LA IMPORTANCIA DE LA PROTECCIÓN DE DATOS Y LA SITUACIÓN ACTUAL DEL ECUADOR

THE IMPORTANCE OF DATA PROTECTION AND THE CURRENT SITUATION IN ECUADOR

A IMPORTÂNCIA DA PROTEÇÃO DE DADOS E A SITUAÇÃO ATUAL DO EQUADOR

*Belén Rivera**

Recibido: 03/05/2020
Aprobado: 13/06/2020

Resumen

Los múltiples avances tecnológicos han traído consigo grandes beneficios a la vida de los individuos, pues facilitan las rutinas diarias y permiten el acceso casi inmediato a la información y al conocimiento. Si bien este gigantesco desarrollo ha revolucionado la forma de vivir y de hacer las cosas; para lograrlo, ha sido necesario crear un mundo digital paralelo, lleno de datos e información que se ha utilizado durante muchos años, sin ningún control. Tal es el caso del Ecuador, donde todavía no existe una Ley de Protección de Datos que permita garantizar el derecho ciudadano a disponer y decidir libremente sobre ellos. El conocimiento que existe sobre esta materia es escaso, y tal situación promueve posibles infracciones. Este ensayo pretende explicar qué son los datos personales y su protección. Además, se enfoca en analizar la realidad ecuatoriana, así como las normas que han desarrollado otras jurisdicciones para proteger a sus ciudadanos. De igual forma se explican cuáles son las consecuencias reales de un posible mal uso, en conexión con el potencial de la Inteligencia Artificial, el Aprendizaje Automático y el Aprendizaje Profundo.

Palabras clave: Protección; Datos; Inteligencia artificial; Aprendizaje automático; Aprendizaje profundo

Summary

The multiple technological developments have brought great benefits to our lives, making daily routines easier and allowing immediate access to information and knowledge. Although this gigantic progress has revolutionized our way of living and how things are done. To achieve this, it has been necessary to create a parallel digital world, full of data and information that have been managed without any control for many years. Such is the case of Ecuador, where there is still no Data Protection Law that allows citizens to freely establish and decide over their data. The knowledge that individuals have on this matter is scarce and this situation promotes possible breaches. This article explains what personal data is and how it is protected. It also analyses the Ecuadorian reality, as well as the legal regulations developed by other countries to protect their citizens. In the same way, it explains the real consequences of the misuse of data, especially when it is connected with the potential of Artificial Intelligence, Machine Learning and Deep Learning.

Key words: Protection; Data; Artificial Intelligence; Machine Learning; Deep Learning

Resumo

Os múltiplos avanços tecnológicos vêm trazendo grandes benefícios na vida dos indivíduos, pois facilitam as rotinas diárias e permitem o acesso quase imediato a informação e ao conhecimento. Ainda que este gigantesco desenvolvimento vem revolucionando a forma de viver e de como sao feitas as coisas; para consegui-lo, foi

* Abogada de los Tribunales de Justicia y Licenciada en Derecho por la Pontificia Universidad Católica del Ecuador; Master of Laws por Leibniz Universität Hannover. Secretaria Adjunta de la Academia Americana de Derecho Internacional CAIL – 2018. Es miembro de la Asociación Internacional de Profesionales de Privacidad, docente de la cátedra de Herramientas Informáticas y Bases de Datos Aplicadas al Derecho de la Universidad Tecnológica Equinoccial y Jefe del Departamento de Litigios Marcarios de Bermeo & Bermeo Abogados. Correo electrónico: mbrivera12@gmail.com

necessário criar um mundo digital paralelo, cheio de dados e informações que se utilizaram durante muitos anos sem nenhum controle. Tal é o caso do Equador, onde ainda não existe uma Lei de Proteção de Dados que permita garantir o direito cidadão para dispor e decidir livremente sobre eles. O conhecimento que existe sobre a matéria é escasso, e tal situação promove possíveis infrações. Este artigo pretende explicar o que são os dados pessoais e sua proteção. Ademais, se concentra em analisar a realidade equatoriana, assim como as normas que vem sendo desenvolvidas por outras jurisdições para proteger os seus cidadãos. Da mesma forma se explicam quais são as consequências reais de um possível uso indevido, em conexão com o potencial da Inteligência Artificial, a Aprendizagem Automática e a Aprendizagem Aprofundada.

Palavras chave: Proteção; Dados; Inteligência Artificial; Aprendizagem Automática; Aprendizagem Aprofundada

ECUADOR Y LA PROTECCIÓN DE DATOS

El Ecuador no cuenta con una Ley de Protección de Datos Personales que regule su tratamiento. Sin embargo, la falta de reglamentación no implica la inexistencia de un marco jurídico mínimo que proteja al individuo y a sus datos (El Universo 2018). Así pues, la Constitución de la República del Ecuador, en su artículo 66 numeral 19, dentro del Capítulo Sexto relativo a los Derechos de Libertad, reconoce y garantiza a las personas: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley."

De tal manera que el país reconoce la protección de datos personales como un derecho constitucional. Existe una obligación por parte del Estado, sus instituciones y todas aquellas compañías o personas que procesen datos, de protegerlos y recolectarlos, previa autorización expresa de su titular, siempre que su tratamiento se realice en cualquier parte del territorio nacional. A pesar de este mandato constitucional, el derecho no ha podido ser plenamente garantizado, debido a la falta de normativa técnica, y también a la falta de que la autoridad competente sea provista de capacidad para controlar y sancionar su uso inadecuado. Así se discutió en la "Mesa de Diálogo acerca del Órgano Rector en Acceso a la Información y Protección de Datos", organizada por Fundamedios, donde se analizó la importancia de contar con un organismo autónomo, capaz de regular estos temas de manera independiente (DINARDAP 2020).

Debido a esta coyuntura, hay que realizar un análisis de la situación actual de la protección de datos en el Ecuador; así como, entender cuál es la percepción del ciudadano común sobre este tema. Además, para determinar la relevancia del tratamiento de datos personales en la vida de los individuos, es conveniente revisar qué es un dato personal y qué significa inteligencia artificial, en paralelo con la normativa que se aplica en otras jurisdicciones.

Todos estos logros nos permitirán obtener una mejor perspectiva, para entender por qué es necesario contar con una regulación que permita procesar los datos de manera adecuada, a fin de proteger los derechos del ciudadano e incentivar el desarrollo tecnológico.

TOLERANCIA EN EL PROCESAMIENTO DE DATOS

La falta de regulación y control en esta materia ha permitido que el acceso a los datos personales de los ecuatorianos se convierta en una práctica tolerada; la cual, hasta cierto punto ha sido justificada por comerciantes y vendedores, quienes utilizan estos datos so pretexto de mejorar sus ofertas, segmentar sus preferencias, tratar al cliente por su nombre e inclusive ofrecer descuentos y ventajas accesibles desde su

ubicación (Lavin 2006). Sin embargo, ¿cuán importante es cuidar esta información? ¿realmente podría afectar a una persona que un tercero recolecte los datos de su localización, estilo de compra o preferencias si, en definitiva, con esa información le brindan un mejor servicio y le permiten acceder de manera más rápida a sus preferencias?

Para una sociedad que está acostumbrada a proporcionar su nombre, número de cédula, teléfono, dirección y correo electrónico cada vez que realiza una compra[1]; o que, entrega su documento de identidad para entrar a cualquier edificio u oficina, ¿el uso de sus datos personales es realmente percibido como una violación a la privacidad?, ¿se podría afirmar que el ecuatoriano considera estos actos como un atentado a su derecho constitucional de disponer y decidir sobre los datos de carácter personal o, por el contrario, lo considera como algo normal y beneficioso?

La sociedad ecuatoriana todavía no es consciente del uso que se puede dar a esta información. Llenar formularios y aportar datos sobre su etnia, tipo de sangre o nivel de ingresos económicos para simplemente obtener una tarjeta de crédito o inscribirse en un sorteo, se ve como algo aceptable y muchas veces necesario, para tener acceso a determinados servicios o calificar para ciertos créditos. Si un tercero solicita esta información es porque así lo requiere o porque forma parte de la "política" de dicha institución.

Son tantas las acciones y omisiones que se estarían cometiendo a la hora de procesar datos de carácter personal, que no es cuantificable el mal manejo que se hace de una base de datos o de la transferencia de los mismos. Sin embargo, cuesta afirmar que este mal manejo sea producto de una mala intención; cuando, en la sociedad ecuatoriana, de hecho, prima el desconocimiento.

Por este motivo es fundamental fomentar una cultura de respeto a los datos personales, y habrá que empezar por educar sobre qué significa un dato y cuáles serían las reales afectaciones que podrían ocurrir en caso de su mal manejo. El construir este marco de respeto, no solo motivará que exista un procesamiento responsable de datos, sino que va a evitar que casos como el de "Novaestrat" se vuelvan a repetir.

1. Caso Novaestrat

La consultora y analista de datos ecuatoriana Novaestrat, alojaba en Miami un servidor con datos personales y sensibles de aproximadamente 20 millones de ecuatorianos (Yeung 2019). Esta base incluía información de 7 millones de menores de edad y otros tantos millones de personas fallecidas. A pesar de que en la actualidad existen casi 17 millones de habitantes en Ecuador, la consultora poseía datos de 20 millones de ciudadanos, debido a que almacenaba la información de difuntos sin justificación alguna.

Los datos que habrían sido develados correspondían a nombres completos, fecha y ciudad de nacimiento, dirección domiciliaria, correo electrónico, cédula de identidad, Registro Único de Contribuyentes, información del Instituto Ecuatoriano de Seguridad Social, estado de cuenta bancaria, balances crediticios y tipo de crédito al que el ciudadano tenía acceso (Yeung 2019). Si bien hubo una respuesta inmediata por parte del Ministerio de Telecomunicaciones, los datos ya fueron expuestos y posiblemente vendidos, sin poder cuantificar el perjuicio que se generó para todos los ecuatorianos.

El representante legal de la compañía fue detenido para investigaciones por un presunto delito de violación a la intimidad, sin que hasta el momento exista una fórmula de juicio o sentencia en el caso (Vanessa Silva, 2019). Hasta la fecha, Novaestrat Compañía de Responsabilidad Limitada consta como una empresa activa, que ha cumplido sus obligaciones societarias y de existencia legal, de acuerdo con la información contenida en la página de la Superintendencia de Compañías, y únicamente figura un nuevo representante legal.

Debido a este sonado escándalo, que inclusive tuvo resonancia a nivel internacional, el 19 de septiembre de 2019, el Presidente del República Lenin Moreno

1 Así lo exige el Sistema de Rentas Internas.

remitió el Proyecto de Ley Orgánica de Protección de Datos Personales a la Asamblea Nacional (GK 2019). Al momento, el Proyecto se encuentra pendiente de primer debate, de acuerdo con la información de la página de la Asamblea Nacional.

Este Proyecto fue desarrollado en base a las necesidades y la realidad ecuatoriana; y fue inspirado en el Reglamento General a la Protección de Datos adoptado por la Unión Europa en 2016, que entró en vigor el 2018, de cuya evolución se hablará a continuación.

2. Normativa relativa a la protección de datos

Las leyes adoptadas por la Unión Europea (UE) para la protección de datos personales han sido siempre un marco de referencia para varias legislaciones, incluidas las de países latinoamericanos, tal como se lee en la página web oficial de la Autoridad de Protección de Datos de la Unión Europea (European Data Protection Supervisor 2018). Los valores comunes contenidos en los Tratados de Integración fomentaron la libre circulación de mercancías y personas (Unión Europea 2020). Este objetivo común, fuertemente perseguido por los Estados Miembros, implicó un gran movimiento de datos entre los países integrantes. El Parlamento y Consejo de la Unión Europea, preocupados por esta realidad, deciden emitir el 24 de octubre de 1995, la Directiva 95/46/EC, relativa a la "Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos".

Esta Directiva fue formulada en una época donde el número de usuarios de internet a nivel mundial alcanzaba apenas el 0.4% de toda la población existente (Internet World Stats 2020). Por esta razón, si bien la Directiva era innovadora para su tiempo, pues definía conceptos y regulaba de manera adecuada la transferencia de datos; pronto quedaría obsoleta por la rápida evolución de la tecnología, por cuyas dinámicas aparecieron sistemas y funcionalidades que se consideraban imposibles para ese momento.

En el año 2012, la Comisión Europea propuso una reforma a la Directiva 95/46/EC para reforzar los derechos de privacidad en línea e impulsar la economía digital de Europa. Desde entonces se empezó a trabajar en el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés).

El 12 de marzo de 2014, el Parlamento de la Unión Europea apoyó la implementación del RGPD con 621 votos a favor. Dicho Parlamento, el Consejo y la Comisión Europea llegaron a un acuerdo sobre el RGPD el 15 de diciembre de 2015, cuando fue finalmente publicado bajo la forma de regulación oficial el 27 de abril de 2016 (European Data Protection Supervisor, 2018). Sin embargo, el Art. 99 del RGPD, relativo a su entrada en vigor y aplicación, estableció que: "1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea"; y, "2. Será aplicable a partir del 25 de mayo de 2018." De manera que, si bien la norma fue aprobada en el año 2016, esta empezó a ser aplicable dos años después de su publicación.

El legislador europeo otorgó estos dos años de plazo para que las instituciones, organizaciones y empresas de los Países Miembros se pusieran a tono con las disposiciones contenidas en el Reglamento, a fin de que elaboraran protocolos, auditaran la cantidad de datos que manejan y eliminaran todos los componentes previos que no fueran absolutamente necesarios. La entrada en vigor del RGPD no solo puso en vilo a toda Europa, sino que exigió que países de fuera de la Unión que procesen datos de ciudadanos europeos acoplaran sus estándares a los exigidos por el RGPD (Goddard 2017, 704).

Todo esto se debió a la disposición de territorialidad contenida en el artículo 3 del RGPD que señala que "el Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, **independientemente de que el tratamiento tenga lugar en la Unión o no**"[2]. Por lo tanto, la normativa sería aplicable incluso fuera de los Estados Miembros, de modo que muchos países han tenido que revisar su legislación y adaptar su normativa al estándar de la Unión Europea (Albrecht 2016, 287).

2 La negrilla es de la autora.

Tal es el caso del Ecuador, que ha utilizado al RGPD como marco de referencia para generar su propia legislación nacional, y se ha adaptado a parámetros internacionales que le permitan calificarse como un país que garantice un nivel adecuado de protección de datos personales.

Al momento, el Proyecto de Ley Orgánica de Protección de Datos del Ecuador sigue siendo ampliamente impulsado para su discusión y aprobación; y se encuentra a cargo de la Comisión de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral de la Asamblea Nacional (PrensaEC 2020).

3. ¿Qué se entiende por dato personal y cuándo es objeto de protección?

Ahora bien, es preciso entender qué es un dato personal y cuáles son los parámetros que permiten determinar si cierta información es susceptible de protección o no.

El RGPD clasifica a los datos en cuatro categorías más una categoría especial, mientras que el Proyecto de Ley ecuatoriano los divide en seis tipos. Si bien las definiciones dadas por el RGPD y el Proyecto difieren en número, estas son muy cercanas en contenido y guardan las mismas características.

Art. 4. Reglamento General de Protección de Datos	Art. 5 Proyecto de Ley de Protección de Datos ecuatoriana
"Datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;	**"Datos personales:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente, en el presente o futuro. Los datos inocuos, metadatos o fragmentos de datos que identifiquen o hagan identificable al ser humano, forma parte de este concepto.
Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;	**Dato genético:** Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobra la fisiología o salud de un individuo; generalmente se analizan a través de las biológicas."
Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;	**Dato biométrico:** Dato personal único obtenido a partir de un tratamiento técnico-específico, relativo a las características físicas, fisiológicas o conductuales de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.

Art. 4. Reglamento General de Protección de Datos	Art. 5 Proyecto de Ley de Protección de Datos ecuatoriana
Art. 9 Categorías especiales de datos personales: Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.	**Datos sensibles:** Se consideran datos sensibles los relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos humanos o la dignidad e integridad de las personas. La Autoridad de Protección de Datos podrá determinar otras categorías de datos sensibles.
Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".	El Proyecto de Ley de Protección de Datos incluye a los datos relativos a la salud dentro de datos sensibles.
El RGPD no define los datos personales crediticios de manera específica, sin embargo, su concepto calza dentro de la definición de datos personales.	**Datos personales crediticios:** Datos que integran el comportamiento de personas naturales para analizar su capacidad de pago y financiera.
El RGPD no define los datos personales registrables de manera específica, sin embargo, su concepto calza dentro de la definición de datos personales.	**Datos personales registrables**: Datos personales que**,** conforme al ordenamiento jurídico**,** deben estar contenidos en Registros Públicos.

Del cuadro comparativo se observa que la legislación ecuatoriana agregó dos definiciones adicionales al RGPD, el dato crediticio y el dato registrable. Dichos conceptos nacieron como un reflejo de la realidad ecuatoriana, donde todos los ciudadanos mayores de edad poseen un perfil crediticio que es ampliamente manejado y consultado por instituciones bancarias y de crédito en el Ecuador. Esta información identifica directamente a su titular, razón por la cual es necesario que exista un control y supervisión respecto al acceso de los datos personales crediticios.

De igual forma, en el Ecuador existe una gran cantidad de información que posee el gobierno de sus ciudadanos, almacenada en registros públicos por mandato de ley. A este tipo de dato se lo conoce como dato personal registrable, el cual, a pesar de ser personal, puede ser procesado y almacenado siempre y cuando exista una disposición legal que así lo permita.

De todas estas definiciones se destacan ciertas características comunes, que son las que limitan el alcance de un dato personal y le permiten diferenciarse del resto de información que no cuenta con protección.

Persona natural*:* Para que un dato sea protegido, el generador de dicha información debe ser una persona

natural. Los datos que provienen de una persona jurídica no son materia de esta legislación.

El objetivo final de la protección de datos personales es proteger al individuo y limitar el uso de la información que emana de este. Esta información podría llegar a perjudicar particularmente su libertad y dignidad según sea su contenido. La Protección de Datos no pretende regular la información o datos todo tipo, al contrario, se circunscribe únicamente al ser humano (Voss, 2016).

Identificada o identificable de manera directa o indirecta: si la cantidad de información contenida en el dato o conjunto de datos permite identificar de manera directa o indirecta al titular de la información, por medios razonables, entonces se convierte en dato personal. Puede ser que el dato procesado no contenga el nombre del individuo o que su contenido corresponda a un dato aislado; mas, si permite identificar al individuo entonces es materia de protección (Sophos 2011).

Identificación sensible: Si los datos identifican a una persona de manera directa o indirecta, entonces son objeto de protección. Sin embargo, existen ciertos datos que podrían poner en riesgo o pueden atentar contra derechos humanos, la dignidad o integridad de las personas, y que pueden ser usados como base de discriminación. Por definición, estos datos no deben ser procesados, debido al alto riesgo que podría existir en caso de un mal uso. Sin embargo, el legislador contempla excepciones específicas en las que se autoriza su tratamiento.

Con estas definiciones, se entiende de mejor manera qué es un dato personal y se deja por sentado que no solamente los datos que evidentemente identifican a la persona, como el nombre, la edad o la fecha de nacimiento, pueden ser considerados como objeto de protección. Al contrario, existe una gran cantidad de información, como la geolocalización, afiliación política o historia clínica que, aun siendo anonimizadas, podrían asociarse al individuo con facilidad.

Con estas aclaraciones, nos preguntamos, ¿cuál es el verdadero riesgo de que estos datos sean procesados?, ¿realmente existe una afectación a los derechos del individuo, si se permite que terceros procesen su información personal?

Cada día es más frecuente que decisiones que afectan al individuo de manera directa sean tomadas en función de sus datos personales. El poder de decisión ya no recae en la deliberación de los seres humanos, sino que la decisión es tomada por Inteligencia Artificial. Máquinas y algoritmos son ahora los encargados de decidir si es que alguien puede acceder a un préstamo o ayuda financiera. Además, seleccionan de manera independiente a lo que un individuo puede acceder, ya sea en sus búsquedas o en sus redes sociales, de acuerdo con los datos personales recolectados por estos (Matheson 2017).

Estas decisiones, generalmente no son apelables y los algoritmos que las toman son prácticamente ininteligibles. El ciudadano común no tiene por qué tener un conocimiento avanzado sobre cómo funciona la inteligencia artificial o cómo se creó el algoritmo. Por este motivo existen cada vez más discusiones respecto de la necesidad de que tanto los algoritmos como sus resultados sean más transparentes y puedan ser corregidos en caso de un error. Al Estado le corresponde establecer regulaciones y derechos mínimos que deban ser respetados por quienes procesan los datos, para que exista un buen uso de estos y se proteja el bienestar de los individuos (Smith 2016).

4. ¿Qué se entiende por Inteligencia Artificial?

El concepto fue acuñado en 1956 por John McCarthy, y se desarrollaron tres acepciones, de acuerdo con el enfoque que se le dio al término. La primera acepción se enfocaba en el comportamiento de la máquina y se entendía a la Inteligencia Artificial como "programar computadoras para comportarse de una manera inteligente o "astuta". El enfoque cognitivo hacía referencia a "intentar recrear el proceso de razonamiento humano para entender la mente de mejor manera" y, finalmente, el enfoque robótico no se limitaba a la programación, sino que se refería a la acción de "construir la máquina" (Trappl 1985).

Una definición más actual señala a la Inteligencia Artificial como "la capacidad de las computadoras

o programas para operar de manera que se cree que imitan los procesos de pensamiento humano, como el razonamiento y el aprendizaje" (Saffiong 2020). Justamente esta capacidad es la que ha permitido que la máquina reemplace ciertas funciones que antes eran realizadas por el ser humano. El resultado ha sido que las decisiones sean mucho más precisas y tomadas en cuestión de segundos o fracciones de estos.

Gracias a la Inteligencia Artificial, las máquinas pueden a emular el pensamiento humano. Pero ¿cómo aprenden las computadoras? ¿cómo adquieren la capacidad de razonar?

Hay dos técnicas que forman parte de la Inteligencia Artificial y permiten "enseñarle a pensar" a la máquina, el Aprendizaje Automático o *Machine Learning* y el Aprendizaje Profundo o *Deep Learning*.

El Aprendizaje Automático es la capacidad que tiene la computadora de aprender nuevas habilidades sin ser programada continuamente. Consiste en un conjunto de técnicas y herramientas que permiten que la computadora interactúe activamente con datos acumulados, a través de un conjunto de algoritmos (Borgese, Newman y Norris 2019). Tales datos provienen generalmente del procesamiento de datos personales. El *Big Data* es utilizado para entrenar a los algoritmos que van a ser utilizados en el *Machine Learning*. Con este entrenamiento, el sistema puede razonar de manera independiente del aporte humano y puede por sí solo crear nuevos algoritmos (DATATILSYNET 2018).

Es decir, con el Aprendizaje Automático se le enseña a la computadora a "pensar" de cierta manera, gracias al uso de algoritmos. Los algoritmos fueron previamente entrenados para generar experiencia y enseñarle a la computadora cómo actuar. Una vez que la computadora ha aprendido a identificar los mismos patrones, tendencias y relación de datos, se le puede aportar nuevos datos para que por sí sola, ya sin entrenamiento ni ayuda humana, pueda actuar de la forma en la que se le enseñó, respecto de esos nuevos datos.

Por su parte, el Aprendizaje Profundo, que es una derivación del Aprendizaje Automático, permite a la computadora construir conceptos complejos a partir de conceptos simples. Consiste en capas anidadas de nodos interconectados. Después de cada nueva experiencia, aprende al reacomodar las conexiones entre los nodos (Banafa 2016). Estas capas procuran asimilarse al uso de redes neuronales, que crean conexiones y generan mayor conocimiento.

Para que la máquina "aprenda" necesita una exuberante cantidad de información que es recolectada a través del procesamiento de datos, incluidos los personales. La máquina los analiza y empieza a identificar patrones y similitudes. Estos patrones son los que se utilizan para enseñar a la máquina, en base a los cuales crea modelos que le permitirán actuar de tal o cual forma, si es que encuentra información similar a la previamente aprendida.

Por ejemplo, una aplicación de música recolecta grandes cantidades de información de sus usuarios, especialmente su selección musical. Esta información es procesada para identificar patrones de conducta similares y arroja como resultado un modelo de conducta identificable, con ellos se alimenta el algoritmo para que aprenda a distinguir dicho modelo. Una vez que la maquina ha aprendido a identificarlo, puede programarse para que, cuando identifique que el usuario concuerda con el patrón enseñado, le prediga que canción podría ser compatible con sus gustos, tras un análisis de su historial musical. Así, con la Inteligencia Artificial la máquina aprende de toda la información que recibe, se ajusta a la nueva información y responde casi de manera inmediata, sin que exista intervención humana (DATATILSYNET 2018).

Si bien estas innovaciones pueden facilitarnos la vida, ¿Hasta qué punto podemos aceptar que "recomendaciones" de este tipo puedan ser legítimas y consideradas de buena fe? ¿Qué evita que la información obtenida no sea direccionada por intereses propios de la empresa? ¿Cómo se puede estar seguro de que la recomendación a la que un individuo tiene acceso solo se apega a su gusto musical y no es el resultado de una sugerencia patrocinada sin su aprobación? Si algo tan intrascendente como las preferencias musicales de un individuo pueden ser analizadas y luego influenciadas por estos algoritmos, ¿Qué garantiza que no se utilice

el mismo tipo de comportamiento cuando se trate de elecciones presidenciales, cuando se solicite una visa o se aplique a asistencia social gubernamental?

Con el análisis anterior no se pretende desconectar a la sociedad de los avances tecnológicos. Sería descabellado pensar que puede detenerse el progreso de la tecnología y oponerse de manera absoluta al tratamiento de datos. Una actitud como esta solo retrasaría investigaciones y convertiría al individuo o a la sociedad respectiva en analfabetos digitales, y limitaría su acceso a posibles curas para enfermedades catastróficas como el cáncer, o a desarrollos tecnológicos tan increíbles como prótesis robóticas en interacción con el cuerpo. No obstante, tampoco se puede aceptar un tratamiento irresponsable o irrestricto de los datos. Resulta fundamental que exista una legislación que permita garantizar un apropiado tratamiento de datos personales, y que respete los derechos del ciudadano de conocer y decidir el fin que se va a dar a dicha información. Es indispensable que se reduzca al mínimo la cantidad de datos recolectados, y que se los guarde únicamente por el tiempo estrictamente necesario. Cada vez crece más la necesidad de llegar a un equilibrio, donde las empresas y el gobierno puedan utilizar los datos personales de manera responsable, de forma que respeten los derechos de sus usuarios.

CONCLUSIONES Y RECOMENDACIONES

El uso y alcance que se puede dar a los datos es todavía desconocido, por lo que es adecuado contar con una normativa que controle su procesamiento y que prevea futuros desmedros o abusos; tal y como lo han hecho un gran porcentaje de países, incluidos varios estados latinoamericanos (Leite 2016).

El Ecuador no puede ser ajeno a una realidad en la que ya está inmerso, de modo que se vuelve primordial adoptar medidas de protección que limiten la recolección, el procesamiento y el uso indiscriminado de datos personales. Resulta fundamental fomentar el uso responsable de datos personales. Se debe evitar que terceros utilicen esta información de forma inadecuada y que, como consecuencia, se desconozca el propósito que se les da. Es importante no olvidar que la información que almacena una computadora, muchas veces es sensible, y que debe ser procesada con absoluto cuidado, debido a las graves consecuencias que puede traer la divulgación de temas delicados como preferencias sexuales, religiosas, políticas, entre otras.

El Proyecto de Ley de Protección de Datos Personales es, sin lugar a dudas, una norma necesaria y fundamental que no solo permitirá alcanzar los estándares internacionales adecuados que facilitará recibir y transferir información de manera segura, sino que coadyuvará a estar a tono con los avances que la tecnología genera.

El contar con un marco jurídico adecuado no solo permitirá que el país cumpla con sus deberes internacionales, sino que otorgará seguridad jurídica a empresas que pretenden hacer negocios digitales en el país, y, así, promoverá un mayor desarrollo económico. Además, el incentivar que la Inteligencia Artificial sea utilizada de una manera transparente permitirá que los avances tecnológicos sean de amplio beneficio para el ser humano. Se ha demostrado que el hecho de enseñar a pensar a una máquina puede traer desarrollos y ventajas que antes eran inimaginables. Sin embargo, no podemos olvidar que los derechos del ciudadano están por sobre cualquier descubrimiento e interés particulares de las empresas.

Finalmente, hay que educar a la población respecto a la importancia de conservar y limitar el acceso a sus datos personales, dado que esta información define al ciudadano. Es necesario inculcar el valor de estos, para que el individuo tome decisiones en libertad, sin verse influenciado por recomendaciones o sugerencias que responden a intereses de terceros. El ciudadano debe poder ejercer su derecho de conocer el uso de sus datos y pedir su eliminación de forma absolutamente voluntaria.

BIBLIOGRAFÍA

Albrecht, Jan Philipp. 2016. "How the GDPR will change the World". *European Data Protection Law Review*, Volume 2 (2016), Issue 3, Pages 287 – 9. DOI https://doi.org/10.21552/EDPL/2016/3/4

Banafa A. 2016. "Qué es el aprendizaje profundo?". *OpenMind BBVA*, 7-VIII-2016. Consultado el 7-III-2020. https://www.bbvaopenmind.com/tecnologia/mundo-digital/que-es-el-aprendijaze-profundo/

Borgese A., Newman J. Y A. Norris. 2019. "AI, Machine Learning & Big Data 2019". *Australia, Global Legal Group*. 41. Acceso el 7-IV-2020. https://iapp.org/media/pdf/resource_center/ai_machinelearning_bigdata_2019_gli.pdf

DINARDAP. "Dinardap participó en la Mesa de Diálogo acerca del Órgano Rector en Acceso a la Información y Protección de Datos". Consultado el 25-IV-2020. https://www.dinardap.gob.ec/dinardap-participo-en-la-mesa-de-dialogo-acerca-del-organo-rector-en-acceso-a-la-informacion-y-proteccion-de-datos/

Directiva 95/46/EC del Parlamento Europeo y del Consejo de 24 de octubre de 1195 relativa a la "Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. Consultado el 30-III-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=EN

El Universo. "Lorena Naranjo: Protección de la información es un derecho", El Universo, 29-IV-2018. Consultado el 2-V-2020. https://www.eluniverso.com/noticias/2018/04/29/nota/6736137/proteccion-informacion-es-derecho

European Data Protection Supervisor. 2018. "The History of the General Data Protection Regulation". Consultado el 23-II-2020. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

GK. 2019. "La información de millones de ecuatorianos fue expuesta en línea". GK, 17-IX-2019. Consultado el 6-II-2020. https://gk.city/2019/09/16/filtran-datos-de-ecuatorianos/

Goddard, Michelle. 2017. "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact". *International Journal of Market Research* Vol. 59 Issue 6: 703-5. DOI: 10.2501/IJMR-2017-050

Internet World Stats. 2020. "Internet Growth Stadistics". Consultado el 24-III-2020. https://www.internetworldstats.com/emarketing.htm

Lavin, Marilyn. 2006. "Cookies: What do consumers know and what can they learn? *Journal of Targetting, Measurement and Analysis for Marketing* Vol 14, 4, 279-288. Consultado el 24-III-2020. https://link.springer.com/content/pdf/10.1057/palgrave.jt.5740188.pdf

Leite, R. 2016. "Data Protection Law in Latin América–an overview". *International Association of Privacy Professionals*, Consultado el 30-III-2020. file:///C:/Users/brivera/Documents/PERSONAL/Propuesta%20Articulo/Data%20protection%20laws%20in%20Latin%20America%20–%20an%20overview.pdf

Mathenson, Lee. 2017. "WP29 releases guidelines on profiling under the GDPR". *International Association of Privacy Professionals*, 18-X-2017. Consultado el 25-III-2020. https://iapp.org/news/a/wp29-releases-guidelines-on-profiling-under-the-gdpr/

Saffiong, K.. 2020. "Artificial Intelligence Applied Computer Science", CSI 3106 *African Virtual University*, 14. Consultado el 12/III/2020 .https://oer.avu.org/bitstream/handle/123456789/669/CSI%203106_EN%20Artificial%20Intelligence1.pdf?sequence=1&isAllowed=y

Servicio de Rentas Internas. "Facturación física, formatos". Consultado el 18-III-2020. https://www.sri.gob.ec/web/guest/facturacion-fisica

Silva, Vanessa. 2019. "La Policía arresta a gerente de Novaestrat, por supuesta filtración de datos de ecuatorianos", 16 de septiembre de 2019. Consultado el 7-II-2020. https://www.elcomercio.com/actualidad/policia-arresto-gerente-novaestrat-filtracion.html

Smith, Lauren. 2016. "Algorithmic transparency: Examining from within and without", 28-I-2016. Consultado el 25-II-2020. https://iapp.org/news/a/algorithmic-transparency-examining-from-within-and-without/

Sophos White Paper. 2011. "Protecting personally identifiable information: What data is at risk at what you can do about it". *Sophos White Paper*, octubre 2011. Consultado el 23-III-2020. https://www.sophos.com/es-es/medialibrary/PDFs/other/sophosprotectingPII.pdf

Trappl, R. 1985. "Impact of Artificial Intelligence". *Elsevier Science Publishers B.V*. 6-7. Consultado el 30-III-2020. http://pure.iiasa.ac.at/id/eprint/2758/1/XB-86-001.pdf#page=13

Unión Europea. 2020. "Tratados de la EU". Consultado el 23-IV-2020 https://europa.eu/european-union/law/treaties_es

Voss, W. Gregory. 2016. "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting". *The Business Lawyer*, 72(1), 221-234. doi:10.2307/26419118

Yeung, Jessie. 2019. "Almost entire population of Ecuador has data leaked". CNN WORLD, 17-IX-2019. Consultado el 16-II-2020. https://edition.cnn.com/2019/09/17/americas/ecuador-data-leak-intl-hnk-scli/index.html"

DATATILSYNET. 2018. "Artificial intelligence an privacy", The Norwegian Data Protection Authority, 6 -7. Consultado el 30-IV-2020. https://iapp.org/media/pdf/resource_center/ai-and-privacy.pdf