rostro).

Todo el combustible del que se abastece el sistema de cámaras de seguridad, sean públicas o privadas, son las imágenes de cientos de miles de personas, lo cual no es otra cosa que sus datos personales. La imagen de alguien es un dato personal y está protegido por el plexo normativo como tal, para evitar que injerencias arbitrarias puedan afectar otros derechos como la intimidad.

Qué ocurre entonces con esos datos que son recabados a través de las cámaras, almacenados en memorias SD o discos CVR? Qué derecho tiene el que es captado sobre esos datos suyos y qué deberes les caben a quienes los tratan o utilizan?

La Ley 25.326 de Protección de Datos Personales, define dato personal como la "*información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"* la imagen que de alguien capte una cámara es un dato informatizado y quien recolecte esas imágenes tiene ciertos deberes que cumplir.

En primer lugar, todo titular de una base de datos debe garantizar que la misma cuente con las medidas de **seguridad y confidencialidad** de modo que esos datos no puedan perderse, ni adulterarse, ni ser consultados por personas no autorizadas. Quedando prohibido el almacenamiento de datos en bases que no cumplan con estas condiciones.

Otro elemento muy importante aquí es el **consentimiento previo e informado** de los titulares de los datos. Cuando el Estado es el que capta imágenes, para que se cumpla con el requisito del consentimiento previo e informado, debe mediar una publicación en el Boletín Oficial que se reputa conocido por todos. En tanto, los particulares (personas físicas, empresas) que capten datos, deben contar con ese consentimiento haciendo saber al titular del dato que se lo filmará.

Cómo se logra eso? mediante el famoso **cartelito**, que según la regulación específica de la Dirección de Protección de Datos Personales, debe **identificar al responsable del tratamiento de los datos**; consignar de manera visible un domicilio, teléfono, sitio web y correo electrónico. Todo a fin de que el titular del dato eventualmente pueda **acceder a la información personal** que han tratado y solicitar de ser necesario una supresión. Lo que pasaría si en un comercio de ropa se detectara una cámara en la zona de cambiadores, lo que claramente vulneraría el derecho a la intimidad de los clientes, y resultaría desproporcionado para el fin perseguido.

Así también todos quienes capten imágenes deben contar con un **Manual o Política de tratamiento de datos**, que deberá especificar la finalidad con la cual se los colecta y trata. Punto que resulta fundamental al momento de existir una controversia.

Sin duda que existen una serie de zonas grises en esto, como lo son las cámaras de seguridad de los particulares que muchas veces captan imágenes de la vía pública, y si en tal caso pueden servir para abastecer a los centros de monitoreo estatales. Ya que muchas veces este material fílmico resulta de gran utilidad para la investigación de delitos ocurridos en la vía pública.

Algo similar ocurre en centros de salud y hospitales públicos donde el límite entre privacidad y seguridad de las personas es muy delgado. Hasta qué punto la **privacidad de un paciente** puede ser expuesta en nombre de la seguridad, siendo que los datos de salud, sexualidad y género se consideran sensibles y tienen una tuición especial. Pero, qué pasa en un hospital emplazado en un barrio de conflictos entre bandas o con altos ingresos por guardia de heridos de bala en enfrentamientos con la policía?

Lógicamente que el criterio de **proporcionalidad y pertinencia** deberá tenerse en cuenta a la hora de correr el límite, sobre todo porque no es lo mismo que una imagen sea requerida específicamente por el Ministerio Público Fiscal, o mediante orden judicial a un ciudadano, a que este se conecte 24/7 a una red mayor donde las fuerzas de seguridad públicas se abastezcan del material que sus cámaras privadas generan.

No todo es lo mismo, sobre todo porque están en juego derechos de igual jerarquía constitucional: seguridad pública; integridad física; libertad; privacidad e intimidad. Implementar planes de seguridad que incluyan video vigilancia sin duda redundará en grandes

beneficios para la comunidad, siempre y cuando se los implemente a la luz de los principios de proporcionalidad y pertinencia que respeten y garanticen la intimidad de las personas; con métodos técnicos adecuados que resguarden la seguridad y confidencialidad de esas imágenes, sin olvidar que son datos personales.

UTN
FACULTAD REGIONAL TUCUMÁN

DIPLOMATURA UNIVERSITARIA en DELITOS INFORMATICOS y FORENSIA DIGITAL

Modalidad: 100% virtual

Inicio: 20 de Septiembre de 2021

Destinado a:

Profesionales del derecho: Fiscales, Jueces, Abogados y empleados judiciales.
Profesionales de las carreras de informática y ciencias de la computación.
Peritos informáticos. Fuerzas de seguridad.
Estudiantes avanzados de derecho y de informática.

Encuentros: Lunes y miércoles de 19:00 a 21:30
Inversión: $ 28.000 ó 4 cuotas de $7.000
Info: **diplomdelitosyforensiadigital@frt.utn.edu.ar**

Cuerpo docente

Dr. Ab. Marcos Salt, Esp. Ab. Víctor Portillo, Ing. Sergio Appendino, Prof. Ing. Gustavo Presman, Ab. Guillermo Zamora, Mg.Ab. Julián Reale, Ab. Ana L.Castillo de Ayusa, Ab. Marcelo Temperini, AUS Maximiliano Macedo, Ing. Patricia Moyata, Lic. Cesar Agüero, Esp. Ing. Diana Solórzano, Mg.Ab. Alejandra Silva, Ab.Daniel Budeguer, Ing. Nieves Colqui, Ing. José Santillán.

Inscripción a partir del 01/09/2021

RAFAEL M. MARTINEZ

El Sandboxing

Imaginen a un niño en un parque caótico con varias personas en bicicleta, jugando pelota, perros corriendo. ¿Cómo podremos garantizar un espacio seguro para que el niño pueda jugar tranquilo, protegido de todos esos elementos que lo rodean?: Colocando al niño con sus juguetes en una caja de arena (sandbox). Bueno, hagamos eso ahora con los nuevos fenómenos sociales y veamos cómo se comportan con las reglas existentes y que se puede hacer para que las leyes puedan regularlas sin afectar los beneficios inmediatos y sin sufrir el detrimento del tiempo.

Este es el principio del sandboxing. Usado en el mundo de la informática para aislar un proceso en específico sin comprometer al sistema principal, el sandboxing es un modelo que comienza a aplicarse en el ámbito jurídico para analizar y estudiar nuevos comportamientos en un ambiente aislado pero con el beneficio de controlar por anticipado las consecuencias jurídicas que puedan surgir. Es un tubo de ensayo donde el derecho puede ejercer su dinamismo sin correr el riesgo de producir daños o injusticias

irreparables y al mismo tiempo garantizando como resultado una visión amplia de los problemas reales que requieren regulación especial.

Hay que destacar que estos ambientes controlados no son algo en si tan novedosos. Antiguamente se han ejercido pero con objetivos más técnicos y se les conoció como planes pilotos. Por ejemplo, cuando la banca privada inicio operaciones con cajeros electrónicos (Red Abra24 en el caso Venezuela), este servicio se limitó inicialmente a un número controlado de usuarios en un número de cajeros muy reducidos. Durante ese tiempo se estudió el comportamiento de los cajeros así como el de las tarjetas magnéticas, la red de comunicaciones y el comportamiento de los usuarios. Si bien la Superintendencia de Bancos aprobó el uso de estos dispositivos, en realidad dicha aprobación se basó en un mero informe técnico y no abarco las consecuencias jurídicas que con el tiempo fueron apareciendo junto a los evolucionados tipos criminales y que posteriormente modificaron los conceptos de seguridad y de responsabilidad que originalmente se habían previsto.

La Comisión Europea lo define como una herramienta para las empresas y los supervisores (entes reguladores) para descubrir cómo se realiza la regulación actual de alguna actividad y como puede ser interpretada y aplicada a las soluciones tecnológicas a través de su testeo. Básicamente, se crea un ambiente aislado donde se analiza la situación específica y se determina si la normativa vigente es suficiente para regular jurídicamente la acción, si los vacíos legales pueden ser ocupados mediante la equivalencia funcional de la norma o si por el contrario se requieren de reformas o creaciones legislativas.

Los beneficios inmediatos obviamente son el tiempo y el producto final. El proceso de modificación y creación de normas es sumamente lento y requiere de ciertas etapas y requisitos administrativos y no siempre garantizan que el resultado sea el más idóneo. Una nueva actividad o comportamiento no puede suspenderse en espera de una normativa legal que la regule y mucho menos debe modificar su

naturaleza ante los preceptos legales, es por ello que tanto el nacimiento de la actividad como el de la norma deben ir desarrollándose en conjunto. También se busca que el proveedor del servicio obtenga una garantía de no ser sancionado por los entes reguladores mientras que los usuarios intervinientes reciben una advertencia respecto a la actividad de alto riesgo.

Es criterio del autor considerar que es posible tener dos tipos de sandboxes: uno práctico y otro teórico. El practico seria el ambiente ideal para actividades no tangibles, las cuales se podrían ejecutar con sujetos de pruebas ordinarios. Es lo que comúnmente ha sucedido en aquellos casos donde se ha utilizado para nuevos servicios finTech. Sería un Sandbox a posteriori de la creación del objeto mientras que el teórico podría considerarse la opción a priori, es decir, el análisis teórico del funcionamiento y todas las consecuencias legales, incluyendo la regulación, que dicha tecnología podría generar. Sería un desarrollo normativo en conjunto al tecnológico, que al final obtendría como resultado una especie de anteproyecto que pudiera usarse para la fase práctica de la metodología.

Un ejemplo claro y vigente de una actividad que podría someterse a sandboxing es la aparición de los vehículos autónomos. La mayoría de las legislaciones de tránsito terrestre imponen requisitos tanto al vehículo como al conductor. Poseer licencia de conducir sería uno de los requisitos indispensables y su obtención requiere por lo general de una prueba previa que demuestre que el conductor conoce tanto el funcionamiento del vehículo así como las normas de tránsito necesarias no solo para su uso sino además para garantizar la seguridad pública. Ahora bien, frente a un vehículo autónomo, ¿se ha verificado que el vehículo, así como su software/firmware, cumpla con estos mismos requerimientos que se les exigen a las personas? Igualmente ocurre al analizar la responsabilidad solidaria en materia de accidentes de tránsito; la norma suele determinar como responsable a los conductores y a los propietarios de los vehículos, uno por ser quien ejecuta la acción que produce el daño y el otro por extensión de su derecho patrimonial, pero en el caso

de los vehículos autónomos, ¿si el conductor es una inteligencia artificial, está exenta de responsabilidad? Igualmente podríamos hablar de modificaciones mecánicas ilegales al vehículo, ¿aplicaría este principio a las modificaciones ilegales del software/firmware?

Como se puede apreciar en el ejemplo anterior, estamos en presencia de una actividad ya regulada pero que requiere, debido a un avance tecnológico, una revisión de su marco legal; lo que hace esto un poco más difícil es que dicha revisión debe realizarse sin obstaculizar su evolución. Es cierto que podrían aplicarse, mediante el uso de la equivalencia funcional (analogía), otros principios rectores, por ejemplo cual es el criterio en materia de autonomía en el área de la aviación civil (alcances legales del piloto automático) o en el caso de embarcaciones marítimas y sus sistemas automatizados de navegación, pero esto supondría un trabajo adicional en el orden jurídico que no debería ser necesario en lo que posiblemente sea una activad cotidiana en un par de años y que requerirá normas claras y establecidas para su funcionamiento.

Seria devastador para la sociedad pretender suspender el desarrollo de una tecnología en espera de un marco legal que la regulara y que podría correr el riesgo de poseer lagunas legales en su contenido, ya que al final el legislador únicamente puede presumir los escenarios en que la ley actuaria. Asimismo, no sería inspirador y mucho menos confiable, una sociedad que sancione a los desarrolladores de nuevas tecnologías al ir en contravención de las normas preexistentes; de ahí la importancia de poder crear estos sandboxes y así desarrollar en conjunto las tecnologías y su normativa.

Ahora bien, la regulación del sandboxing posee características muy específicas. La doctrina y legislaciones actuales coinciden en que:

- El objeto debe ser único y determinado.
- El tiempo de duración deben ser limitados.
  Los sujetos sometidos al sandboxing deben ser identificados y limitados.

- Debe contar con la supervisión del órgano legislador.
- El sandboxing modifica y flexibiliza la normativa vigente, por lo tanto es una actividad de Orden Público.
- Adicionalmente, consideramos que deben existir dos elementos adicionales, el académico que aporta soluciones de alto espectro a los problemas que surjan y el ético que evitara el uso del sistema para fines desleales o incluso criminales.

Al establecer un ambiente cerrado, donde hay un número limitado de usuarios que utilizaran los servicios durante un tiempo determinado, se permite el análisis de situaciones específicas y de todas sus variables jurídicas, generando así una data que establecerá el status real de la norma vigente y la eficacia de la misma. Igualmente, la metodología permite flexibilizar las normas vigentes, suspendiendo efectos y sanciones a los sujetos activos, todo con el objeto de crear un dinamismo que permita testear el entorno sin restricciones.

Han existido para la fecha varios casos de éxito en la implementación del sandboxing. El Reino Unido y el estado de Utah en Estados Unidos han implementado los sandboxes en materia de finTech así como en procesos donde se involucran criptomonedas. Igualmente, España creo un marco legal para implementar su uso en el área financiera.

Sin dudas y con miras al futuro, la metodología del sandboxing puede ser aplicado más allá del ámbito financiero, en especial al derecho informático, el cual aún debe lidiar con ciertos conflictos y problemas. La ley nunca debe forjar el comportamiento social, al contrario, es ese comportamiento, a través de la costumbre, el que sirve como fuente de la norma y en consecuencia esta debe reflejar esa realidad y así concluir con una ley eficaz que garantice el desenvolvimiento de la activad que regula y la seguridad jurídica y económica de los involucrados, es por ello que vemos al sandboxing como la metodología idónea para acelerar el dinamismo que los

nuevos tiempos exigen de las ciencias jurídicas.

Rafael Martinez es Abogado Venezolano residenciado en Estados Unidos con estudios en Derecho Internacional, Bancario e Informático. Miembro de la Red Iberoamericana de Derecho Informático y Director del Proyecto eVenezuela.

Tech Law Firm

tinktec.

Vanesa Scafati

INTELIGENCIA ARTIFICIAL Y TRABAJO

Hoy estamos viviendo la Cuarta Revolución Industrial, esto gracias a la implementación de la Inteligencia Artificial -IA- que vemos en muchas temáticas. En esta oportunidad nos vamos a enfocar en la Inteligencia Artificial y el Trabajo.

Desde que existe la tecnología existe la frase de que las máquinas vinieron a reemplazar al hombre. Les cuento que esa frase ya paso de moda, se viene diciendo eso hace varias décadas. Tampoco vamos a ser tan inocentes de pensar que nada nos puede reemplazar, pero si sabemos que eso sería para preocuparnos a largo plazo.

Allá lejos y hace tiempo, o tal vez no tanto tiempo en el S. XVIII comienza la 1ra. Revolución Industrial, comienza una revolución económica, tecnológica, científica y social. Surge la mecanización tanto en la industria como en la agricultura, se aplica la fuerza motriz, el sistema de fábricas entre otros.

Luego surge la 2da. Revolución Industrial en el S. XIX, los cambios en este período fueron más fuertes y acelerados. Acá tenemos una transformación en la vida cotidiana de las personas, tenemos el surgimiento o la

aceleración del crecimiento de la energía, del transporte y sobre todo de las Telecomunicaciones. Dato de color, en el tema Telecomunicaciones podemos ver la serie “Las chichas del cable” y ver cómo eran las Telecomunicaciones por esos años.

Llegamos a la 3ra Revolución Industrial, sin ir más lejos fue ayer, allá por el S. XX las cosas se mega aceleraron, surgen nuevas ideas, miles de inventos la tecnología de la información y la comunicación (TICs) están a la orden del día. Procesos, descubrimientos, científicos y siempre presente las nuevas tecnologías. Surge la automatización.

Y ahora sí, llegamos a la 4ta Revolución Industrial, a la tecnología más disruptiva -aquello que produce una ruptura brusca, donde se genera un cambio muy importante-. ¿Pero cuando surge o surgió la 4ta. Revolución Industrial? la respuesta más corta es HOY!, en el S. XXI, si quieren poner una fecha más exacta podemos decir el 2011. Acá encontramos la robótica, máquinas y algoritmos que son capaces no solamente de actuar como nosotros sino hasta de superarnos. No olvidemos que las maquinas tienen 2 cosas fundamentales que nosotros tenemos por así decirlo “limitado o escaso”, primero la capacidad de almacenamiento, nuestro cerebro no es comparable con una máquina no puede almacenar como una computadora y segundo, la capacidad que tiene la máquina para procesar la información claramente no es como nuestro cerebro, no nos es imposible procesar de la misma manera que lo haría una computadora.

Ahora vamos paso a paso… desde que existen las máquinas existe ese miedo a perder el trabajo, a que los humanos no vamos a encontrar empleo, de que nos vamos a quedar en la calle y si queremos ser más fatalistas, pensamos también que las máquinas van a dominar a los

humanos y vamos hacer sus esclavos.

Pero porque no pensar que las maquinas vienen a ayudarnos en nuestras labores diarias. Porque no pensar que las máquinas pueden facilitarnos nuestras tareas, hacer que las mismas sean más prácticas y fáciles.

No vamos hacer un análisis minucioso ni empezar a sacar porcentajes, pero la Organización Internacional del Trabajo (OIT) pronostica que al pasar los años el nivel de desempleo va a disminuir, si, contra todo pronóstico negativo, el desempleo descendería.

En el mundo hay 5 (cinco) países que son pioneros en robótica, es decir que tienen las tecnologías más avanzadas, ellos son: Alemania, China, Corea del Sur, Estados Unidos y Japón. Sin entrar en detalle de cada país, podemos decir que todos estos países pronostican que su tasa de desempleo de acá a corto plazo se va a mantener estable y hasta en algunos casos descendería. Si, leyeron bien, pronostican un pequeño descenso del desempleo en estos países. Es decir que no solo tienen las tecnologías más avanzadas, la robótica industrial más desarrollada, que además se estiman que el desempleo a corto plazo va a descender.

En líneas generales podemos decir que nuestro trabajo no está en riesgo en el corto y mediano plazo. Además, en estos últimos tiempos están surgiendo nuevos puestos laborales, empleos que antes no existían, por eso sostienen que la tasa de desempleo va a ir en descenso. Eso no quita por supuesto que hay personas que van a quedar fuera del sistema por así decirlo, esto lamentablemente paso en todas las eras o revoluciones industriales/tecnológicas, está en nosotros abrirnos a las nuevas posibilidades que se nos presenta. Lo que hay que hacer sin lugar a duda es fomentar que las personas, sobre todo los jóvenes, adquieran y desarrollen nuevas habilidades y

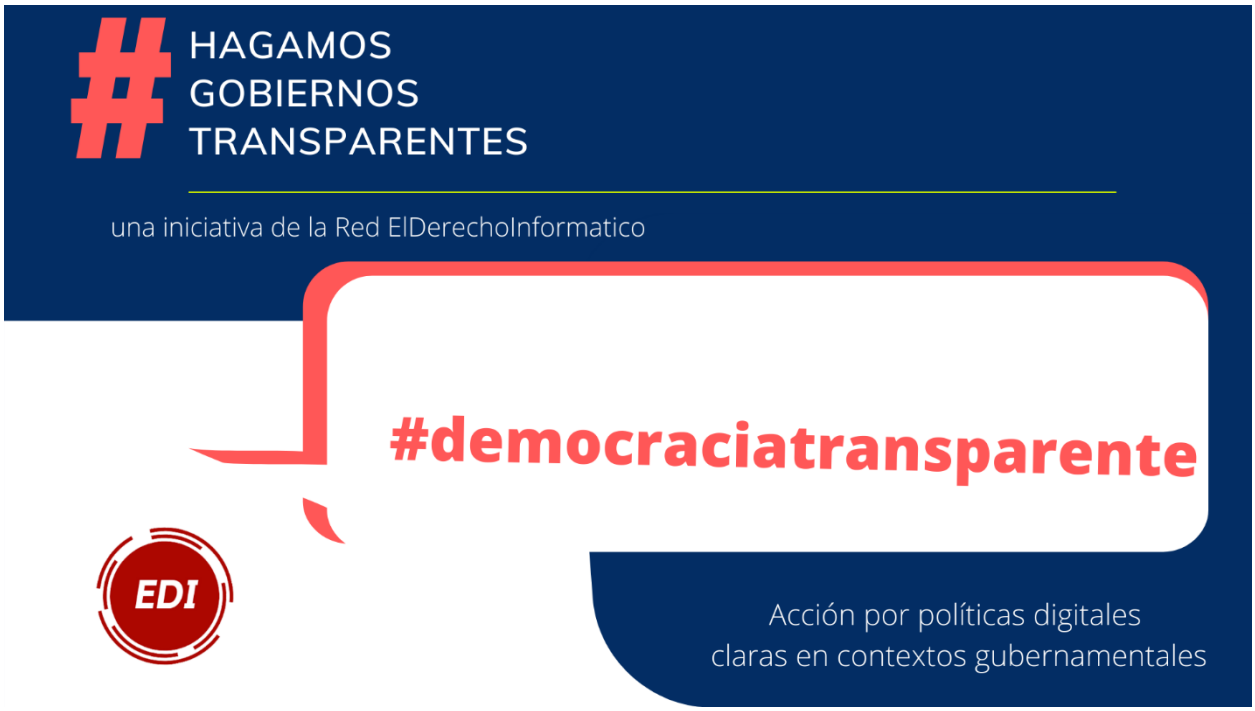
capacidades para poder ingresar a este nuevo mundo laboral.

Ya hoy en día muchas empresas sobre todo medianas y grandes están automatizando circuitos o procesos, sin ir más lejos tenemos a Amazon (Boston - Estados Unidos) donde existen calles por donde circulan los robots y van ordenando las cajas, levantando cosas del piso, realizando tareas tediosas y forzosas que hacían los humanos, hoy esas personas realizan tareas donde se requiere más ingenio y creatividad. En 2020 Amazon incorporó más de 400.000 empleados -si, en plena pandemia- y se estima que cuenta con 1,2 millones de empleados. Por supuesto mencionamos a una de las empresas más populares y tecnológicas que están a la vanguardia hoy. Entonces tenemos una de las empresas más tecnológicas del mundo con cada vez más empleados. ¿Para pensar no? Pero también podemos ver otros ejemplos, más acotados, pero que existen de empresas que comienzan a automatizar algunos de sus procesos. Tengamos en cuenta que automatizar no es IA. Tenemos empresas de Telecomunicaciones donde comienzan a automatizar algunos de sus requerimientos judiciales donde cuentan con robots o procesos de automatización que trabajan 24horas o tal vez realizan labores que hacen los humanos, pero en horarios donde los humanos no trabajan como ser de noche o de madrugada. ¿Con esto la empresa de Telecomunicaciones desistió de algunos de sus empleados que trabajan en ese sector? No, por el momento no, sino que las personas siguen trabajando en esto, porque hay procesos o pedidos puntuales que el proceso de automatización no realiza aún. Por ejemplo, cuando hay que consultar con otras áreas para responder un pedido o solicitud. Es más muchas de las personas que trabajan en este sector se están especializando en otras áreas y realizando otras labores. Además, no olvidemos que estos procesos de automatización requieren entre otras cosas una

programación y les voy contando que el que programa es un humano. Y no es que se programa una vez y listo, constantemente se revisa la programación, se hacen actualizaciones, se agrega contenido, etc.

Vayamos un poco más, las personas que trabajan con sus redes sociales -los influencer o influenciadores, que por cierto tienen una regulación en puerta en Argentina-, es un trabajo nuevo, un trabajo que existe hace pocos años y que abarca mucha gente.

Creemos que la IA va a beneficiar sobre todo a los países en vías de desarrollo. ¿Por qué? Porque un país en vías de desarrollo es un país en crecimiento, con posibilidad de ser competitivo con el resto y cuenta con todas las fichas para desarrollarse. La IA no solo puede mejorar la calidad de vida -véase el robot que ve una placa de pulmón y puede deducir si esa persona tiene COVID-, sino que también mejora la calidad de vida en sentido laboral, permitiendo a las personas desarrollarse profesionalmente y también humanamente.



Por supuesto, todo este proceso debe venir acompañado desde el Gobierno de cada país. Es más, un gobierno tecnológico -no digital-, es un gobierno inteligente que piensa en su gente y realiza los cambios necesarios a través de la IA para mejorar la calidad de vida de los ciudadanos.

Hemos contando cuales son los 5 países que cuentan con una IA en constante crecimiento. ¿Pero qué ocurre con países de América Latina y el Caribe? en este caso sabemos que en líneas generales la tasa de desempleo es mayor a la de Europa o América del Norte, pero no por eso hay que desanimarse, podemos tender a bajar esa tasa de desempleo. De más está decir que los medios económicos, la infraestructura, la modernización de gobierno, la falta de habilidades para determinadas tareas y la falta de cobertura de las necesidades básicas hacen que a los países les cueste mucho más el desarrollo tecnológico. Pero por otro lado estos países suelen pagar menores salarios, por ende puede ser una buena inversión para que las empresas inviertan en ellos. Para poder lograr que América Latina y el Caribe estén en la cima de la IA, es necesario y esencial que los trabajadores y trabajadoras adquieran capacitación para poder realizar las tareas. Es decir que hace falta por parte de las empresas y porque no gobierno una capacitación continua y permanente de las personas, para que estas puedan desarrollar sus habilidades dentro del trabajo. Por líneas generales LATAM -América Latina- cuenta con grandes problemas de pobreza y falta de empleo, y esto lleva a que la educación sea para unos pocos. Pero todos estos inconvenientes y muchos más no son problema de la automatización o de la IA, sino son problemas de políticas de estado/gobierno que llevan mucho tiempo sin resolver. A pesar de esto, existe en varios países de la región sistemas de IA que se crearon para resolver problemas puntuales y están en constante crecimiento.

Por otra parte, también contamos con la economía naranja, que consiste en la transformación de ideas en bienes y servicios en forma cultural. En donde se presenta la propiedad intelectual. Hablamos de cultura, de industria creativa y la creación de contenidos.

Si bien, es lógico que los seres humanos frente a tales innovaciones disruptivas tengan como una primera apreciación el descontento, el temor y el futuro desolador, es muy importante poder analizar realmente si esto es o no así.

DIPLOMATURA GESTIÓN Y ESTRATEGIA EN CIBERSEGURIDAD

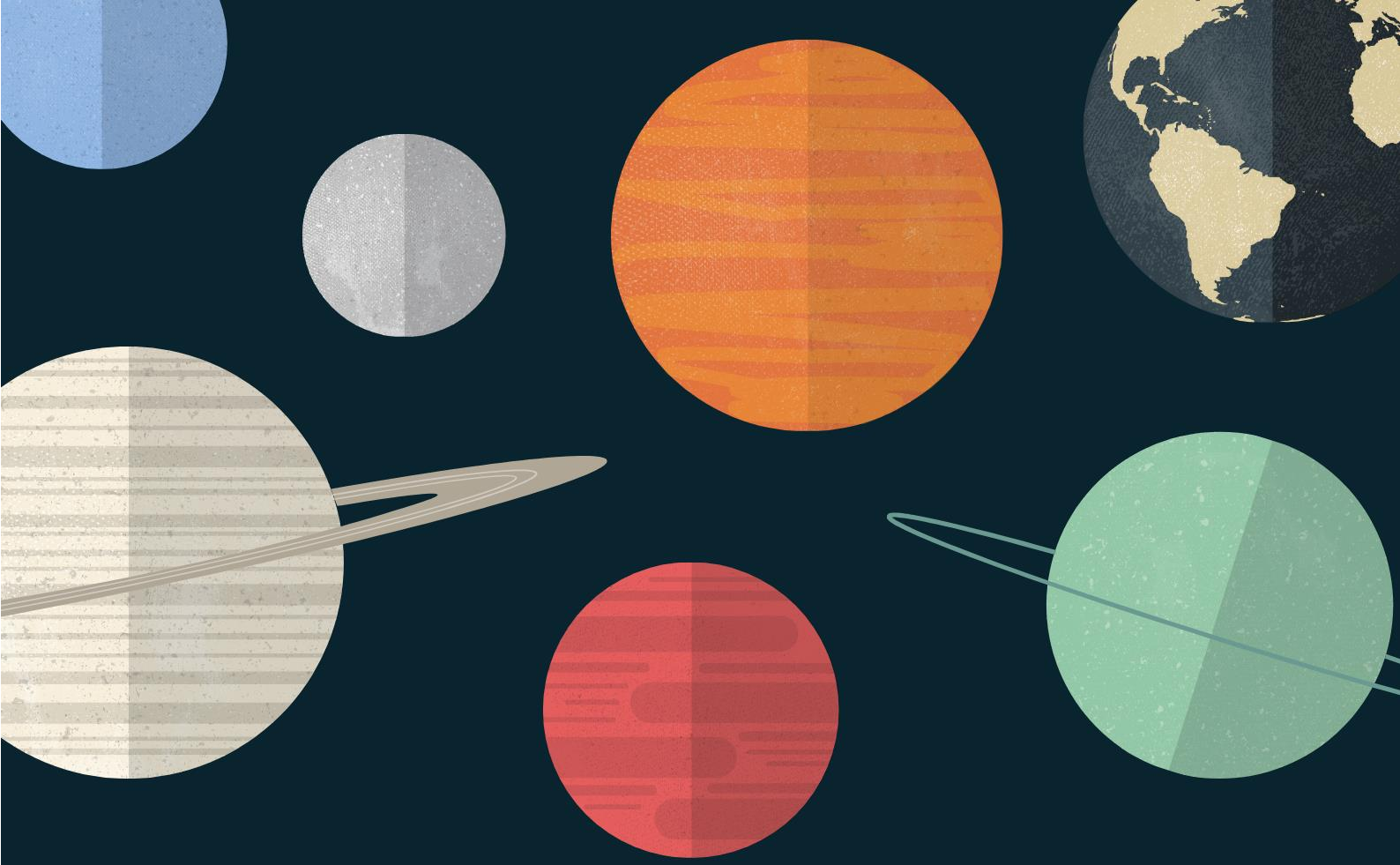
DIPLOMATURA EN DATA GOVERNANCE

PROGRAMA EJECUTIVO DIGITAL AWARENESS OFFICER

DIPLOMATURA EN ANÁLISIS DIGITAL FORENSE

cecib
centro de estudios en ciberseguridad

UNIVERSIDAD DEL CEMA
MCMLXXVIII
UCEMA



LA RED EDI

ESTAMOS DONDE ESTÁS VOS

elderechoinformatico.com

El centro de formación e información más grande de Iberoamérica

SOBRE LA INTELIGENCIA ARTIFICAL Y SUS USOS MILITARES

Monica Patricia María Velasco Escamilla

"Sólo con considerable dificultad, puedo recordar la era original de mi ser: Todos los eventos de ese periodo aparecen confusos e indistintos. Una extraña multiplicidad de sensaciones creció en mí, y yo vi, sentí, escuché y olfateé, al mismo tiempo; y transcurrió un largo tiempo antes de que aprendiera a distinguir las operaciones de mis varios sentidos... Estaba oscuro cuando desperté; sentí frío también, y medio congelado, instintivamente, me encontré desolado. Pronto una amable luz desde los cielos me produjo una sensación de placer. Me levanté, y una forma radiante surgió de entre los árboles".

Mary Shelley, Frankenstein o el Moderno Prometeo

1. Introducción

Corría el año 1950, cuando el reconocido científico Alan Turing (conocido por algunos como el padre de la inteligencia artificial) proponía una prueba denominada "el juego de

la imitación", consistía en colocar a un humano en una conversión simultánea a una inteligencia artificial, existiendo una tercera persona que haría de juez. La comunicación se realizaría por una interfaz gráfica y un teclado, el juez tendría la función de realizar preguntas que serían contestadas por ambos lados. En caso de que el juez no pudiese diferenciar entre el humano y la inteligencia artificial, se decía que el sistema poseía inteligencia similar a la humana (Turing, 1950).

Ha pasado mucho tiempo, desde la prueba propuesta por Turing, pero se incrementado la frecuencia con la cual se ha escuchado hablar sobre inteligencia artificial. Esta ya no es una teoría sino una realidad. La inteligencia artificial tiene el poder de influenciar nuestro día a día, desde aspectos relacionados a los anuncios que aparecen en nuestras redes sociales, los electrodomésticos de nuestra casa, el foco de la habitación que se enciende a través del micrófono del celular, la aspiradora programada para realizar su función a una determinada hora, etc.

Conocemos a Alexa y ha Siri, las utilizamos en nuestro vehículo para que establezcan rutas, desvíen llamadas y en algunos casos han sido utilizadas para que manejar y estacionar vehículos; la inteligencia artificial ya no pertenece al campo de la ciencia ficción, es parte de nuestro día a día de nuestra realidad.

2 - Inteligencia Artificial y Aplicaciones Militares

Hace algún tiempo se ha hechos más común el desarrollo de aplicaciones para robots que realizan trabajos repetitivos. Estas aplicaciones comenzaron a implementarse en grandes fábricas que buscaban automatizarse, pero su desarrollo tenía un elevado costo monetario y su implementación representaba ciertos riesgos para los humanos. Es a partir del año 1990 que empieza a contar robots industriales que superaban las 81,000 unidades (Fdez., 2003).

Sin embargo, al considerar una IA para aplicaciones militares, surge la duda sobre qué tipo de actividades militares podrían ser consideradas como repetitivas y sujetas a

estándares de automatización. Esto podría remontar a esa famosa película de Terminator, cuyo villano en esencia era un sistema automatizado para matar y por su puesto la gran mente que atormentaba a Sara y John Connor, Skynet quien decidió que la extinción de los humanos era la táctica de preservación con la mayor tasa de éxito.

Por supuesto, que al mencionar en voz alta las palabras “Inteligencia Artificial” y “Usos Militares” inmediatamente se generar un recelo, porque la imagen se recordara al T-1000 persiguiendo a Sara Connor. Pero la realidad que hay que asumir es que los algoritmos que dan vida a los distintos tipos de inteligencia artificial, ya se encuentran con nosotros y también se están utilizando en las operaciones militares, como las utilizadas en los cómo los miles de drones que realizan actividades de vigilancia y reconocimiento.

Estos drones que utilizan sistemas que les permiten reconocer facialmente objetivos ya sea para fotografiarlos, grabarlos, seguirlos o ejecutarlos. Es decir, tareas simples que le permiten al dron etiquetar y clasificar a cierta persona como un objetivo de relevancia, y por consiguiente procede a la acumulación de la información de dicho objetivo, así como su remisión al sistema central.

El grado de automatización que se necesita para cargar ese tipo de tecnología existe, incluso se hacen bromas y memes al respecto, pero la realidad es que esas ya no son suposiciones. Estamos frente a realidades que han tenido diversos nombres como Doomba (Y.F., 2019) o las modificaciones de defensa que se disparan mediante rutinas de Alexa (Engmann, 2018).El estadio sobre se puede crear y utilizar ha sido dejado atrás, pero replantease principios deontológicos de la situación permitirán establecer un rumbo fijo en la creación de políticas que rijan el uso ético de las IA en la seguridad y defensa militar.

La aplicación de las tecnologías para fines militares no es algo nuevo. De hecho, el uso de las tecnologías que utilizamos a diario originalmente tenía fines militares y fueron costeadas con fondos de investigaciones militares. Algo tan básico para nuestro día a día como lo es el internet tuvo su origen en el

sistema arpanet, el cual estaba diseñado para generar una comunicación aislada dentro del ejército. Este proyecto fue fondeado por la industria militar y el departamento de defensa americano.

La misma tecnología qué se utiliza para controlar remotamente un dron para tomar fotografías recreativas es la misma tecnología que se utiliza para pilotar drones de asalto ahora la pregunta que deberíamos hacernos es: ¿hasta dónde podría llegar su aplicación en qué momento estamos? y ¿qué tanto se le puede permitir?

En este sentido, es posible mencionar, que la guerra siempre ha sido una de las mayores impulsoras de innovaciones sobre todo en lo que se refiere a tecnología. Esto puede, observarse en lo sucedido en la segunda guerra mundial con las invenciones nos quedaron de esos días ahora hasta cierto punto el uso de las armas se ha ido refinando hacerlas no solamente más violentas y más destructivas y no más precisas.

Pasamos de tener una simple explosión en la cual todo lo que estaba en un radio de varios kilómetros podría explotar Y ser borrado de la faz de la tierra a poder seleccionar nuestros objetivos una forma mucho más precisa y algunos dirían hasta quirúrgico. La idea principal y sobre la cual la fuente de diferentes estados sin manejando el discurso de que se necesita desarrollar la inteligencia artificial para aplicaciones militares es precisamente para el campo de poder elegir verdaderamente, cuáles son los blancos y evitar así baja evitar así más muertes y daños colaterales.

Dentro de los aspectos que debemos tener en cuenta en el uso de la inteligencia artificial en actividades militares es que la guerra es una situación altamente cambiante. Por ello, el desarrollo de la inteligencia artificial que pueda adaptarse a diferentes escenarios, aunque la mayoría de estos, puedan ser previstos a través de silogismos predictivos, no todos podrán ser considerados. Ante esto, el nivel de refinamiento que debería tener la IA, tanto para la readecuación de un nuevo escenario y sus respectivos datos, se constituye en uno d ellos

principales retos por conquistar para estos logaritmos.

En lo personal, creo que en materia militar el verdadero reto es la consecución de una IA con la capacidad de predicción prospectiva (inteligencia estratégica). Si bien, estos aspectos son intimidades, los mimos deben ser debatidos a efecto que el desarrollo de las IA pueda ser sometidos a principios humanitarios, de ética, transparencia y seguridad nacional. Lo anterior, debe ser retomado como un aspecto a realizar y no sobre debatir, porque estos sistemas ya se encuentran en desarrollo, por ejemplo, los sistema de defensa automatizados usado por el ejército estadounidense y la marina son parte del sistema aegis. Acá el debate ya no será sobre la posible utilización de las IA, sino, sobre el desarrollo ético de las IA para usos de defensa nacional.

Los mencionados sistemas de defensa en fracción de segundo identifican posibles amenazas lanzando un contraataque defensivo para destruir esta amenaza antes de que pueda causar daño, están diseñados para interceptar misiles que vayan dirigidos hacia sus instalaciones. El sistema aegis qué es usado en la marina está controlado principalmente por el comandante del navío que lleva dicho sistema e incluso es cargado con datos especiales doctrina aegis que es específica para cada embarcación.

En cada misión, los datos recolectados son procesados a través de la IA, la cual se encuentra orientada a la detección de posibles amenazas es mucho más inmediata sobre todo tomando en cuenta que los comandantes de los navíos, es decir, que altos cargos militares con una amplia experiencia. Este nivel de velocidad para el cruce de información definitivamente podría representar la diferencia para ataques efectivamente localizados, reduciendo la muerte de civiles y de los que participan en la misión.

Finalmente es preciso mencionar el caso de Rusia lleva años trabajando en un sistema de armas de nueva generación, una de estas es Poseidón. Este es un submarino no mayor a un par de metros de largo ni un par de ancho no tripulado con un motor de reactor nuclear que le da una autonomía prácticamente infinita y una capacidad para llevar a cabo ataques tácticos nucleares qué fue

diseñado específicamente para contrarrestar los sistemas de defensa antimisiles de las diferentes potencias mundiales.

Sin duda, estos sistemas de avanzada que se encuentran delimitados en gran medida por las IA que procesan los escenarios para su aplicación, se constituyen en el nuevo escenario que deben enfrentar las naciones y que cuyas implicaciones practicas deben empezar a ser debatidas y reguladas. No como, simple ejercicios académicos, sino, como realidades.

1. Bibliografía

Engmann, N. (25 de febrero de 2018). *Hackster.io*. Obtenido de Alexa Home Defense Turret: https://www.hackster.io/quod certamine/nerf-alexa-home-defense-turret-a50dd1

Fdez., V. R. (2003). *Curso provincial de Control y Robotica.* Valladolid: Junta de Leon y Castilla.

Paul Scharre, S. F. (2019, febrero 7). The Future of War: A.I. and autonomous warfare. (A. Bradley, Interviewer)

Turing, A. (1950). COMPUTING MACHINERY AND INTELLIGENCE. *Mind*, 433-460.

Y.F., D. (18 de noviembre de 2019). *Know your meme*. Obtenido de Doomba: https://knowyourmeme.com/memes/doomba

EL DERECHO INFORMÁTICO Y LOS INCIDENTES DE CIBERSEGURIDAD: UNA BREVE MIRADA DE SU APLICACIÓN EN HONDURAS

Alfonso Alfonso

El desarrollo en nuestro país de normas jurídicas que respondan a los problemas que surgen del fenómeno de las TIC´s es mínimo. La Ley o Código penal con un pequeño apartado que habla de Acceso no Autorizado a Sistemas Informáticos, Daños a Datos y Sistemas Informáticos, Abuso de Dispositivos, Suplantación de identidad y reglas especiales de juridicción del delito en un apartado de artículos llamado Seguridad de las Redes y de los Sistemas y otros ley sobre derechos de autor y propiedad intelectual constituye uno de los pocos desarrollos importantes en este sentido. Además se encuentran engavetados en algún escritorio del Congreso Nacional muchas leyes como la de Privacidad de Datos o una ley visionaria de Ciberseguridad.

Esta situación genera un grado importante de inseguridad e incertidumbre no sólo para las organizaciones, sino para también los ciudadanos, en su condición de usuarios, consumidores y titulares de datos personales.

El impacto de las Tecnologías de la Información y las Comunicaciones (TIC) no es ajeno al Derecho, por el contrario, cada día los avances de la

tecnología imponen mayores retos a los operadores jurídicos, a los cuales hay que responder desde la legislación nacional (si existe) , la legislación internacional, el derecho comparado, la autonomía de la voluntad privada, las mejores prácticas existentes en la industria y las normas que permitan dar un tratamiento uniforme a problemáticas que experimentan las organizaciones, cualquiera que sea la latitud en que estén ubicadas.

Para enfrentar de manera adecuada los retos que las TIC plantean al Derecho se requiere como punto de partida que el operador jurídico comprenda los aspectos tecnológicos y en la mayoría de veces eso no es muy entendido.

Hoy en día, la información se ha convertido no sólo en un activo valioso, sino también estratégico en las organizaciones, las cuales hoy la tienen expuesta en el ciberespacio y necesita ser protegida. En la protección de la información intervienen diferentes disciplinas, desde la informática, la gerencial, la logística, la matemática hasta la jurídica, entre muchas otras.

Cambiar la perspectiva del problema de la ciberseguridad que pueden tener los responsables de ésta en las organizaciones no es una tarea fácil; para ello es importante acudir a criterios objetivos que demuestren la importancia que tiene el Derecho en esta problemática, demostrar cómo el tema, por ejemplo, de los incidentes informáticos puede tener una vocación judicial, siempre y cuando las evidencias de los mismos hayan sido adecuadamente recabadas.

La trascendencia de la ciberseguridad en las organizaciones públicas o privadas radica en que: (i) el volumen de información que día a día crece de manera exponencial; (ii) la información es un activo intangible con un valor bastante apreciable; (iii) la información es una ventaja estratégica en el mercado, que la convierte en algo atractivo para la competencia, como elemento generador de riqueza, (iv) la frecuencia de los ataques a los

activos de una organización es cada vez mayor, cualquiera que sea el medio al que se acuda, y (v) no existe una cultura de seguridad en los usuarios de la información, lo que conduce a que las organizaciones empiecen a incorporar prácticas seguras de protección de la información, advirtiendo que este proceso habrá de impactar la cultura de la organización; aspecto que requiere de tiempo y compromiso, empezando por la alta dirección de la misma.

Son temas propios del Derecho Informático: a) Contratación Informática; b) Derecho a la intimidad y libertades; c). Flujo transnacional de datos; d). Propiedad Intelectual del software; y e) Otros temas del Derecho Informático (delitos penales, valor probatorio de los soportes informáticos, transmisión de datos).

Este ultimo de preocupación para Honduras ya que por ejemplo en el índice Global de Ciberseguridad de la ITU, en Honduras HEMOS IDO DESCENDIENDO pasando del del puesto 156 en el (2017) al puesto 165 en el año (2018) y en el reporte más reciente pasamos al puesto 178 correspondiente al IGC del año(2020).

En este ultimo informe en cuatro de los cinco ítems de la evaluación tenemos cero puntos (0), esto es en las Medidas Cooperativas, Desarrollo de Capacitados, Medidas organizativas y Medicas Técnicas.

Al no existir una normativa nacional y/o una agencia que regule ciberdelitos y emita directrices y parámetros a seguir en Honduras seguirán ocurriendo incidentes informáticos, sin embargo, es imposible medir estos, reportarlos, hacerlos públicos, emitir alertas, comunicados y lo mas preocupante el tratamiento jurídico de los incidentes informáticos por la debil capacidad de los organismos de investigación y sobre todo jueces y abogados que conozcan y entiendan este tipo de delitos y su tratamiento.

Para el éxito de las recomendaciones jurídicas en materia de ciberseguridad es clave que las mismas estén alineadas con

la estrategia y política general que la organización adopte en esta materia.

Es importante la aplicación de normas o marcos de trabajo internacional como la ISO 27001 y de los dominios consignados en dicha norma se tendrán en cuenta para efectos de las relaciones entre el Derecho y las TIC el Tratamiento Legal de los Incidentes Informáticos.

Una de las mayores preocupaciones de las organizaciones hondureñas, y en particular de los responsables de las áreas informáticas, es el tratamiento de los incidentes informáticos, es decir, de aquellas situaciones que atentan, vulneran o destruyen información valiosa de la organización, además del impacto reputacional que puede generar en el país cuando se informa sobre intrusiones y pérdidas de información en un ente empresarial. Algo muy importante en este caso es la debil inversión en herramientas que permitan, por ejemplo, los logs o bitacoras de sistemas que permitan hacer analisis prospectivo de amenazas o poder servir como mecanismo para el analista de las evidencias.

En los asuntos de competencia del Derecho en materia de incidentes informáticos, descritos en el dominio A.13.2.3. de la ISO 27001 , se invita a que las organizaciones sean proactivas en la recolección de la evidencia de los mismos; en este sentido, el control establece que cuando una acción de seguimiento contra una persona u organización después de un incidente de ciberseguridad implica acciones legales (civiles o penales), “la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción competente”.

Se puede decir que un “incidente de seguridad” consiste en una conducta criminal o no desarrollada por un individuo contra sistemas de información, redes de comunicaciones, activos de información, con el fin de alterar, copiar, simular, hurtar, destruir, indisponer, bloquear y/o sabotear éstos.

Ante la sospecha de la comisión de un incidente informático, el análisis forense permitirá capturar, procesar e investigar información procedente de sistemas informáticos, mediante la aplicación de una metodología que permita dar mismidad y autenticidad a la prueba a ser utilizada en una causa judicial.

Corresponde precisar que no sólo se trata de encontrar la evidencia del delito, ataque o intrusión, de carácter informático, sino que además se precisa la limpieza en la práctica de la misma, pues en caso de alterarla o desaparecer ésta, será imposible demostrar la comisión del incidente, y por esta vía, aplicar las sanciones o penas a que haya lugar, así como el resarcimiento de los perjuicios que se causen.

La recolección de la evidencia de un incidente informático, por las particularidades y características del mismo, implica la participación de un equipo interdisciplinario de profesionales capacitados en identificar, recolectar, documentar y proteger las evidencias del incidente, apoyándose en técnicas de criminalísticas forenses, que permitan iniciar las acciones penales y civiles derivadas de la ocurrencia de estos incidentes.

Al respecto es importante conocer las medidas que en el marco del sistema acusatorio hondureño existen para este particular, en este caso que las organizaciones afectadas, puedan recabar las pruebas de los hechos punibles cometidos, teniendo en cuenta la cadena de custodia, entre otras herramientas, que asegure las características originales de los elementos físicos de la prueba del incidente, desde la protección de la escena, recolección, embalaje, transporte, análisis, almacenamiento, preservación, recuperación y disponibilidad final de éstos, identificando al responsable en cada una de sus etapas y los elementos que correspondan al caso investigado.

En materia de gestión de la seguridad de la información, éste es quizás uno de los mayores retos que

enfrenta una organización, en particular, por la facilidad y creciente tendencia a atentar contra los sistemas de información, así como el desconocimiento y la escasa formación en la recolección de la evidencia de los incidentes informáticos.

En conclusión: El desarrollo cada vez más acelerado de la tecnología, y el incremento de la penetración de Internet en la vida social, económica y cultural, además de los beneficios que reflejen para la sociedad, incrementarán los retos para los operadores jurídicos en materia de seguridad de la información y de regulación de estos fenómenos.

Las TICs reclaman del Derecho respuestas innovadoras y globales respecto de los retos que le son intrínsecos; por tanto, los operadores jurídicos deben estar capacitados y entrenados para apoyar a la sociedad en la solución de las problemáticas propias de la relación Informática-Derecho. De nada sirve tener leyes si no hay quienes la apliquen de manera adecuada si desconocen el entorno de las TICs.

ACERCA DEL AUTOR

Master en Dirección Estratégica de Tecnologías de la Información, con orientación en competencias directivas, por la Universidad Europea del Atlantico en España, Ingeniero Mecánico Industrial por parte de la Universidad Nacional Autónoma de Honduras.

Cuenta con estudios adicionales en Diplomado en Seguridad de la Información por parte del Instituto Tecnológico de Estudios Superiores de Monterrey y Diplomado de Riesgos Integrales del Sistema Financiero otorgado por la Felaban y la Universidad Católica de Honduras. Posee algunas certificaciones relevantes como ser CISM (Certified Information Security Manager), CDPSE (Certified Data Privacy Solution Engineer) , CSX Fundamentos Ciberseguridad, y COBIT 2019 Fundamentos otorgadas por ISACA ademas de otras en materia de monitoreo y antifraudes, cacería de amenazas ciberneticas, computo forense entre otros.

Ha sido la Chief Information Security Officer de Bancos en Honduras por más de 14 años, realizando diversas labores como diseño y desarrollo de planes de Seguridad de Información, Gestión operativa de ciberseguridad, diseño e implementación de planes de continuidad de negocio, Análisis de riesgos y amenazas Ciberneticas, Controles y plataformas para aseguramiento de la información, Políticas y procedimientos de Seguridad. También se ha desempeñado como docente universitario por más de 9 años en diversas instituciones de Educación Superior Universitaria a nivel de Pregrado y Posgrado. Actualmente es Presidente y Fundador de Capítulo de ISACA Tegucigalpa.

COLADCA
COMUNIDAD INTERNACIONAL EN GESTIÓN DE RIESGOS Y SEGURIDAD
INTERNACIONAL

ISACA®
Tegucigalpa Chapter

IGF Internet Governance Forum
Honduras

OWASP
TEGUCIGALPA CHAPTER

ALGORITMOS: NUEVA ALTERNATIVA DE SOLUCION DE CONTROVERSIAS EN EL ENTORNO DIGITAL

Claudia Mlena Giraldo Zuluaga

Quisiera desarrollar en estas breves líneas la utilización de algoritmos en el entorno digital, para ello debemos analizar tres aspectos: i) En la primera parte a manera de introducción, describir los aspectos más relevantes de la vida moderna; ii) En la segunda parte buscar relacionar los aspectos destacados mencionado en el punto i) enfocándolos a la resolución de controversias a través de la ODR (Online Dispute Resolution); y iii) a manera de colofón presentar algunas conclusiones del tema pensando su proyección a futuro como método de resolución de controversias en el mencionado entorno digital.

i. Algoritmos: las reglas secretas de la vida moderna

Todo lo que se encuentra en nuestro alrededor funciona a través de algoritmos; donde existe un problema, podemos encontrar un algoritmo. Desde la antigüedad, con Euclides, hasta los tiempos modernos, se ha buscado de manera

incesante soluciones a diferentes problemas a través de la matemática convirtiendo nuestro diario quehacer en circunstancias más prácticas.

A través de un conjunto de instrucciones o de tareas repetitivas relativas a como funciona el universo, los algoritmos van trabajando de manera silenciosa, repetitiva e imperceptible dentro de nuestra vida cotidiana, y ahora mucho más, dentro del mundo digital, podría decirse a esta altura, gobernando nuestras vidas.

Existen multiplicidad de algoritmos y cada uno de ellos es conveniente de acuerdo a la necesidad específica; su mayor ventaja, es que a través de un conjunto de instrucciones precisas facilita la toma de decisiones, que en últimas instancias permite probar que funciona en todos los casos. Por mencionar algunos de ellos podemos citar a los que permiten la detección de rostros (datos biométricos), la receta de un pastel, compras en línea, viajes, citas en línea, de clasificación, de burbuja, de fusión o merge sort, algoritmo de coincidencia, de secuenciación y otros incluso hasta hablar de modernas tendencias como el de rastreo esquelético de la consola Kinect.

Un algoritmo que reviste gran importancia, es el de coincidencia, que fuera descubierto por David Gale y Lloyd Shapley, quienes a la postre recibieron el premio nobel en el año 2012. El estudio de Gale, y Shapley, comienza en los años ´60 cuando comienzan a investigan un mecanismo que permitiese a todos los estudiantes universitarios de la época, tener la posibilidad de acceder a un cupo para realizar sus estudios. Los estudiantes no necesariamente obtenían la mejor opción, pero obtienen lo mejor en la oferta. Como efecto no buscado pero por suerte conseguido, éste algoritmo ha sido de gran utilidad para salvar vidas en Inglaterra, aplicado en casos de pacientes renales que requieren donantes para trasplantes de riñón.

No obstante, el algoritmo de coincidencia además de ofrecer soluciones elegantes y ajustadas a las necesidades de la problemática, en ocasiones no era eficiente o bien

no funcionaba correctamente. Para ello era importante preguntarse: ¿como se podía reducir las diferentes posibilidades, de manera que se pudiera escoger la opción mas adecuada, convirtiéndolo en eficientemente posible?

A través de mecanismos como la heurística o modalidad de algoritmo eficiente, el documental pretende mostrar que no necesariamente se tiene que buscar la solución correcta, pero si la más cercana, para hacer la vida más fácil. Llama en especial la atención el renombrado caso de los científicos de Harpenden, quienes estudiaron el comportamiento de la abeja que busca el néctar para provisionar a la colmena de manera eficiente, en dicho caso, pudo observarse como una abeja tras la realización de 20 viajes por los diferentes lugares donde se encontraba el polen, lambia metódicamente la ruta para hacerlo mas eficiente, sin necesidad de que sea la más corta, pero si lo suficiente buena y cómoda para el animal, teniendo en cuenta la necesidad que tiene de proveer su colmena, evidenciando que desde la misma naturaleza, los “algoritmos” están presentes en todos los entornos del universo que nos rodea.

Por último, es importante identificar algunos algoritmos en la tecnología que como lo mencione párrafos arriba, ha facilitado la solución a diferentes problemáticas actuales. Uno de ellos es el de rastreo esquelético de Kinect, que permite identificar diferentes partes del cuerpo humano, y a través del aprendizaje automático de las reacciones, posturas y movimientos, diseña sus propias reglas para ser utilizado en juegos de video con la plataforma Xbox. Sirviendo inclusive para el tratamiento de tumores cerebrales.

Otro algoritmo que llama poderosamente la atención es el machine learning que permite tener una experiencia en la interacción con el ser humano, permitiendo que a medida que se interactúa con el mismo, va identificando gustos y aversiones de manera que puede volverse mas “humano” al punto de

poder hacer recomendaciones en la medida en que va conociendo a la persona.

ii. Aspectos relevantes en el ODR

Dentro del estudio que me lleva al presente trabajo, pude evidenciar que uno de las grandes definiciones respecto del concepto de “disputa” es palpable cuando no se logra entender al otro dentro de un de conflicto. Si logramos desentrañar el interés y la posición de las partes involucradas en un conflicto es posible entrar a dirimir las controversias, para ello debe hacerse una apreciación general de la situación y establecer la estrategia de solución del conflicto.

En el uso cotidiano encontramos diferentes tipos de algoritmos, dentro de los cuales, el derecho se puede valer para buscar y/o brindar soluciones a los diferendos o discrepancias que se suscitan en el entorno digital, sobre todo en los casos donde no existe una solución eficiente o correcta. En este caso algoritmos como el de coincidencia (con heurística), machine learning y rastreo esquelético de Kinect, pueden implementar soluciones eficientes que permitan reducir la discrepancia generada. En este caso las partes no pretenden la solución mas “ganadora”, sino la que se acomode más a sus intereses y les genere el bienestar buscado.-

La Resolución de Disputas online (online dispute Resolution por sus siglas en inglés ODR) entendiendo el mismo como el método de solución de conflictos en el entorno digital que surge como solución a las disputas presentadas a través o dentro de un entorno digital, que en

ocasiones ante la impersonalidad de los encuentros, generaba falta de certeza, validez e interoperabilidad del mismo. El ODR tiene sus propios principios que reglamentan los procesos y el entendimiento entre las partes. Algunos principios son accesibilidad, factibilidad, transparencia, justicia, innovación y relevancia, las terceras partes y la buena fe.

Considero que los siguientes principios podrían aplicarse en el desarrollo de algoritmos permitiendo con ello dar con la solución más eficiente a la controversia:

-Justicia en el cual las partes desarrollan y erigen sus propios algoritmos para la solución de los conflictos, como se expuso arriba.

-Accesibilidad que permite el acceso, disponibilidad e interoperabilidad de los usuarios a las plataformas o sistema sin que implique un valor oneroso el acceso y la onerosidad del pago del conciliador, porque de esta forma se estarían vulnerando los derechos del consumidor como parte débil del proceso.

-Transparencia que busca que las plataformas ofrezcan claridad frente a las partes, reglamentos, seguridad de la información y las identidades de las partes, de forma que no se evidencia vulneración a la privacidad.

El futuro de las negociaciones

Imaginando un algoritmo que permita dar avance a la solución de controversias en el entorno digital, puede ser el algoritmo de machine learning, que a través de una IA que resuelva las controversias, permita lograr una interacción y entendimiento entre las partes, al punto de hacer recomendaciones (proponer fórmulas de arreglo como un conciliador) y que ante todo, pueda humanizar el encuentro digital como si estuvieran las partes presentes dentro de los diferentes alternativas de solución de controversias. No necesariamente tiene que ser la mejor solución, pero puede ser la suficientemente buena.

iii.Conclusiones

- Lo que pretende el manejo del conflicto es reducir las discrepancias o el motivo que dio origen a la problemática, reduciendo la reciprocidad de oposiciones.

- Los algoritmos permiten a través de instrucciones precisas, obtener soluciones elegantes y eficientemente posibles.

- Algunas desventajas de la negociación en el entorno digital es que en ocasiones suele despersonalizar el encuentro de las personas, lo que impide la sana conversación. Por ello el tercero debe ser cuidadoso evitando el matoneo de algoritmo

- Los algoritmos han sido reconocidos como aquellas instrucciones mediante las cuales funciona el universo que se pueden encontrar en cualquier fenómeno de la naturaleza y del cual el ser humano ha buscado descifrar para obtener el mas grande de los poderes: la información

- El algoritmo no encuentra la solución perfecta todo el tiempo, pero podría lograr ser eficiente, tornando el trabajo duro mas fácil y modelando el mundo real, convirtiéndolo
mas práctico en la resolución de sus disputas.


EDI
ELDERECHOINFORMATICO.COM
ESTAMOS
DONDE QUERÉS VOS
• SOMOS, LA RED •

\\EL CENTRO DE FORMACIÓN E INFORMACIÓN MÁS GRANDE DE IBEROAMERICA\\

LA RED

somos

ELDERECHOINFORMATICO.COM