

Tratamiento de datos personales y acceso a la información. Visiones a partir de la academia

*Access to information and processing
of personal data. Visions from the academy*

Yadira Rosario Nieves-Lahaba

Universidad Autónoma de Nuevo León, México
yadira.nieveslahaba@gmail.com
<https://orcid.org/0000-0001-8465-4869>

Gloria Ponjuan-Dante

Universidad de la Habana, Cuba
gponjuan@infomed.sld.cu
<https://orcid.org/0000-0003-2063-0934>

Recibido: 09-03-2021 **Revisado:** 08-05-2021 **Aceptado:** 16-06-2021 **Publicado:** 01-09-2021

Resumen

Hoy en día, el acceso y uso de datos ocupa un lugar destacado en cualquier actividad humana. Cada vez hay más atención no solo a su uso, sino también a la necesidad de estudiar cómo se obtienen, cómo se comparten, cómo se protegen, tanto en el plano personal como en lo institucional, ya que la comunicación social se magnifica y ocupa un altísimo lugar en el comportamiento humano empleando no solo lo presencial. Este trabajo sintetiza una investigación realizada en la Facultad de Filosofía y Letras de la Universidad Autónoma de Nuevo León en México con el objetivo de describir el comportamiento de una muestra de más de 300 estudiantes en relación con el tratamiento de los datos personales destacando las preocupaciones más significativas que tienen sobre estos temas. Se presenta el análisis de los resultados de la encuesta, técnica de investigación empleada. El principal resultado fue que los estudiantes conceden gran importancia a tener derechos sobre los datos personales y en especial a poder oponerse o cancelar que estos se obtengan o se usen, pero por otra parte no son muy cuidadosos con la privacidad de estos pues comparten en su mayoría datos personales con amigos y conocidos. Se concluye que este tipo de comportamiento hacia el tratamiento de los datos es poco congruente, lo que advierte de la necesidad de un mejor y mayor conocimiento sobre el tratamiento de los datos personales.

Palabras clave

Datos abiertos, datos personales, procesamiento de datos, privacidad de datos, seguridad de los datos, normatividad de datos.

Forma sugerida de citar: Nieves-Lahaba, Y., & Ponjuan-Dante, G. (2021). Tratamiento de datos personales y acceso a la información. Visiones a partir de la academia. *Universitas-XXI*, 35, pp. 167-185. <https://doi.org/10.17163/uni.n35.2021.08>

Abstract

Currently, the access and use of data rank high in any human activity. People, organizations, and countries pay attention not only to their use, but also to the need of studying how they are obtained, shared, protected, both at the personal and institutional level as social communication is magnified and occupies a higher place in the human behavior, not only face-to-face but also in social networks. This article summarizes a research accomplished in the academic environment of a Mexican university aiming to reflect the behavior of a sample of over 300 students relating to the access to information and data management, highlighting the most significant concerns they have on these topics. An analysis of the results of the survey and research technique used is presented. The main result obtained was that the students granted great importance to have rights on the personal data and, specially, to be able to oppose or annul that these can be obtained or used. On the other hand, they are not very cautious with the privacy of the data as most of them share personal information with friends and acquaintances. This means that this type of behavior towards data management is little congruent

Keywords

Open data, personal data, data processing, data privacy, data security, data regulations.

Introducción

En la actualidad se desarrollan diferentes enfoques que permiten fortalecer la acción individual de diferentes segmentos de la sociedad en lo relativo al acceso y uso de datos e información, en forma tal de poder elevar y perfeccionar el comportamiento de diferentes colectivos. La literatura especializada reporta aisladas experiencias que abordan el tratamiento de los datos con diferentes alcances, desarrolladas principalmente en contextos educacionales, a fin de conocer comportamientos, proponer escenarios y mecanismos que faciliten la captación, almacenamiento y difusión de datos e informaciones que se emplean en diferentes momentos de la actividad individual (Barreau, 1995, 2008, 2009; Cotino et al., 2020). Ferran-Ferrer y Pérez-Montoro (2009) investigaron el comportamiento individual en una muestra de estudiantes en una universidad de Barcelona. En el estudio se tuvo en cuenta variables como: acceso a la información (necesidades/fuentes/formas de acceso-suscripciones.), gestión de la información (tratamiento

to e integración/recuperación y preservación/criterios de selección/criterios de satisfacción), usos de la información (creación/integración/ canales de comunicación/ compartimiento de información/formas de trabajo colaborativas), competencias informacionales (experto/no experto), entre otras. Los avances que se reportan en las ciencias sociales, sitúan en un lugar destacado todo lo relativo a la gestión de datos personales. La sociedad contemporánea da un lugar prioritario a la comunicación en todas sus manifestaciones, con especial atención a la comunicación en ambientes digitales en pos de facilitar diferentes actividades y responsabilidades de la comunidad y donde el tratamiento de los datos personales es de gran interés para todos (Arellano & Ochoa, 2013). Sin embargo, el estudio de la percepción del estudiantado universitario sobre el tratamiento de datos personales no ha sido abordado ampliamente de forma tal que permita explorar datos cualitativos o cuantitativos para advertir comportamientos generalizados por lo que este estudio contribuye a la formación de ideas en torno al tema. Mucho debe avanzarse aun en términos de que los medios tecnológicos cuenten con elementos que contribuyan al respeto de estos derechos y que faciliten un flujo de datos e informaciones de calidad. Es la era de la verdad, y es una obligación que los mensajes y datos que se transmiten por diversos canales sean portadores de información y no de desinformación.

La gestión de los datos y la seguridad de la información

La autodeterminación informativa es un derecho esencial a tener en cuenta en el diseño y operación de los sistemas de información, ya sean automatizados o no, por lo que el tratamiento de los datos no solo debe cumplir con las normativas, sino que debe contribuir a la alfabetización de los ciudadanos en esta materia, de manera que se informe sobre los derechos del titular del dato y al mismo tiempo se mantenga el principio de calidad de los datos (Sánchez-Castañeda & Márquez, 2017; Hernández & Zavala, 2018; Garriga, 2009; Porcelli, 2019; Domínguez, 2016).

Hace algunas décadas, Páez (1992) expresó: “en la antigüedad, el hombre occidental quería ser sabio; luego el hombre moderno quiso ser conocedor; el hombre contemporáneo parece contentarse con estar informado (y posiblemente el hombre futuro no esté interesado en otra cosa que en tener datos)” (p. 10).

Los datos nos permiten representar hechos, conceptos, dimensiones y forman parte de nuestro lenguaje, de nuestra gestión, posibilitan además establecer relaciones para determinar comportamientos en diferentes procesos. A partir de los datos se genera, distribuye y se utiliza información.

En los últimos años se han presentado proyectos y experiencias en relación con el manejo de los datos, no solo para la investigación, sino para cualquier actividad personal. El volumen de datos electrónicos y su intercambio por diferentes vías, aumentan con rapidez. Siendo un aspecto tan vital para diferentes facetas de la vida ciudadana, es de esperar que en torno a ella se desarrollen estudios y se generen políticas que conlleven a su protección puesto que un dato erróneo, al multiplicarse, puede dar lugar a una falsedad, y de ella sigue creciendo y multiplicándose aplicaciones inadecuadas. Las políticas públicas en relación con la gestión de datos han ido surgiendo, aunque lamentablemente siguen presentándose ejemplos de incumplimiento y de mal manejo, intencional o no, de los datos personales (Ortega, 2015).

El ejercicio de los derechos sobre datos personales, en materia legal, ha sido objeto de observación desde distintas aristas y en distintas épocas (González, 2019; Requena & Sánchez, 2014; Araujo, 2016). Paulatinamente se ha modificado sus alcances y significación para evidenciar políticas que se esfuerzan por el robustecimiento de las garantías colectivas (Aparicio & Pastrana; 2017, Hernández, 2006). En México, el artículo 6 de la constitución mexicana ha sido modificado en distintos momentos, actualmente no solo expresa el derecho a la libre expresión, sino también el derecho al acceso a la información. El artículo 16, modificado el primero de junio de 2009, es específico cuando menciona que todas las personas tienen derechos de proteger sus datos personales. Este derecho está ratificado y asentado (Feregrino, 2012), en el cuerpo normativo de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (Cámara de diputados del H. Congreso de la Unión, 2010) aprobada por el Congreso de la Unión en 2010, a través de los derechos ARCO que tienen que ver con el acceso, rectificación o corrección de los datos personales que se obtienen de los individuos, así como el derecho de oponerse a que estos sean recabados (Derechos ARCO: Acceso, Rectificación, Cancelación u Oposición).

Además de estos derechos en el reglamento adjunto a esta ley (Cámara de diputados del H. Congreso de la Unión, 2011) se abordan ocho principios rectores para la protección de datos personales, estos son: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y, responsabilidad.

Al interrelacionar estos principios con el entorno del fenómeno informacional, Ozmen-Ertekin y Ozbay (2012) presentan su visión acerca de la calidad de los datos, a través de las dimensiones accesibilidad y seguridad. Consideran la accesibilidad, para referirse a la facilidad y amplitud del acceso a la información y la seguridad con respecto a si existe protección o no contra un acceso no autorizado. Las dimensiones de calidad se refieren al conjunto de atributos de calidad al que reaccionan en forma consistente los consumidores. (Wang et al., 2001; Portilla-Romero, 2017). Otros elementos más esclarecedores los aporta Páez (1992) cuando ofrece una serie de parámetros para evaluar la calidad de los datos, estos son: “volatilidad, comparabilidad, actualidad, racionabilidad, sensibilidad, funcionalidad” (p. 104).

Mendoza (2018) hace énfasis en su importancia dentro del dominio de las empresas cuando plantea:

Es importante conocer la dimensión de la regulación del derecho de protección de datos personales en posesión de las empresas de servicios establecidas en México, a través del razonamiento lógico normativo que permita analizar los principios y el cumplimiento de obligaciones y deberes en la materia, atendiendo a las características propias de este derecho humano. (p. 269)

Es indudable que el valor de los datos ha aumentado tanto desde el punto de vista económico, como social (Mendoza, 2018; Monsalve, 2017).

Actualmente, los datos personales cuentan con un valor económico, equiparable a ciertos activos intangibles, tales como el software o el valor comercial de los nombres de dominio. Esto ha llevado a considerarlos como el petróleo de la sociedad de la información y del conocimiento. (Mendoza, 2018, p. 269)

La información como resultante de la combinación lógica de los datos, que evidencia una significación razonada, es un activo esencial para desempeño de las organizaciones “el aseguramiento de dicha información y de los sistemas que la procesan es un objetivo de primer nivel” (Orrego, 2013, p. 21).

La relevancia de la relación entre datos e información, “no radica en el dato por sí mismo, sino en el tratamiento, asociación con otros datos y utilidad que se le dé” (Mendoza, 2018, p. 269). Las organizaciones deben llevar procesos de seguridad (Meraz, 2018; Hernández, 2006, Galvis & Pesca, 2019, Cámara de diputados del H. Congreso de la Unión, 2017) e “implantar un sistema que aborde esta tarea de una forma metodológica, documentada y basada en unos objetivos claros de seguridad y una acertada evaluación de los riesgos a los que está sometida la información de la organización” (Orrego, 2013, p. 21).

Material y métodos

El objetivo de esta investigación fue explorar el comportamiento de estudiantes universitarios hacia el tratamiento de los datos personales. La metodología se basó en el análisis de documentos sobre el tema, definición de variables, definición de técnica a aplicar, diseño de encuesta, prueba piloto de encuesta, aplicación de encuesta, estandarización de datos, análisis de resultados y comunicación de resultados. El límite espacial estuvo conformado por los estudiantes y las licenciaturas de la Facultad de Filosofía y Letras de la Universidad Autónoma de Nuevo León. La población seleccionada fue de tipo intencional, por ser una población a la que se podía tener acceso. El tamaño de la población fue de 5000 estudiantes. De esta población se tomó de manera aleatoria una muestra de 420 estudiantes. Los datos de obtuvieron a través de una encuesta, que se aplicó en línea, con el apoyo de la herramienta electrónica QuestionPro. De las 420 encuestas fueron válidas 383. El 91.73 % de los encuestados se ubicó en una edad de 18 a 30 años.

Las variables utilizadas se describen a continuación:

- Derechos sobre datos personales: Se refiere a los derechos de acceder, rectificar, corregir u oponerse a la recogida de datos personales (Derechos ARCO en México).
- Seguridad de datos personales: Se refiere a las rutinas para proteger datos personales en ambientes digitales, así como con quien se comparte los datos personales
- Privacidad de datos personales: Se refiere a los tipos de consecuencias de perder datos personales Normatividad en México: Se refiere a los instrumentos normativos que existen en México para proteger los datos personales y garantizar el acceso a la información

Análisis y resultados

Derechos sobre datos personales

Esta variable se abordó por medio de una escala de Likert (muy importante, poco importante, y nada importante) las situaciones que se incluyeron están relacionadas con el ejercicio de los derechos ARCO que existen en México.

Los resultados operacionalizados es posible observarlos en la siguiente tabla 1. El alto porcentaje de respuestas en el indicador muy importante, apunta hacia el reconocimiento positivo de los encuestados ante las situaciones relacionadas con los derechos ARCO.

Tabla 1
Distribución de respuestas sobre derechos ARCO
para indicador “Muy importante”

Situaciones que ejemplifican los derechos sobre datos personales	Porcentaje de respuesta muy importante
Solicitar la cancelación de los datos personales cuando están siendo utilizados de manera indebida.	98 %
Oponerse al tratamiento de sus datos personales si estos se hubiesen recabado sin su consentimiento.	96 %
Tener acceso al aviso de privacidad al que está sujeto el tratamiento de mis datos.	94 %
Que tus datos personales puedan ser suprimidos cuando, por ejemplo, cancelas tu cuenta de banco.	94 %
Conocer el tratamiento del cual son objeto mis datos personales, así como las cesiones realizadas.	94 %
Conocer dónde puedo rectificar mis datos personales.	94 %
Solicitar y ser informado sobre sus datos personales, el origen de los mismos.	93 %
Conocer los medios por los que las organizaciones brindan información sobre el uso de tus datos personales.	90 %
Solicitar la rectificación de sus datos personales cuando estos sean inexactos.	89 %
Oponerse al tratamiento o recopilación de los datos personales cuando esta no se realice por una entidad pública.	89 %

En el contexto de las instituciones educativas, especialmente las universidades, estos derechos son muy significativos porque van estableciendo una cultura que debe prevalecer ha de predominar en todas las acciones del estudiantado durante sus responsabilidades y acciones futuras.

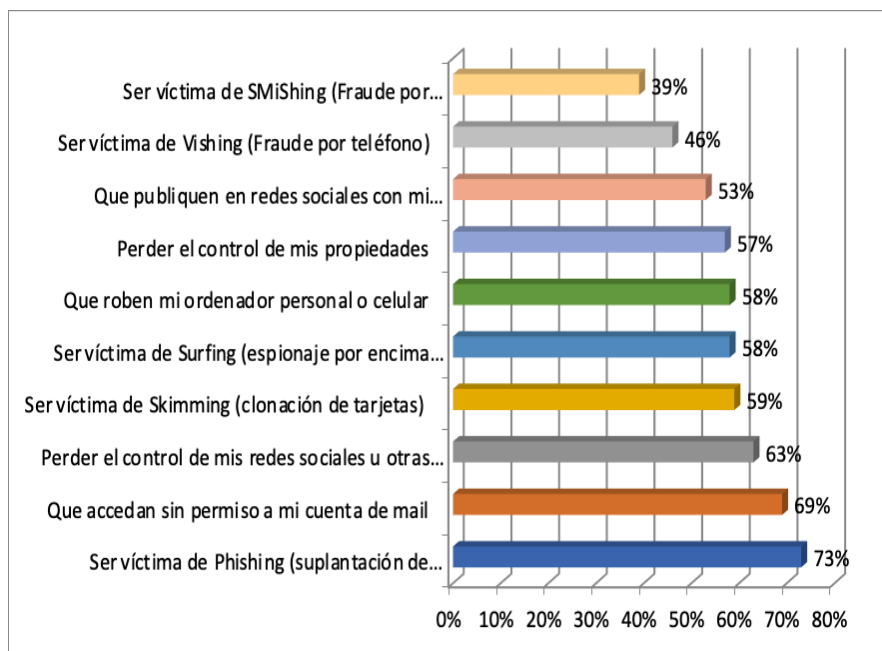
Privacidad de los datos

La privacidad de los datos se abordó por medio de con quién se comparte los datos personales en redes sociales así como las consecuencias de la pérdida de estos.

Otro aspecto a analizar en relación con la privacidad de los datos es la que aborda las consecuencias en caso de estos ser vulnerados. A las personas encuestadas se les presentaron algunas de estas consecuencias y se les pidió que revelaran cuáles les preocupaban más. La figura 1 muestra los resultados en orden de mayor a menor preocupación.

La consecuencia que más le preocupa a los encuestados es ser víctima de *phishing* (suplantación de identidad, 73 %) y lo que menos les preocupa (39 %) es ser víctima de *SMiShing* (Fraude por mensajes SMS).

Gráfico 1
Distribución de consecuencias al ser violentada la privacidad de datos personales



Al vincular los anteriores resultados con la variable *género* se observan convergencias y divergencias en las opiniones (ver tabla 2).

Tabla 2
Distribución de entrecruzamiento entre en la variable
privacidad de los datos y la variable género

Consecuencias	Masculino	Femenino	Otros
Que accedan sin permiso a mi cuenta de mail	13.82 %	11.41 %	25.00 %
Que roben mi ordenador personal o celular	9.68 %	10.11 %	8.33 %
Que publiquen en redes sociales con mi nombre	9.45 %	9.09 %	8.33 %
Ser víctima de <i>surfing</i> (espionaje por encima del otro)	9.45 %	10.34 %	8.33 %
Ser víctima de <i>phishing</i> (suplantación de identidad)	11.98 %	12.83 %	16.67 %
Ser víctima de <i>SMiShing</i> (Fraude por mensajes SMS)	6.45 %	6.81 %	0.00 %
Ser víctima de <i>skimming</i> (clonación de tarjetas)	10.83 %	10.16 %	8.33 %
Ser víctima de <i>vishing</i> (Fraude por teléfono)	6.68 %	8.46 %	0.00 %
Perder el control de mis redes sociales u otras plataformas digitales	10.83 %	11.07 %	8.33 %
Perder el control de mis propiedades	10.83 %	9.71 %	16.67 %
Total	19.66 %	79.79 %	0.54 %

Tanto para el género masculino (13.82 %) como para el género otros (25.00 %), que accedan sin permiso a su cuenta de correo electrónico es lo que más le preocupa con respecto a la privacidad de sus datos. Sin embargo, para el género femenino este aspecto ocupa un segundo lugar (11.41 %).

Lo que más le preocupa al género femenino es ser víctima de *phishing* (suplantación de identidad, 12.83 %). En este caso este aspecto tanto para el género masculino (11.98 %) como para el género otros (16.67 %) este aspecto ocupa un segundo lugar de importancia.

El tercer aspecto más neurálgico con respecto a la privacidad de los datos se comporta de la siguiente manera: al género masculino le preocupan tres situaciones: ser víctima de *skimming* (clonación de tarjetas, 10.83 %), perder el control de redes sociales u otras plataformas digitales (10.83 %), en este caso comparte este tercer lugar con el género femenino (11.07 %) y perder el control de las propiedades que lo comparte con el género otros (16.67 %).

La preocupación por la pérdida de datos personales al ser víctima de suplantación de identidad, o al perder el control de las redes sociales, plataformas digitales, o clonación de tarjetas, para ser específicos en el caso de este estudio, involucra al menos dos aspectos; el temor de las personas hacia la

pérdida de su intimidad y la injerencia en su privacidad, ambas inciden en; la restricción del ejercicio de los derechos de las personas, al no tener dominio de su información personal, el uso no autorizado de fondos bancarios que resultan en deudas dañando el patrimonio financiero e historial crediticio, así como repercusiones a la imagen pública al poder quedar expuesta la reputación de la persona afectada.

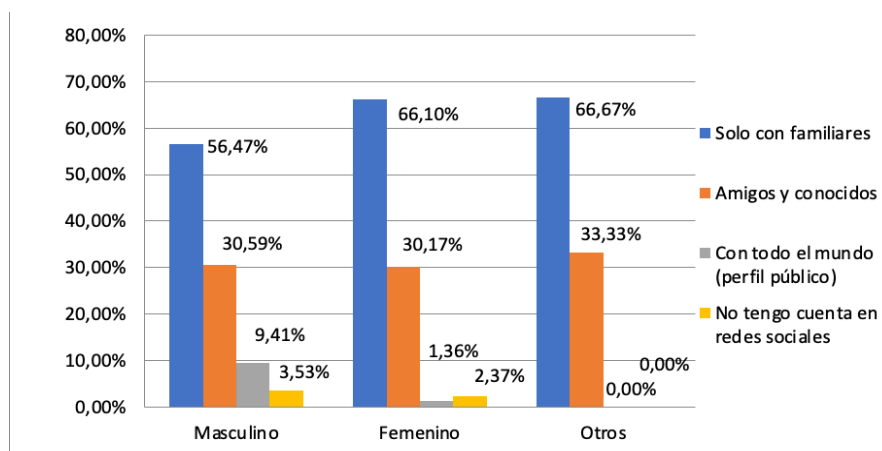
Seguridad de datos personales

La seguridad de los datos personales se investigó a partir de las rutinas utilizadas para proteger los datos personales en ambientes web, así como con quién se comparten datos en redes sociales.

Al abordar con quién se comparte los datos personales, el 64 % respondió que comparte datos con amigos y conocidos, el 30 % solo con familiares, y el 3 % con todo el mundo. Solo el 3 % respondió que no cuenta con redes sociales.

Al profundizar en el análisis y relacionar estos resultados con la variable *género* los resultados indican que Masculino, Femenino y Otros responden de manera similar cuando se trata de compartir información con familiares, amigos y conocidos, o al tomar la decisión de no tener redes sociales (Gráfico 2).

Gráfico 2
Distribución de entrecruzamiento entre la variable privacidad de los datos (compartir datos) y la variable género



Sin embargo, la distancia aumenta —es decir— ya no hay tanta similitud, cuando se trata de compartir datos de forma pública. En este caso el género masculino tiende significativa y mayoritariamente a llevar a cabo esta práctica (ver tabla 4).

Al examinar cómo se lleva a cabo la protección de datos, en este caso las respuestas se inclinaron en primer lugar a elaborar una contraseña complicada (81 %), en segundo lugar a no publicar datos en redes sociales (64 %), así como a no realizar descargas de sitios sospechosos y en tercer lugar a no chatear con desconocidos (57 %) (ver tabla 3).

Tabla 3
Distribución de rutinas en ambientes web
para proteger datos personales

Rutinas para proteger datos personales	Porcentaje
Elaborar una contraseña complicada	81 %
No publicar mis datos en redes sociales	64 %
No realizar descargas de sitios sospechosos	64 %
No chatear con desconocidos	57 %
Verificar los correos si te invitan a hacer clic en algún enlace	49 %
Cambiar mi contraseña cada cierto tiempo	36 %
Usar filtros de seguridad o de dos pasos en mis cuentas	36 %
Navegar en ventana incógnito	29 %
Usar bloqueador de anuncios	26 %
Llamar a mi entidad financiera en caso de sospecha de intromisión	17 %
Publicar con datos falsos	17 %

Las rutinas que menos utilizan los encuestados para proteger sus cuentas corresponden a la de publicar con datos falsos (17 %) o llamar a la entidad financiera en caso de sospecha de intromisión (17 %).

Es posible corroborar los datos anteriores (tabla 4) al relacionarlos con los resultados de con quien se *comparte datos personales*. Elaborar una contraseña complicada es la rutina más utilizada.

Tabla 4
Relación entre de rutinas para proteger datos personales y con quien se comparte datos en ambientes web

Indicadores	Amigos y conocidos	Familiares	No tengo cuenta en redes sociales	Con todos (perfil público)
Elaborar una contraseña complicada	18.12 %	14.93 %	13.11 %	22.45 %
Cambiar mi contraseña cada cierto tiempo	7.21 %	7.99 %	9.84 %	10.20 %
Llamar a mi entidad financiera en caso de sospecha	3.61 %	3.82 %	4.92 %	2.04 %
No publicar mis datos en redes sociales	13.72 %	14.76 %	11.49 %	6.12 %
Publicar con datos falsos	2.55 %	4.86 %	8.19 %	4.08 %
Usar bloqueador de anuncios	5.54 %	4.69 %	6.56 %	8.16 %
Navegar en ventana incógnito	5.80 %	6.77 %	4.92 %	4.08 %
No realizar descargas de sitios sospechosos	13.19 %	12.67 %	11.48 %	16.33 %
Verificar los correos si te invitan a hacer clic en algún enlace	10.38 %	9.72 %	9.84 %	12.24 %
Usar filtros de seguridad o de dos pasos en mis cuentas	7.74 %	7.47 %	6.56 %	8.16 %
No chatear con desconocidos	12.14 %	12.33 %	13.11 %	6.12 %
Total	62.37 %	31.60 %	3.35 %	2.69 %

Se mantiene en segundo lugar de preferencia para la seguridad de los datos personales en ambientes web, la rutina de no publicar datos en redes sociales, tanto para los que comparten con amigos y conocidos como para los que comparten con familiares. Sin embargo, para aquellos que tienen perfil público la segunda opción elegida es la de no realizar descargas de sitios sospechosos. Siendo esta misma rutina la tercera elegida para los restantes grupos. Para los del grupo que comparte información de manera pública la tercera rutina preferida para la seguridad de los datos es la de verificar los correos si te invitan a hacer clic en algún enlace.

Estos resultados revelan que los encuestados están enterados de las cuestiones básicas con respecto a la seguridad de sus datos personales en los ambientes web. Sin embargo, cuestiones de usuarios un tanto más avanza-

dos como navegar en ventana incógnito o usar bloqueador de anuncios no fue de las más seleccionadas por los encuestados. Aunque estas acciones no son garantía absoluta para la seguridad de los datos personales si denota que el uso de rutinas que tienen que ver con las llamadas *cookies* no es tomado muy en cuenta.

Los usuarios un poco más avanzados en los ambientes digitales, realizan acciones como advertir a las entidades financieras con las que se relacionan, verifican los correos con enlaces, así como utilizan bloqueadores de anuncios conjuntamente con revisar las políticas de uso de cookies para estar enterados que tipo de datos se recopila y elegir si permite o no su uso. Comprender las funciones de las *cookies*, los tipos o niveles que existen, los procesos para su gestión o, los tipos de datos que recaban, es parte de la alfabetización contemporánea. Las cookies, pequeños archivos de texto que permiten navegar en el sitio web y hacer uso de sus funciones, así como, tener información y diferenciar a los visitantes del sitio también pueden, en dependencia de la categoría, recopilar datos e información personal. Un sitio web puede utilizar *cookies* propias y/o de terceros o también puede utilizar cookies anónimas protegiendo a los usuarios para que su actividad no sea rastreada al navegar por otros sitios web.

Normatividad en México

En relación con los instrumentos normativos que existen en México para la protección de los datos personales y garantizar el acceso a la información los resultados dan un indicio de la necesidad de educación y capacitación en materia normativa como una de las vías para propiciar un comportamiento informacional coherente y seguro en ambientes digitales.

En este caso se indagó en el conocimiento (por medio de una escala de Likert Mucho, Poco, Nada) de leyes y otros instrumentos normativos. Aproximadamente solo el 7.5 % expresó conocer mucho: la Ley de Acceso Abierto, la Ley de Ciencia y Tecnología, la Ley de Transparencia y Acceso a la Información Pública y los Artículos 6, 7 y 8 de la Constitución Nacional. Un porcentaje un poco más elevado pero poco significativo también, fue que el 15 % se refirió a conocer mucho las páginas de transparencias de la información nacionales en las que se incluyó a las páginas de transparencia de la universidad.

Discusión y conclusiones

Los estudiantes universitarios de ciencias sociales y humanidades consideran muy importantes, los derechos sobre los datos personales que permiten; acceder, rectificar, corregir u oponerse (derechos ARCO) a su tratamiento. En este sentido destacan en importancia el derecho de oponerse o cancelar los datos personales cuando están siendo utilizados de manera indebida o recabados sin consentimiento. Este reconocimiento advierte no solo la importancia que le conceden desde el punto de vista pragmático, sino a la concordancia con el principio de la autodeterminación informativa (Sánchez-Castañeda & Márquez, 2017; Garriga, 2009).

Al tener en cuenta que los datos personales se refieren a aquello que hace identificable a una persona conciernen a aquello que hace de una persona física identificable (Rivera, 2019; Remolina, 2013; García, 2007) y que al combinarse se convierten en información que describe, caracteriza o diferencia a los individuos, se hace necesario tener y conocer el derecho sobre el tratamiento al que se somete. En este sentido Ferrán-Ferrer y Pérez-Montoro (2009) mencionan la importancia de:

Disponer de la información exacta, en el lugar adecuado, en el formato correcto, en el momento justo, y lo suficientemente completa y de calidad como para satisfacer todas las necesidades de información que surgen en los distintos ámbitos de la vida diaria. (p. 366)

La privacidad de los datos es un aspecto que reflejó las preocupaciones del estudiantado universitario, en relación con las consecuencias al ser vulnerados sus datos. Esta situación debe ser atendida desde diferentes ámbitos, ya sea desde los distintos niveles de la educación formal o de manera informal por las instituciones gubernamentales encargadas de la vigilancia y protección de los datos personales de manera que este desasosiego no sea un elemento que limite la libertad y efectividad de sus derechos. El uso de los ambientes y tecnologías digitales no debería limitar el ámbito de la libertad y la protección de datos (García, 2007; Castellanos, 2020), sin embargo, en la medida que se desarrollan aparecen nuevas formas para violentar la privacidad. Los hallazgos indican que, a las personas encuestadas, les inquieta ser víctima de phishing (suplantación de identidad), que accedan sin permiso a la cuenta de correo electrónico, o perder el control de redes sociales u otras plataformas digitales y es de esperarse pues en México, el fraude en materia

de identidad es un problema creciente. En 2015 ocupaba el octavo lugar a nivel mundial en este delito, en ese mismo año en todo el sistema financiero se recibieron 100 000 quejas, con esta cifra, los reclamos habían aumentado más de 500 % con respecto al 2011 (Juárez, 2016).

Sin embargo, los hallazgos indican que las acciones que llevan a cabo para asegurar los datos personales, en ambientes digitales, es básica. Las personas encuestadas se protegen elaborando preferiblemente una contraseña complicada. Aunque hay al menos tres rutinas específicas que también son utilizadas: no publicar datos en redes sociales, no realizar descargas de sitios sospechosos y no chatear con desconocidos, estas recalcan la naturaleza básica de las rutinas empleadas. Se advierte la necesidad de educación en materia de protección de datos y comportamiento informacional algo que Swigon (2013) propone como el *personal knowledge and information management* o lo que Gray et al. (2012) llamaron alfabetización de datos. Esta propuesta no solo se refiere a la gestión de información personal sino al desarrollo de competencias informacionales imprescindible para elevar las competencias que faciliten este objetivo. El hallazgo también coincide con el estudio realizado por el Instituto Federal de Telecomunicaciones en México (2019), que advierte de la necesidad de acciones públicas y privadas para ampliar las habilidades de la población en uso de las TIC con especial atención en los adolescentes.

Este estudio sugiere que se conoce poco sobre las normativas para el tratamiento y la protección de datos personales existentes en México. Se hace evidente que esta época exige políticas públicas que regulen todo lo referido a los datos y la información (Araujo, 2016; Requena & Sánchez, 2014) y que las mismas sean conocidas por todos los grupos sociales que a su vez, conscientes de sus derechos, se comporten en correspondencia con lo normado y establecido y que igualmente contribuyan con su difusión y cumplimiento. Este hallazgo hace reflexionar sobre el desempeño de las organizaciones gubernamentales en la educación de la población, si se tiene en cuenta que entre las obligaciones genéricas de la ley general de transparencia y acceso a la información pública en México, se enuncia en el artículo 66 que es obligación establecer las condiciones tecnológicas y usar medios de difusión de la información para desarrollar el conocimiento de la población en materia de transparencia y protección de datos personales (Sánchez-Castañeda & Márquez, 2017; Cámara de diputados del H. Congreso de la Unión, 2020).

Por otro lado, el resultado de que la normativa más conocida por los encuestados es la relacionada con las páginas de transparencia de la universidad se corresponde con el papel de las universidades públicas de establecer y dar a conocer un modelo de datos abiertos que sea útil para su comunidad (Domínguez, 2016; Islas 2017).

Los resultados alcanzados por esta investigación, brindan una oportunidad para trazar nuevas metas y objetivos que permitan que las otras generaciones dominen estos temas y actúen en consecuencia. Una verdadera sociedad de la información exige que sus componentes estén instruidos, alfabetizados en todo lo relativo al manejo de datos, información y conocimiento, pero que igualmente dominen políticas, derechos y obligaciones.

Una limitación del trabajo es que no se encontraron estudios con los que se pudieran establecer amplias comparaciones. Otra de las limitaciones es el hecho que en México el tema es abordado de manera relativamente reciente fuera del ámbito empresarial.

Bibliografía

- Aparicio, J., & Pastrana, M. (2017). Conceptos y legislación de transparencia sindical y protección de datos personales de los trabajadores en México. *Revista latinoamericana de derecho social*, 24, 175-193. <http://bit.ly/3uu2v15>
- Araujo-Carranza, E. (2016). El derecho a la información y la protección de datos personales en el contexto general y su construcción teórica y jurídica. *Revista IUS*, 3(23). <https://doi.org/10.35487/rius.v3i23.2009.195>
- Arellano, W., & Ochoa, A. (2013). Derechos de privacidad e información en la sociedad de la información y en el entorno TIC IUS. *Revista del Instituto de Ciencias Jurídicas de Puebla A.C.*, VII(31),183-206. <https://bit.ly/3pZcZSM>
- Barreau, D. K. (1995). Context as a factor in personal information management. *Journal of the American society for information science*, 46(5), 327-339. <https://bit.ly/3qY2EYo>
- Barreau, D. K. (2009). Gestión de información personal, no solo recuperación de información personal. *El Profesional de la Información*, 18(4), 61-364. <https://doi.org/10.3145/epi.2009.jul.01>

- Barreau, D. K. (2008). The persistence of behavior and form in the organization of personal information. *Journal of the American Society for Information Science and Technology*, 59(2) 307-317. <https://bit.ly/3qY2EYo>
- Cámara de diputados del H. Congreso de la Unión (2010). Ley Federal de Acceso a la Información y Protección de Datos personales. <https://bit.ly/3kmw2F7>
- Cámara de diputados del H. Congreso de la Unión (2011). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. <http://bit.ly/2MoLHr9>
- Cámara de diputados del H. Congreso de la Unión (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. <https://bit.ly/3bB5OuB>
- Cámara de diputados del H. Congreso de la Unión (2020). Ley General de Transparencia y Acceso a la Información Pública. <https://bit.ly/3uzesm0>
- Castellanos, J. (2020). La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos. *Métodos de Información*, 11(21), 59-82. <https://dx.doi.org/10.5557/IIMEI11-N21-059082>
- Cotino-Hueso, L., Rebollo-Delgado, L., Vidal-Fueyo, María del Camino, Troncoso-Reigada, A., García-Mahamut, R., Rallo-Lombarte, A., Murillo de la Cueva, Pablo Lucas, & Medina-Guerrero, M. (2020). Encuesta sobre la protección de datos personales. *Teoría y Realidad Constitucional*, (46), 15-118. <http://bit.ly/3smSZej>
- Domínguez, A. (2016). *Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación ubicua*. Dykinson, S.L.
- Feregrino, E. (2012). *Ley Federal de Protección de Datos Personales en posesión de los particulares*. Ediciones Fiscales ISEF. 100.
- Ferran-Ferrer, N., & Pérez-Montoro, M. (2009). Gestión de la información personal en usuarios avanzados en TIC. *El profesional de la información*, 18(4), 365-373. <http://bit.ly/37Kwo3r>
- Galvis-Cano, L., & Pesca-Mesa, D. A. (2019). Límites del tratamiento de los datos personales en el ámbito laboral frente al uso de las tecnologías de la información y comunicación en la era digital. *Iusta*, (52), 51-76. <https://doi.org/10.15332/25005286.5482>
- García, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado*, 40(120), 743-778. <http://bit.ly/3snKSy4>
- Garriga, D. A. (2009). *Tratamiento de datos personales y derechos fundamentales*. Dykinson.

- González, L. (2019). Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros *Revista Estudios Socio-Jurídicos*, 21(1), 209-244. <https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.941>
- Gray, J., Chambers, L., & Bounegru, L. (2012). *The Data Journalism Handbook*. O'Reilly Media.
- Hernández, A., & Zavala, O. (2018). Datos personales en las relaciones laborales del sector privado. *Revista Latinoamericana de Derecho Social*, (27). <http://bit.ly/3aRWC6b>
- Hernández, V. (2006). Referentes legales para un marco protector de datos personales. *Ra Ximhai*, 2(3), 567-580. <https://doi.org/10.35197/rx.02.03.2006.02.vh>
- Instituto Federal de Telecomunicaciones en México (2019). *Uso de las TIC y actividades por internet en México: impacto de las características sociodemográficas de la población* (versión 2019). IFT. <https://bit.ly/2ZTF1UM>
- Islas, J. (2017). *Estudio sobre los alcances del derecho de acceso a la información en Universidades e Instituciones de educación superior públicas dotadas de autonomía derivado de la Reforma Constitucional en materia de transparencia*. INAI. <https://bit.ly/3srbcXY>
- Juárez, R. (2016). Iniciativas. Senado de la República. *Gaceta del Senado*. México, 2016. <http://bit.ly/2MnapYO>
- Kettinger, W. J., & Marchand, D. A. (2011). Information management practices (IMP) from the senior manager's perspective: An investigation of the IMP construct and its measurement. *Information Systems Journal*, 21(5), 385-406.
- Mendoza, A. O. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. *Revista del Instituto de Ciencias Jurídicas de Puebla*, 12(41), 267-291. <https://bit.ly/3uGgAZs>
- Meraz, A. (2018). Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales *Revista IUS*, 12(41) 293-310. <https://bit.ly/3qRZSDW>
- Monsalve, V. (2017). La protección de datos de carácter personal en los contratos electrónicos con consumidores: análisis de la legislación colombiana y de los principales referentes europeos. *Prolegómenos. Derechos y Valores*, XX(39),163-195. <https://bit.ly/3ko0JtJ>
- Orrego, V. M. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Revista Pensamiento Americano*, 4(6). <http://bit.ly/2O3BYHi>

- Ortega, A. (2015). La desprotección “internacional” del titular del derecho a la protección de datos de carácter personal barataria. *Revista Castellano-Manchega de Ciencias Sociales*, 19, 37-56. <http://bit.ly/3uyioTY>
- Ozmen-Ertekin, D., & Ozbay, K. (2012). Dynamic data maintenance for quality data, quality research. *International Journal of Information Management*, 32, 282-293. <https://doi.org/10.1016/j.ijinfomgt.2011.11.003>
- Páez, I. (1992). *Gestión de la inteligencia, aprendizaje tecnológico y modernización del trabajo informacional. Retos y oportunidades*. Universidad Simón Bolívar. <https://bit.ly/3dHkKKs>
- Porcelli, A. M. (2019). La protección de los datos personales en el entorno digital, los estándares de protección de datos en los países iberoamericanos. *Quaestio Iuris*, 12(2). <https://doi.org/10.12957/rqi.2019.40175>
- Portilla-Romero, J. (2017) Gobierno de datos, un potenciador de los sistemas de gestión de calidad. *Signos*, 9(2)159-172. <https://doi.org/10.15332/s2145-1389.2017.0002.10>
- Requena, E. J., & Sánchez, L. F. J. (2014). El derecho a la información y la protección de datos personales en la constitución mexicana. *Acalán Revista de la Universidad Autónoma del Carmen*, 1(4), 27-31. <http://bit.ly/3swHYqZ>
- Remolina, N. (2013). Tratamiento de datos personales en el contexto laboral. *Revista Actualidad Laboral*, 175, 19-24. <https://bit.ly/2ZR0HnA>
- Rivera, V. (2019) Realidad sobre la privacidad de los datos personales en Costa Rica. *E-Ciencias de la Información*, 9(2), 68-81. <https://doi.org/10.15517/eci.v9i2.37503>
- Sánchez-Castañeda, A., & Márquez, D. (2017). *Estudio sobre transparencia y acceso a la información en personas físicas y morales. Alcances de la reforma constitucional y legal*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. <https://bit.ly/37NPbeh>
- Swigon, M. (2013). Personal knowledge and information management-conception and exemplification. *Journal of Information Science*, 46(5), 832-845. <https://doi.org/10.1177/0165551513501435>
- Wang, R. Y., Ziad, M., & Lee, Y. W. (2001). *Data quality*. Kluwer Academic Publishers.