ENSAYO

Avance Tecnológico: Cambio Cultural y Vulnerabilidad de los Datos

Technological Advancement: A Cultural Process or Data Vulnerability

Recepción: 09-04-2021
Aceptación: 14-06-2021

MÁSTER OLDA ESTER BUSTILLOS ORTEGA

Máster en Auditoría de Sistemas Informáticos

Universidad Internacional de las Américas

San José, Costa Rica

Correo electrónico: olda.bustillos@gmail.com

Resumen

En los últimos tiempos, el uso acelerado de las redes sociales, las telecomunicaciones, el *Cloud*, *Big Data,* la Robótica *Cognitive*, el 5G, la Inteligencia Artificial y el Internet de las cosas, ha acelerado una transformación digital en las empresas que desencadena un cambio cultural. El presente artículo describe la importancia de la automatización como parte de un cambio cultural, los resultados de este cambio en empresas españolas y la consideración del escenario costarricense. Además, se identifica cuáles datos deben ser protegidos y se expone lo señalado en la "Ley de protección de la persona frente al tratamiento de sus datos personales", Ley No. 8968, del 05 de setiembre de 2011. El artículo contrapone el avance tecnológico, particularmente el empresarial con la vulnerabilidad de la información del individuo. Plantea interrogantes válidas relacionadas con el establecimiento de protocolos, controles y procedimientos de seguridad en el proceso de transformación digital.

Palabras clave: Privacidad, cambio cultural, cambio digital, avance tecnológico.

Abstract

In recent times, the accelerated use of social networks, telecommunications, the Cloud, Big Data, Cognitive Robotics, 5G, Artificial Intelligence and the Internet of things, has accelerated a digital transformation in companies that triggers a change cultural. This article describes the importance of automation as part of a cultural change, the results of this change in Spanish companies and considering the Costa Rican scenario. In addition, it identifies which data should be protected and the provisions of the Law on the protection of the person against the processing of personal data, Law No. 8968, of September 5, 2011 are exposed. The article opposes technological advance, particularly the business one with the vulnerability of the individual's information. It raises valid questions related to the establishment of security protocols, controls and procedures in the digital transformation process.

Key Words: Privacy, cultural change, digital change, technological advancement.

Introducción

Cada vez con mayor frecuencia, las empresas recurren al empleo de tecnologías que les permiten innovar y digitalizar sus procesos y estrategias. Sin embargo, este escenario de cambio exige contar con trabajadores que cuenten con capacidades digitales.

En este ensayo se desea identificar la importancia de la automatización en las empresas costarricenses como parte de un cambio cultural. Para esto, se mencionan las principales herramientas tecnológicas que pueden participar en un cambio digital y cultural, analizado desde una perspectiva mundial, para luego revisar el cambio en Costa Rica.

Asimismo, se define el concepto de privacidad de la información desde la perspectiva técnica. Se describe qué información debe protegerse y se mencionan las normativas existentes para el manejo de datos y privacidad de la información. Por último, se compara el avance tecnológico empresarial costarricense en contraposición con la vulnerabilidad de la información.

Este ensayo abordará, desde una visión conceptual, algunas temáticas que permiten la comprensión del fenómeno en estudio, por ejemplo, la importancia de la automatización, o de la privacidad de la información. Asimismo, se mencionan algunas normativas existentes para el manejo de los datos y la privacidad de la información, el proceso de automatización, el cambio cultural digital y la vulnerabilidad de los datos.

Se establecen tres objetivos de estudio. Primero, se pretende identificar la importancia de la automatización como parte de un cambio cultural en las empresas costarricenses, entendido desde el cambio digital mundial hasta la realidad nacional. Además, se

menciona el cambio digital mundial y luego se describe el cambio digital en Costa Rica.

La segunda unidad abarca la privacidad de la información desde la perspectiva técnica. Por último, se contraponen el avance tecnológico empresarial y la vulnerabilidad de la información que se solicita, que se procesa y que se comparte en las entidades en donde las personas gestionan sus transacciones.

La línea teórica que se emplea se realiza desde el enfoque señalado principalmente por Terrón (2019). Se toma en cuenta la consideración respecto de un cambio cultural y no solamente de un cambio tecnológico, cuando se menciona la importancia de la transformación digital (Kirby, 2018, citado por Terrón, 2019). En cuanto al tipo de investigación, el enfoque es cuantitativo, pues se requieren los datos obtenidos a nivel mundial y nacional, sobre el uso de la tecnología, para el análisis respectivo.

En los dos últimos años se ha vislumbrado un acelerado avance tecnológico en cuanto a los medios, plataformas y herramientas de automatización que se pueden utilizar para hacer eficientes los servicios empresariales. Junto con este panorama, existe la preocupación de las compañías por sobrevivir en el mercado, ya que la rápida incursión de la tecnología y de las herramientas digitales ha traído un acelerado cambio en la cultura. Por un lado, se requiere de la tecnología para actualizarse y permanecer compitiendo en el mercado. Por otro, los requerimientos solicitados a los empleados por las compañías resultan más exigentes que el perfil tradicional, pues ahora se demanda conocimiento y experiencia en temas digitales.

Este perfil presupone que en esta nueva normalidad (post-pandemia COVID-19), el candidato a solicitar empleo debe agregar a su hoja de vida una lista de competencias tecnológicas. En este sentido, como indica Terrón (2019), la contratación de trabajadores con capacidades tecnológicas inspira a la compañía a promover una mentalidad digital, a adaptarse a los cambios de la sociedad y al mercado en el que compite.

Digitalizar la actividad empresarial es un cambio cultural, y no solamente se habla de tecnología, sino también de cambio cultural (Ibañez, 2018, citado por Terrón, 2019). Este proceso de cambio no siempre resulta sencillo de implementar en las entidades, particularmente porque la inversión para digitalizar puede ser muy elevada. La selección de las herramientas y de los elementos tecnológicos que se deben considerar en el cambio digital empresarial deben ir acordes a la naturaleza del negocio. Dentro de las herramientas que se toman en cuenta para este cambio cultural, principalmente se encuentran seis: *Cloud, Big Data*, Robótica *Cognitive*, el 5G, la Inteligencia Artificial y el Internet de las cosas.

Las herramientas tecnológicas permiten procesar los datos de las personas y

la empresa decide qué tipo de datos se debe resguardar y de qué forma. Por otro lado, la persona dueña de la información tiene derecho a sentirse recelosa al brindar datos personales, ya que el robo o uso indebido de esta información puede atentar contra su seguridad. Las normas y leyes establecidas para el resguardo de la data tienen un papel importante, particularmente si se considera que la tecnología permite manejar de manera más eficiente los datos para minimizar el tiempo de respuesta y agilizar la toma de decisiones.

El avance en los procesos de la digitalización en otros países obliga al nuestro a tener que estar alineado para hacer frente a los procesos de intercambio, de producción y de los costes, entre otros.

Desarrollo

El rápido avance tecnológico y el acelerado ingreso de plataformas que permiten la comunicación, obliga a pensar que quienes no se actualizan tecnológicamente, quedarán rezagados en el mercado. La constante competencia empresarial por determinar quién llega primero al cliente, se vuelve una carrera digital, en donde las compañías compiten día a día por obtener las mejores herramientas automatizadas que les permitan transformar rápida y correctamente la información.

Se trata de un desafío, no involucra solamente la implementación de la tecnología, sino que se trata de una nueva cultura que obliga al empleado a tener un compromiso mediante el cual debe desarrollar nuevas habilidades. Por otro lado, debe darse un cambio en la cultura corporativa de las organizaciones (Remedio, Rosado y Lacasa, 2020).

En este proceso de digitalización intervienen herramientas tecnológicas que facilitan el cambio. Huerta (2018, citado por Terrón, 2019) señala seis principales tendencias: *Cloud, Big Data*, Robótica *Cognitive*, el 5G, la Inteligencia Artificial y el Internet de las cosas.

En el caso del *cloud computing*, de acuerdo con Del Miglio y Jansen (2018, citados por Terrón, 2019), permite a sus usuarios ahorrar en almacenamiento de información, en *software* y en movilidad; además, puede optimizar las tareas y proporcionar la seguridad necesaria para la protección de datos.

Esta tecnología dota a los sistemas de flexibilidad y escalabilidad, capacidades que posibilitan la optimización del trabajo, la rápida adaptación según las circunstancias y la resolución de problemas gracias a su eficaz habilidad de respuesta (Bommadevara, 2018, citado por Terrón, 2019).

El *big data* representa la recolección de gran cantidad y variedad de datos e información en rápido movimiento, que se procesan y analizan para generar valor. Cuenta con tres características fundamentales, el volumen, la variedad y la velocidad (Souza y Trollinger, 2013, citado por Terrón,

2019). Estas propiedades son claves para las empresas puesto que les permiten entender mejor las necesidades de los clientes y adaptarles sus productos, es por esto que permite a las compañías un apoyo básico para su competencia y crecimiento (Chui y Manyika, 2011, citados por Terrón, 2019).

La robótica *cognitive* es otra de las herramientas utilizadas para la automatización. Se compone de un conjunto de diversos subsistemas de inteligencia artificial, como el *machine learning*, que permite el aprendizaje automático utilizando las matemáticas y la estadística para mejorar el rendimiento, la eficacia y el análisis de datos de los sistemas informáticos. El objetivo último de esta tecnología es la creación de robots que puedan tomar decisiones en situaciones críticas y mejorar los procesos (Huerta, 2018, citado por Terrón, 2019).

El 5G corresponde a la quinta generación de tecnología inalámbrica, basada en una velocidad sorprendentemente más rápida y una latencia (tiempo de transmisión de un objeto a través de la red) muchísimo más baja, un consumo menor de energía y tiene la capacidad de transportar varias conexiones de manera simultánea (Meakin, Shea, Wong y Zikry, 2019, citados por Terrón 2019). Se enfoca particularmente en el uso de cuatro elementos claves: banda ancha móvil mejorada, que proporciona una alta definición y realidad virtual; internet de las cosas, que permite la simultaneidad de conexiones; control de la misión crítica, que posibilita un tiempo de transmisión aproximado de un milisegundo; y, por último, acceso inalámbrico fijo, que funcionaría como sustituto de la banda ancha por cable (Collins, Das, Ménard y Patel, 2018, citados por Terrón, 2019).

Otro de los apoyos tecnológicos para realizar el proceso de automatización, es la inteligencia artificial (IA), la cual consiste en un conjunto de tecnologías que posibilitan a los computadores imitar las funciones cognitivas humanas. Esta capacidad la adquieren gracias al uso de algoritmos que evolucionan y mejoran con la práctica, generando un aprendizaje automático (Román, 2016, citado por Terrón, 2019).

Las aplicaciones de la IA como el reconocimiento de voz, la visión y la automatización de procesos, están empezando a ser muy comúnmente utilizadas por las compañías debido a que fomentan una mejor experiencia de sus clientes, impulsan una reducción de costos y simplifican los procesos (Dullweber, Moreau y Hatheral, 2018, citados por Terrón, 2019).

El Internet de las cosas es otra herramienta que permite la interconexión y la interacción de lo digital y el mundo físico, en el que se puede integrar "cosas" físicas a las redes de información a través de infraestructuras de internet existentes y emergentes; es decir, es una plataforma para conectar personas, objetos, y entornos para informar y permitir la visibilidad, el compromiso y la innovación (Herrera, 2018, citado por Terrón, 2019).

El uso y la aplicación de estas herramientas no es suficiente, el proceso de cambio tecnológico no se supedita a estas. También se debe considerar que el proceso lleva a un cambio cultural, lo que implica pensar en contar con colaboradores con algún nivel de preparación en herramientas tecnológicas como las mencionadas. Estas capacidades digitales que debería adoptar un empleado contribuyen a que la empresa incursione de forma rápida en el proceso de cambio tecnológico.

Al respecto, Pedreño (2017, mencionado por Terrón, 2019) indica que la digitalización no solamente está ligada a la tecnología, sino a la inversión en talento y a un cambio cultural empresarial y social. Por lo tanto, la digitalización empresarial también incluye la contratación de colaboradores con mentalidad digital que puedan adaptarse a los cambios de la sociedad y del mercado en el que compite.

Un ejemplo de este cambio empresarial lo muestra España. Klynveld Peat Marwick Goerdeler (KPMG), con la cooperación de la Confederación Española de Organizaciones Empresariales (CEOE), realiza anualmente una previsión de las perspectivas empresariales, en la cual reúne las respuestas dadas por directivos de varias empresas españolas (KPMG, Informe, 2019).

Tal y como se aprecia en la figura 1, los empresarios españoles opinan que la digitalización ha influido, por encima de todo, en la relación con los clientes (56%), en la reducción de costes y en la mejora de la eficiencia (51%), en los procesos de producción (40%) y en la mejora de la gestión de riesgos (18%), pero un 13% de los encuestados afirmaron que aún no habían comenzado con el proceso de transformación digital (Rivals y Uría, 2019).

Figura 1. Influencia de la transformación digital en las empresas españolas, 2019.
Fuente: Rivals y Uría, 2019.

Los datos anteriores muestran cómo un alto porcentaje de las empresas españolas fue impactado por el uso de la digitalización a nivel de clientes, sin descartar la mejora que se obtuvo en la eficiencia de los procesos productivos. Esto refleja que la automatización y la digitalización empresarial están tomando cada vez más fuerza, y que este cambio permite mejorar la condición de las empresas a nivel competitivo.

Asimismo, de acuerdo con los estudios realizados por Katz, Jung y Callorda (2020) sobre la adopción del internet en América Latina, se obtiene que el promedio ponderado para la región indica el progreso que ha realizado este sector en los últimos años, tal y como puede verse en la tabla 1.

Tabla 1.

Penetración de internet en América Latina (2018-2020).

	2018	2019	2020
Argentina	77,78 %	81,42 %	85,24 %
Barbados	84,03 %	86,37 %	88,77 %
Bolivia	48,22 %	53,04 %	58,34 %
Brasil	74,22 %	81,64 %	89,80 %
Chile	82,33 %	82,33 %	82,33 %
Colombia	66,68 %	71,40 %	76,47 %
Costa Rica	74,09 %	76,88 %	79,79 %
República Dominicana	74,82 %	82,31 %	90,54 %
Ecuador	60,67 %	64,27 %	68,09 %
El Salvador	37,20 %	40,92 %	45,02 %
Guatemala	71,50 %	78,65 %	86,52 %
Honduras	34,06 %	36,60 %	39,33 %
Jamaica	60,58 %	66,64 %	73,30 %
México	65,77 %	67,75 %	69,79 %
Panamá	62,01 %	66,45 %	71,20 %
Paraguay	64,99 %	69,16 %	73,60 %
Perú	52,54 %	56,65 %	61,08 %
Trinidad & Tobago	81,58 %	86,06 %	90,79 %
Uruguay	70,21 %	72,20 %	74,24 %
Venezuela	79,20 %	87,12 %	95,83 %
América Latina (promedio ponderado)	68,66 %	73,52 %	78,78%
OCDE (promedio ponderado)	83,93 %	86,07 %	88,33 %

Fuente: Unión Internacional de Telecomunicaciones; análisis Telecom Advisory Services, 2020.

Como se aprecia en la Tabla 1, la penetración del internet en Costa Rica alcanza casi el 80% para el año 2020. Cada vez más, las empresas e instituciones migran a plataformas y utilizan herramientas que les permiten la digitalización de la cadena de aprovisionamiento, la digitalización de los canales de distribución y la transformación de la fuerza de trabajo. El uso de plataformas como Amazon permite migrar los procesos y servicios a la nube y lograr más eficiencia en el servicio al cliente.

Paralelamente a esta transformación, los empleados deben adoptar un compromiso ante el cambio tecnológico, la innovación y la adaptabilidad, considerando tener un cambio en el perfil y nuevas habilidades. Al respecto, la práctica de digitalizar implica un cambio que transforma a la misma empresa y a los profesionales, ya que no se trata de un desafío

para implementar solamente la tecnología, sino de una nueva cultura, de un renovado compromiso de la empresa y el empleado para desarrollar nuevas habilidades (Chiapello, 2019, citado por Remedio, Rosado y Lacasa, 2020).

Esta transformación digital establece la necesidad de meditar en la privacidad de los datos que se ponen en riesgo a medida que se avanza en la digitalización y automatización de los procesos del negocio. El riesgo existe por ambos lados, sea por parte de los empleados o para los clientes. El llenado de formularios, solicitudes y documentos en donde se indican números de cédula, fechas de nacimiento y otra información personal delicada, son una fotografía de la persona que se debe custodiar con especial cuidado.

La privacidad de la información se relaciona con el derecho legal que tiene un individuo de custodiar sus datos de modo que no se vulneren. Existen tres tipos básicos de privacidad: la privacidad física, entendida como la libertad para que no haya intromisiones en lo físico de las personas, posesiones y espacio; la segunda es la información privada, definida como la información personal recolectada en formatos digitales; la tercera se refiere a la privacidad organizacional, que se concibe como aquella que tienen las agencias de gobierno, compañías y demás organizaciones para no revelar actividades y secretos a personas ajenas (Craig, Terence y Ludloff, 2011, citados por Meraz, 2018).

Esta data debe ser resguardada de manera adecuada; sin embargo, surgen algunas interrogantes, ¿se utilizan los dispositivos y plataformas con la suficiente seguridad para el procesamiento y resguardo de la información de una persona? El trámite de información personal a través de redes sociales, ¿representa un riesgo de ser "hackeada"? ¿Los procesos automatizados de las empresas cuentan con protocolos de seguridad rigurosos para custodiar la data?

Desde una perspectiva jurídica, el manejo, uso y almacenamiento de la información necesitan la certeza legal que permita a sus titulares (dueños de la información) confiar en el cuidado de esta, pero esa certeza es también importante para sus dueños, quienes son los poseedores de la información respecto de su uso y resguardo (Meraz, 2018).

La información que se brinda a las diferentes organizaciones va desde la solicitud de un servicio hasta la compra o venta de algún artículo e incluye información como el nombre, domicilio, teléfono, edad, sexo, escolaridad, estado civil, religión, filiación política, ocupación, amigos, familia, cuentas bancarias, pasatiempos, estado de salud, entre otros. Esta documentación tan sensible es accedida por cualquiera y representa una auténtica radiografía personal de un individuo, y se puede encontrar en las bases de datos electrónicas de los diferentes negocios y organizaciones que la hayan solicitado y puede ser vista por otros (Nolan, 2014, citado

por Meraz, 2018).

En la mayoría de los casos, se facilita realizar la captura de datos personales a través de páginas web. Estos medios resultan atractivos y eficientes para el cliente, pues se tienen disponibles a través de aplicaciones, sea en un ordenador o en un móvil. Quienes recopilan esta data deben ser responsables de protegerla, y su regulación jurídica es propia a la de protección de datos, en particular los que se almacenan en bases de datos digitales. No se debe perder de vista que esta información hace referencias de identidad muy personales y su robo, o bien, su uso indebido, atenta y perjudica directamente a su dueño, no solo de forma personal sino social, en el entorno que lo rodea, ya que incluye datos financieros, religiosos, estados de salud, entre otros (Meraz, 2018).

La protección de datos en Costa Rica se encuentra regulada bajo la Ley 8968, "Protección de la persona frente al tratamiento de sus datos", y su fin es garantizar a cualquier persona que sus derechos fundamentales deben ser respetados. La ley indica que el titular debe otorgar su consentimiento para que terceros puedan tratar sus datos personales, de esta forma, cada persona decide a quién darle sus datos. Además, en Costa Rica existe la Agencia de Protección de Datos de los Habitantes (PRODHAB), adscrita al Ministerio de Justicia y Paz. Esta entidad es la encargada de fiscalizar y regular las bases de datos de nuestro país, pudiendo acudir a ella en caso de anomalías relacionadas con datos personales.

A pesar de que existen leyes que protegen a los titulares de los datos cuando estos son manipulados de forma incorrecta, también se debe tener cuidado con la información que se comparte en redes sociales, plataformas y otros medios.

Con la realidad señalada, se puede inferir que el avance de la tecnología no se puede detener. Tampoco se puede paralizar el crecimiento empresarial, el de las ciudades y del mundo. La aparición de plataformas cada vez más sofisticadas, el alto crecimiento en el uso del internet y redes sociales para compartir información, nos llevan a algunos cuestionamientos, ¿la tecnología genera elementos de riesgo para exponer información sensible del ciudadano? ¿A mayor tecnología, mayor riesgo de vulnerar la información personal?

Las empresas que solicitan datos están reguladas por las leyes. En Costa Rica, una de estas normativas es la Ley 8968 de protección de la persona frente al tratamiento de sus datos personales, del 05 de setiembre de 2011. El artículo 5 de esta ley señala, sobre el principio de consentimiento informado, la obligación que se tiene de informar. Cuando son datos de carácter personal, es necesario que se informe previamente a las personas titulares o representantes de modo, expreso, y sobre el otorgamiento del consentimiento, el cual indica que quien recopile datos personales deberá tener el consentimiento expreso del

titular de los datos o de su representante.

En el artículo 6 de la mencionada ley, que versa sobre el principio de calidad de la información, se hace referencia a los datos que son tratados de forma automatizada o manual; que son recolectados, almacenados, o empleados con carácter personal, y menciona que deberán ser actuales, veraces, exactos y adecuados al fin para el que fueron recolectados, por lo que se debe garantizar su seguridad. Asimismo, en el artículo 7 se garantiza el derecho de toda persona sobre los datos personales, su rectificación o supresión, y a que pueda consentir si se los proporciona a terceros o no, y el responsable de la base de datos en donde se encuentren debe cumplir lo solicitado, gratuitamente (Ley No. 8968, Ley de protección de la persona frente al tratamiento de sus datos personales, 2011, citada por Rivera, 2019).

El usuario es dueño de sus datos sensibles y puede negarse a compartirlos o cederlos. No obstante, si pensamos que no se puede detener la culturización tecnológica, entonces pareciera que debemos detenernos a meditar que la digitalización y el avance empresarial no se remiten a la existencia de medios electrónicos y tecnificados para manipular la información, sino que también incluyen medios físicos y de transferencia, apropiados para resguardarla. Al mismo tiempo que se tecnifican las empresas, las ciudades, el país y el mundo deberían utilizar protocolos de seguridad efectivos que combatan las intenciones maliciosas de quienes roban información sensible. Es primordial actuar de forma preventiva y no esperar a que se produzcan los ciberataques.

Estos protocolos de seguridad están relacionados a procedimientos, políticas y normativas institucionales que, actuando conjuntamente con la tecnología, permiten blindar los datos y la información que se resguarda. Cuando se interactúa con tecnología, es vital contar con auditorías informáticas, estas permiten validar la seguridad informática en todas sus aristas, sea de *hardware*, *software*, física, procedimental, entre otros. Sea cual fuere el grado de adopción de la tecnología, particularmente el *cloud*, se debe pensar en la seguridad a nivel de las comunicaciones, ya que la mayoría de los servicios están alojados en máquinas remotas a las cuales se llega atravesando redes de terceros (Roa, 2013).

Debemos seguir viviendo en este escenario social conforme avance la tecnología, teniendo presente que nuestra información y datos sensibles quedan bajo nuestra responsabilidad, y nosotros decidimos con quién los compartimos.

Conclusiones

La tecnología ha sido un elemento fundamental en la concepción y la implementación de iniciativas empresariales exitosas. Sin duda, la automatización de la cadena de valor en una compañía permite un tiempo de respuesta menor en los procesos, minimiza costos, aumenta la productividad,

genera clientela, y posiciona en el mercado.

Esta automatización conlleva a un cambio cultural si se considera que quienes operan los equipos, gestionan los procesos y toman las decisiones, deben hacerlo bajo un perfil que permita interactuar con la tecnología. En otras palabras, al mismo tiempo que se automatiza la empresa, también debe automatizarse el perfil profesional. Mientras más relación con la tecnología tenga el puesto por desempeñar, más preparación técnica debería tener el empleado. Esta relación entre preparación y cambio tecnológico permite visualizar el cambio social que también se genera, pues el individuo es parte de una sociedad y como tal, su entorno se ve afectado.

Las herramientas y plataformas tecnológicas actuales, particularmente el *cloud*, son aliados fuertes para las empresas. No obstante, no es suficiente automatizar la empresa, se debe trabajar conjuntamente para la aplicación de auditorías informáticas que permitan validar los controles y protocolos de seguridad en el *software*, *hardware*, aspectos físicos, procesos, entre otros.

Por otro lado, se debe considerar que el conocimiento técnico no queda solamente a lo interno de la compañía, sino que se expande a su alrededor cuando se considera que el día a día de las personas gira en torno a una cantidad de actividades que demandan ceder información personal a quienes la soliciten. Estos datos personales están ligados a una credencial de identificación pues tienen que ver con creencias religiosas, partidos políticos, estados civiles, datos de salud, nombre, cédula, direcciones, teléfonos, entre otros.

A pesar de que se cuenta con leyes que asignan castigos a quienes vulneran la información confidencial de una persona, podría pensarse que, ¿acaso se actúa a *posteriori*? Es decir, ya el daño está hecho, ya se ha "hackeado" información, ya se han utilizado los datos en perjuicio del individuo.

Corresponde a la persona la responsabilidad de administrar y gestionar su propia información y también decidir qué información comparte y cuál se reserva.

Referencias

Katz, R., Jung, F. y Callorda, F. (2020). El estado de la digitalización de América Latina frente a la pandemia del COVID-19. *Scioteca.* https://scioteca.caf.com/handle/123456789/1540

Ley No. 8968. Ley de protección de la persona frente al tratamiento de sus datos personales. 05 de setiembre de 2011. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

Meraz, A. (2018). Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales. *Revista IUS*, *12*(41). http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100293&lang=en

Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal, 10 de julio de 2012.

Remedio, Z., Rosado, M. y Lacasa, P. (2020). Las Prácticas de Digitalización Implementadas en las Empresas desde los Departamentos de Recursos Humanos: Análisis Crítico del Discurso. *Prisma Social: revista de investigación social*, (32). https://dialnet.unirioja.es/servlet/articulo?codigo=7742143

Rivera, V. (2019). Realidad sobre la Privacidad de los Datos Personales en Costa Rica. *E-Ciencias de la información*, *9*(2). https://www.scielo.sa.cr/pdf/eci/v9n2/1659-4142-eci-9-02-68.pdf

Roa, J. (2013). *Seguridad Informática*. México: McGraw-Hill.

Rodríguez, R. (2019). La privacidad en las ciudades inteligentes. *CES Derecho*, *10*(2). http://dx.doi.org/10.21615/cesder.10.2.7

Terrón, P. (2019). *Digitalización, de opción a obligación*. Madrid: Universidad Pontificia Comillas. https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/27896/TFG%20-%20TerroIn%20GarciIa%2c%20Paula.pdf?sequence=1&isAllowed=y