ENSAYO CIENTÍFICO

El impacto de la protección de datos en el sector empresarial: el caso Costa Rica

THE IMPACT OF DATA PROTECTION IN THE BUSINESS SECTOR: THE CASE OF COSTA RICA.

Perla Maxiel Taisigüe Obregón [1], María Paula Hernández Vásquez [2], Andy Fabricio Gómez Guido [3], Arianna Argüello Astorga [4]. Bajo la supervisión del prof. Gabriel Silva Atencio [5]

Fecha de recepción: 12 de mayo de 2022 | Fecha de aprobación: 6 de junio de 2022

Resumen

De acuerdo con la información concretada en 1948 en el documento de las Naciones Unidas, se presenta el artículo 12, el cual menciona que nadie es objeto de injerencias arbitrarias en su vida privada, así como a su familia, domicilio o su correspondencia ni de ataques a su honra o a su reputación. Este documento representa por primera vez derechos humanos fundamentales que deben protegerse en el mundo entero.

A lo largo de la historia siempre ha existido esa necesidad y se han creado distintas formas de regularlas según la época, sin embargo, no es hasta la actualidad donde se solidifican todos los esfuerzos de granitos de arena.

En este mismo artículo se hace referencia al derecho de la privacidad, que es una condición necesaria que refuerza a otros derechos como la igualdad, la no discriminación, la libertad de expresión y reunión. Por otro lado, los factores más importantes que han provocado la necesidad de la protección de datos personales son la protección a la dignidad humana, la preocupación jurídica por la intimidad y el honor, así como el impacto social producido con la aparición de los ordenadores. Esto permite protegernos sobre decidir cómo se quiere interactuar con el mundo, tanto físico como digital y colaborar a delimitar el acceso a la información. No obstante, surge la interrogante sobre cómo gestionan las empresas de Costa Rica este derecho. Este artículo analiza el cumplimiento de este derecho en algunas instituciones.

1 Universidad Latinoamericana de Ciencia y Tecnología, ORCID: https://orcid.org/00000003-22349775 taisigue.perla08@gmail.com
2 Universidad Latinoamericana de Ciencia y Tecnología, ORCID: https://orcid.org/00000003-16067827 mariaphdezv@gmail.com
3 Universidad Latinoamericana de Ciencia y Tecnología, ORCID: https://orcid.org/00000002-94115209 fabricio.andy@live.com
4 Universidad Latinoamericana de Ciencia y Tecnología, ORCID: https://orcid.org/00000002-6174-843X arianna04@hotmail.com
5 Universidad Latinoamericana de Ciencia y Tecnología, ORCID: https://orcid.org/00000002-4881-181X gsilvaa468@ulacit.ed.cr

Palabras clave:

Datos sensibles, *habeas data*, tratamiento de datos, RGPD, filtración de datos

Abstract

According to the information provided in 1948 in the document of the United Nations, article twelve is presented, where it mentions that no one shall be subjected to arbitrary interference with his privacy, as well as his family, home, or correspondence, nor to attacks on his honor or reputation. This document represents for the first-time fundamental human rights that must be protected worldwide. Throughout history, there has always been this need, and different forms have been created according to the time and ways to regulate them; however, it is not until today that all the efforts are being solidified granites of sand. Likewise, in this same article, reference is made to the right to privacy, which is a necessary condition that reinforces other rights such as equality, non-discrimination, freedom of expression and assembly. On the other hand, the most crucial factors that have provoked the need for the protection of personal data have been the protection of human dignity, the legal concern for privacy and honor, and the social impact produced by the appearance of computers. This allows us to protect ourselves in deciding how we want to interact with the physical and digital world and to collaborate in limiting access to our information. But how do Costa Rican companies manage this right? This article analyzes the fulfillment of this right in some institutions.

Keywords:

Sensitive data, habeas data, data filtering, GDPR, data processing.

Introducción

En el acoso telefónico en el que indican que llaman para ofrecer un servicio como un préstamo una aseguradora, un concurso, entre otras propuestas en el ámbito costarricense que nunca se solicitó surge la duda de por qué esta empresa tiene mis datos si nunca mantuve una relación de cliente-servicio. Probablemente, la respuesta por parte de algunas entidades no estaría muy lejos a: "Usted compartió los datos con X servicio que nos permite acceso a nosotros", pero cuán realista y cierto es este argumento.

A partir de la creación de la Ley n.º 8968 del 7 de julio de 2011 de Protección de la Persona frente al Tratamiento de sus Datos Personales, se creó la institución de Agencia de Protección de Datos de los Habitantes (Prodhab). Según el informe de denuncias actualizado que rige del año 2014 a 2019 se contabiliza un total de 495 denuncias contra principalmente sectores de banca y finanzas, comercial

y gestionadoras de cobro, por delitos de incumplimiento al derecho de supresión, actualización o rectificación de datos recopilados, acoso telefónico y transferencia de datos sin previo consentimiento (Agencia de Protección de Datos de los Habitantes, 2019).

Por otro lado, el *habeas data* es una especie de amparo que permite el derecho de acceso a los datos que se encuentran en bases de datos públicas o privadas y Costa Rica sigue el modelo regulatorio europeo que tiene origen en 1970 en Alemania a partir de la regulación del uso de los datos. Lo anterior especialmente por los antecedentes en los cuales Alemania mantuvo una mala experiencia por parte del Estado como resultado del holocausto por la existencia de bases de datos en manos de régimen nazi que permitían determinar características de las personas como religión, racial o demográfico. No obstante, las primeras regulaciones, aunque fueron visionarias en un mundo analógico, no se contó con que más tarde se convertirían en el activo principal de un modelo económico global, donde las grandes compañías se dedican en la actualidad a la extracción del rastro de datos de usuarios, producto del empleo de las tecnologías para perfilar y ofrecer servicios, dos grandes ejemplos de esto son Facebook y Google (París, 2021).

Sin embargo, aunque Costa Rica creó la legislación anterior, la norma pasó inadvertida en su primera década de existencia, hasta el año 2020 que surgió el caso de UPAD y otros acontecimientos que dieron como resultado que el tema fuera de más interés a la población por primera vez en relación con el empleo disfuncional de los datos personales en el país. Por esto, la Ley de Protección de Datos ha quedado desfasada en un escenario tecnológico, social y hasta político, lo que da paso a consecuencias de mala gestión y regulación ineficaz.

Por esto, este artículo analiza el impacto de la protección de datos personales en el sector empresarial de Costa Rica. En la actualidad, con el incesante apoderamiento de la tecnología en el mundo y la masiva cantidad de datos, existen al menos 142 países con leyes de protección de datos. En el caso de América Latina, Chile fue el primer país en adoptar una ley de este tipo en 1999 y después otros países inspirados a partir del Reglamento General de Protección de Datos (RGPD), pero a lo que respecta a la protección de datos en cuanto a aplicación de la ley pocos países han adoptado el modelo de medidas de la Unión Europea (Rodríguez y Alimonti, 2020).

Lo anterior genera un problema significativo de grandes filtraciones de datos, las cuales han tenido como resultado consecuencias perjudiciales a los propietarios y entidades involucradas principalmente por mal gestionamiento, lo que ocasiona un mayor interés por la creación de gobiernos y leyes que velen por la seguridad de la información.

Esto con el empeño de proteger la intimidad de las personas mediante la protección en el tratamiento de sus datos por medio de un marco regulatorio actualizado, sofisticado y exigente.

Revisión de la literatura

Cuál es el activo más importante de las empresas, el inmobiliario, el producto o los servicios. Si se llevan a cabo estas preguntas a cada departamento es posible encontrarse con distintas respuestas, pero si se profundiza en el área de recursos humanos posiblemente la respuesta sea el capital humano (Belluomo, 2022). A pesar de que para dar los mejores esfuerzos para la empresa se necesita designar dentro de lo posible a las personas adecuadas en sus puestos por desempeñar, en cierto modo es la importancia de la información la que destaca en el ámbito corporativo debido a que con ella se puede identificar, de manera efectiva, las necesidades de las personas para trabajar sobre estas y ejecutar un plan que satisfaga a los usuarios (Fernández, 2019).

Por lo tanto, es evidente que estos procesos que se crean en empresas den paso a la constante transformación digital, una revolución que permiten las llamadas tecnologías de la información, donde los datos se convierten en el activo más relevante día tras día.

Existen distintos tipos de información, entre ellos los datos personales y datos sensibles. Los datos sensibles hacen referencia a: "El nivel más íntimo de su titular y cuya divulgación pueda ser causa de discriminación o generar un severo riesgo para su titular" (Sánchez Pérez y Rojas González, 2022, s. p.). Los datos se comparten entre empresas y personas, ya sea por servicios contratados o productos por compras que se llevan a cabo, por lo que diferenciar cuál es la información personal es fundamental. Sin embargo, qué se conoce como información personal. De acuerdo con el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (2022): "Los datos personales son toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables" (s. p.). Entre estos datos se pueden mencionar según la Tabla 1:

Tabla 1. Datos que nos hacen o no identificables

Ejemplos de datos personales	Ejemplos de no personales
1. Nombre y apellidos, **2**. domicilio, **3**. dirección de correo electrónico, del tipo nombre.apellido@empresa.com, **4**. número de documento personal de identidad, **5**. datos de localización (como la función de los datos de localización de un teléfono móvil), **6**. dirección de protocolo de internet (IP), **7**. identificador de una cookie, **8**. el identificador de la publicidad del teléfono, **9**. los datos en poder de un hospital o médico, que podrían ser un símbolo que identificara de forma única a una persona.	**1**. número de registro mercantil, **2**. dirección de correo electrónico, del tipo info@empresa.com, datos anonimizados.

Fuente: Adaptado de la Comisión Europea (2018).

A la vez, los datos personales integran otros conceptos que son importantes para su comprensión y protección. En primer lugar, la privacidad, el Diccionario panhispánico del español jurídico (2022), define la privacidad como: "Facultad de una persona de prevenir la difusión de datos pertenecientes a su vida privada que, sin ser difamatorios ni perjudiciales, esta desea que no sean divulgados" (s. p.), es decir, todos los datos son de pertenencia única y deben mantenerse de esta forma.

El segundo, la confidencialidad, que la Real Academia (2022) designa como: "Que se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho. Información confidencial" (s. p.). Ambos conceptos son relevantes para el análisis de estudio, ya que la información personal es privada, sin embargo, a quienes se les brinda esta información se debe asegurar que sea confidencial, porque las personas no deben compartirlas libremente; una acción que en la actualidad no sucede de manera constante en las empresas.

Tan solo en el campo del Internet se pueden generar 2,5 trillones de *bytes* de datos en el mundo y es un potencial de cambio en la sociedad similar al petróleo o electricidad, por lo que esta se vuelve una mercancía de materia prima, en forma de *big data* para las empresas (International Business Machines, 2015) Además, según Sempf (2020) los datos son tan valiosos como los medios de pago para superar retos empresariales como también para analizar la demanda. Por esto, la idea de negocio de algunas empresas se centra en la recolección y análisis de datos, de modo que les permita comprender a qué mercado apuntar para determinado *target*. De esta manera, no es de extrañar que en la actualidad la información y, por ende, los datos personales sean fundamentales hasta el punto de llegar a la compra de bases de datos para intereses corporativos, aunque no se desee aceptar esta verdad (Contreras, 2015).

Por otro lado, los gobiernos de las tecnologías de la información toman protagonismo, de manera que progresivamente se han apoderado del mercado (Deloitte, 2019) debido a que este forma un órgano de alto nivel que dirigirá la toma de decisiones, tanto evaluativas como de supervisión de la información. Por ende, el gobierno de TI se convierte en una utilidad para realizar y describir ciertos procesos de los recursos de las tecnologías de información y cómo esto puede tener un impacto en las empresas. Por esto, ofrece la posibilidad de ser competitivos gracias a las innovaciones que TI aporta a las organizaciones, el valor que pueden generar al negocio con las inversiones y el acatamiento de las leyes, regulaciones e incluso las políticas pertinentes dejan claro que las TI no es ajeno del negocio que opera.

Ante la pregunta sobre si es posible efectuar la gestión de un gobierno de TI por medio de los monitoreos integrales, Forrester Consulting menciona que la confidencialidad de los datos de la información ocasiona una mejora en todas las áreas posibles de la organización, logra un aumento progresivo en la eficiencia operacional y las capacidades que se pueden desarrollar en el momento de la toma de decisiones y toma como base la confianza e inteligencia sobre los datos custodiados.

Los gobiernos de datos en la compañía regalan una variedad de ventajas, como la accesibilidad de los datos, aseguramientos de estos para cumplir con lo deseado y hasta el gestionamiento de estos como un

activo de la entidad y es importante destacar que debe existir una estrategia eficiente para la protección de los datos del gobierno de TI. Por ejemplo, el bloqueo de accesos de dudosa procedencia, al incorporar sistemas de monitoreo, sistemas de *firewalls*, *switches*, los balanceadores de carga que se encargan de tener un punto de contacto únicamente para el acceso del *software*, entre otros métodos técnicos y herramientas con el punto de custodiar integralmente los datos (E-dea Networks, 2022).

Debido a las nuevas tecnologías de la información, se permite recolectar y tratar una cantidad masiva de información, de forma casi ilimitada, de lo cual se genera una preocupación global, por lo que se da paso a la creación de reglamentos propios de distintos países, pero inspirados especialmente por el caso europeo, así es como la protección de los datos personales ya no se basa solo en el ámbito físico, sino también digital (Colaborador de DocuSign, 2021). No obstante, ante la pregunta sobre cómo involucra a las organizaciones del sector empresarial, se debe puntuar que la protección de datos personales se asocia también a los datos sensibles, ya que se relacionan con características de un individuo, es decir, aquello que involucra una esfera íntima del titular, como:

1. Estado de salud.
2. Origen étnico.
3. Orientación sexual.
4. Afiliación a organizaciones sindicales o políticas.
5. Creencias religiosas o filosóficas
6. Aspectos biométricos o genéticos

Por lo tanto, de no protegerse de manera adecuada, los titulares de esos datos pueden ser identificables hasta discriminados. Por esto la relevancia del tratamiento y la recolección de datos del sector empresarial tanto público y privado, ya que esta pende del involucramiento incorrecto del uso, la divulgación, almacenamiento y transferencia por cualquier medio de los datos.

En la mayoría de los casos la toma de datos es directa de los titulares. Por ejemplo, cuando se suministra nombre y apellidos como correo electrónico para un registro de un servicio en línea o de forma indirecta, cuando se consigue información mediante una base de datos pública o en el que se transfieren a un tercero.

Sin embargo, las empresas deben ser confidenciales y transparentes sobre cómo recaban y tratan los datos de cada individuo mediante aspectos de seguridad y privacidad en especial donde nunca son idénticos de un proceso a otros. (Colaborador de DocuSign, 2021).

En el ámbito internacional, entre los casos más conocidos de violación por privacidad a datos a 50 000 000 de usuarios fue el de Cambridge Analytica, el cual se vio envuelto en una multa de €4,500,000,000 a Facebook en 2018, además de un reporte de obligación sobre las medidas de protección de datos y prevención de abusos. La lección relevante de este hecho es el peligro que presenta compartir información con una finalidad distinta a la informada al usuario; en este caso para crear perfiles psicológicos y predecir el comportamiento con el objetivo de manipular la intención de voto a favor del partido que contrató el servicio, es decir, a favor de Donald Trump (Rodríguez, 2020).

En el caso de Costa Rica, aunque en el 2011 la Asamblea Legislativa aprobó la Ley para la Protección de la Persona frente al Tratamiento de sus Datos Personales, la cual tuvo una reforma en 2016 para especificar su ámbito de aplicación, esta no es suficiente. Lo anterior se debe a dudas que se han presenciado sobre su aprobación en contraste con leyes que toman referencias como el Reglamento General de Protección de Datos de la Unión Europea (RGPD) (Briancesco, 2021).

A la vez, esta ley menciona derechos y principios básicos para la protección de estos en el país. Esta ley refiere dos principios primordiales, el principio de consentimiento informado, el cual impone una serie de obligaciones al responsable de los datos, como informar al titular de los datos personales de manera previa, expresa y precisa, del tratamiento de los datos y de las condiciones por las cuales se tratan estos datos personales. El siguiente es el principio de calidad de la información, el cual establece que los datos recopilados por parte del responsable deben ser actuales, veraces, exactos y adecuados al fin.

En cuanto a los derechos garantizados, la Ley n.º 8968 otorga a todas las personas el derecho al acceso de sus datos personales, rectificación o supresión, así como el derecho a la cesión de sus datos personales.

Por lo tanto, el responsable debe garantizar a las personas el poder de ejercer alguno de estos derechos en los plazos concretos y de manera gratuita. Si esto no se cumple hay una serie de multas que el responsable debe enfrentar, estas se dividen en faltas leves, graves y gravísimas (Durango, 2021).

Para las faltas leves, una multa hasta de 5 salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República. Para las faltas graves, una multa de 5 a 20 salarios base del cargo de auxiliar judicial I, de acuerdo con la Ley de Presupuesto de la República. Para las faltas gravísimas, una multa de 15 a 30 salarios base del cargo de auxiliar judicial, según la Ley de Presupuesto de la República y la suspensión para el funcionamiento del fichero de 1 a 6 meses (Revista Summa, 2020).

Sin embargo, se han iniciado discusiones a partir de distintos casos que cobran relevancia, como el de la Unidad Presidencial de Análisis de Datos (UPAD) el cual consiste en emplear inteligencia de datos para política pública por medio de acceso a datos confidenciales con el objetivo de ayudarse para la toma de decisiones en materia de políticas públicas y presupuestos institucionales y que todavía es punto de críticas y de investigación en curso en la actualidad.

Entre otros casos, se encuentra el Proyecto de Repositorio de Datos Biométricos, que se centralizaría en el Tribunal Supremo de Elecciones para recolección y tratamiento de datos biométricos de la población, donde la policía, Ministerio Público y Organismo de Investigación Judicial y la Dirección General de Migración pueden acceder a estos datos. Este proyecto lo dictaminó la comisión del gobierno y administración en octubre de 2021.

La Dirección de Migración lanzó en el primer trimestre de 2022 un pasaporte con un sistema de datos biométricos inteligentes, sin embargo, la Fundación Privacidad y Datos presentó recursos de amparo, por considerar que la entidad no resolvió dudas ni explicó medidas de seguridad. Además, que no respeta un marco jurídico porque el tratamiento de datos biométricos solo puede darse mediante ley habilitante y esta no existe, por lo que hay problemas ya que ni siquiera se prevén sanciones relevantes cuando es el Estado quien incumple la legislación dentro de una desactualización de al menos 10 años de retraso y donde el precio que se paga es muy alto (Silva, 2022).

Con respecto a la interrogante sobre si se pueden transferir bases de datos libremente entre instituciones o el gobierno, en Costa Rica se define concepto de transferencia de datos como:

> Acción mediante la cual se trasladan datos personales del responsable de una base de datos personales a cualquier tercero distinto del propio responsable, de su grupo de interés económico, del encargado, proveedor de servicios o intermediario tecnológico, en estos casos siempre y cuando el receptor no use los datos para distribución, difusión o comercialización (Medrano Melara, 2020, s. p.).

Además, se establece que:

> Los responsables de las bases de datos, públicas o privadas, solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley, por lo que toda venta de datos o de bases de datos parcial o total debe reunir requerimientos como los mencionados anteriormente, tomando en cuenta el consentimiento informado del titular (Medrano Melara, 2020, s. p.).

Según El Financiero (2017):

> Desde 2014 se recibieron 141 denuncias por infracción a la legislación vigente en Costa Rica sobre la protección de los datos personales. De ellas, 29 se declararon a favor del denunciante, 9 esperan resolución final y 8 se encuentran en trámite. Solo

> el año anterior, se recibieron 62 quejas, según la Agencia de Protección de Datos de los Habitantes (Prodhab), que se encarga de hacer cumplir la legislación y recibir denuncias (s. p.).

Aunque los costarricenses están denunciando, no son muchos quienes lo hacen comparado con la cantidad de personas que ven ese derecho de privacidad violado.

Con respecto a bases de datos, del 2014 al 2016 tan solo 59 bases se inscribieron ante la Prodhab de un estimado de 5000 que deben registrarse tomando en cuenta la Ley n.º 8968.

Según esta ley, todas aquellas bases de instituciones o empresas públicas o privadas de propósito de difusión, distribución o comercialización deben inscribirse a excepción de fines personales o domésticos o de recursos humanos que son internas que se emplean sin que se vendan u otros. Por lo tanto, la obligación es entregar los ficheros que tienen responsable de administrar la base de datos, tipos de datos almacenado y procedimiento de rectificación de información, entre otros (Nelson Ulloa, 2016)

Por ende, a pesar de los intentos por la protección de datos, la divulgación de datos personales actualmente es un problema que afecta a la mayoría de las personas, por lo que según cada país se han creado leyes de protección de los datos, ya que es muy común encontrar empresas que realizan llamadas a personas que no tienen relación alguna, pero que ya poseen sus datos personales. En Costa Rica se creó la Ley n.º 8968, la cual sirve para delimitar cómo debe ser el manejo y divulgación de los datos personales para evitar violentar los derechos de los demás (Barrantes, 2019).

De acuerdo con el Sistema Costarricense de Información Jurídica (2022), el objetivo primordial de esta ley es:

> De orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

En los primeros capítulos se destacan hechos importantes que tanto las personas que toman los datos como quienes los brindan deben estar conscientes de la forma correcta de efectuarlos. Entre los puntos cruciales se menciona que existe la obligación por parte de quien solicite los datos de información, así como cuáles son los fines por los que se piden los documentos, también la identidad del responsable de la base de datos, el tratamiento que se le hará los datos, así como los destinatarios y los consultores de estos,

entre otros. Por lo tanto, es valioso que las empresas conozcan sobre la ley y mantenga a su personal educado y actualizado sobre las normas y leyes para no infringirlas, así como cada persona que ofrezca sus datos y que puedan conocer sus derechos para ser conscientes sobre qué sucedería ante la negativa de brindarlos.

Por último, es fundamental tomar en cuenta que la ley menciona que la transmisión de los datos personales solo pueden realizarla los responsables de las bases de datos bajo aprobación explícita del titular de los datos. Sin embargo, en la actualidad, esto no sucede con frecuencia, ya que muchas empresas consideran prudente vender sus bases de datos a terceros sin autorización del titular, ya que en los últimos años es muy sencillo por las facilidades tecnológicas que existen.

El transmitir una base de datos por medios digitales no representa el mismo esfuerzo que podía representar hace 70 años cuando los datos se manejaban en papel.

Metodología

El artículo se efectuó con un enfoque cualitativo, gracias a la recopilación, análisis e investigación que se llevó a cabo para elaborarlo. Del mismo modo, la principal herramienta que se utilizó es la revisión documental, debido a que se recopiló información de distintas fuentes con el objetivo de analizar y determinar qué información es relevante para el artículo que permitiese profundizar sobre la divulgación de datos personales en Costa Rica y cómo estos se tratan tomando en cuenta la perspectiva en cuanto a importancia de la protección de datos en el ámbito nacional y global.

Según Hurtado (2008), la revisión documental suele ser una técnica donde se recopila información de algún tema en específico. Esto con el fin de obtener diferentes variantes que se relacionen entre sí, directa o indirectamente con el tema principal, lo cual permite la construcción de conocimientos y ampliar la realidad desde la disciplina.

Para finalizar, se lleva a cabo la elaboración de posibles recomendaciones y conclusiones para el campo de la privacidad personal de las personas ciudadanas costarricenses, como lo dicta la Ley n.º 8968. Además, se detalla cómo a partir de esto se logra tener una amplia información y casos sobre cómo las personas funcionarias suelen infringir o tergiversar la verdad en el momento de cometer desfalco ante esta ley.

Resultados

En Costa Rica existen muchos casos de filtración indebida de datos personales, a través del tiempo se pueden mencionar algunos. Entre los más recientes se puede mencionar cuando en el año 2020 comenzando

la pandemia se encontró el paciente cero en el país, el cual era el primer caso de un costarricense portador de la enfermedad. Para ese momento ya era de conocimiento público que existen enormes cantidades de filtraciones en la Caja Costarricense de Seguro Social (CCSS) y en este caso no fue la excepción, varios medios de comunicación dieron a conocer el nombre del médico, Reinaldo Albernas, lo que desató una ola enorme de acoso a su familia y amigos cercanos.

Se afirma que Reinaldo Albernas contagió alrededor de 80 personas, esto sin fuentes certeras y según relata su familia, el acoso recibido era tanto que recibían desde llamadas para amenazarlos de muerte hasta bromas sobre la muerte del médico.

En el medio digital CRhoy (2020), la sobrina de nombre Leya comentó que: "Las llamadas eran reales y eran a toda hora. Tanto que entramos en estado de desesperación que uno no duerme, uno no come". Posteriormente, la familia se enteró de que al menos 35 empleados de la CCSS husmearon en el expediente médico de Reinaldo, personal de todo el país tuvo acceso a información personal y confidencial del paciente, por lo que hubo una gran violación de reglamentos donde no se vio ninguna reprensión.

En cuanto a la CCSS, también existe un caso muy recordado por la población por el año 2016, donde sin autorización del paciente se grabó una cirugía de extracción de una yuca del recto de un hombre y no fue suficiente con grabarlo, acto que está prohibido, ya que el uso de teléfonos celulares está prohibido dentro de una sala quirúrgica, sino que también se publicó en redes sociales y en minutos el país entero tenía conocimiento no solo de la noticia, sino del video de la persona. Vargas (2016), relata por medio de Teletica digital que: "La Gerencia Médica de la Caja Costarricense de Seguro Social confirmó que el video se grabó en el hospital Calderón Guardia" (s. p.).

Adicionalmente, menciona que: "Las autoridades de ese centro médico realizarán ahora una investigación sobre lo sucedido en la situación, la cual podría trascender al campo penal si el paciente decide presentar una denuncia" (Vargas, 2016, s. p.).

Sin embargo, 4 meses después otro medio escrito reportó que para ese momento la CCSS no había realizado nada ni mucho menos había declarado ninguna responsabilidad por la filtración hacia ninguna persona; incluso cuando se tenía muy claro quiénes estuvieron presentes.

Otro caso relacionado con empresa de telefonía es el de Eugenia Cartín, quien sufrió la filtración de una llamada telefónica que tuvo con un empleado de servicio al cliente de la compañía Tigo. En el año 2017 se hizo de conocimiento público una grabación donde la señora le reclamaba al empleado de una manera eufórica el mal funcionamiento del servicio de Internet que le impedía trabajar con facilidad. Esta llamada llegó a miles de teléfonos porque una persona dentro de la empresa incumplió el reglamento y ley de protección de datos personales. Pocas horas después a la publicación existían miles de imágenes con burlas e incluso se llegó a personificaciones en televisión sin su autorización.

Eugenia relata al periódico La Nación (2017) que:

> Al principio no tomé muy en serio el asunto, pero ahora sí me preocupa mucho, porque ha llegado a nivel internacional y me ha inquietado mucho en el plano profesional de que esto vaya a afectar mi trabajo. Dependo de mi trabajo, la casa no es mía (s. p.).

Todos los actos mencionados terminaron en una millonaria demanda que realizó la afectada, ya que las consecuencias para ella fueron graves (La Nación, 2017). En este caso en particular, la empresa tuvo una pérdida económica por el acto indebido de un empleado de violar la privacidad de un cliente, un derecho que muchos desconocen.

Como nuevo caso, se tiene la amenaza de los cibercriminales Conti. El pasado 19 de abril de 2022, el Gobierno de Costa Rica se enfrentó a un ataque cibernético en el que el objetivo fue el Ministerio de Hacienda. Este ataque provocó una afectación en el sistema de declaraciones de impuestos y también puso en riesgo la plataforma para el pago de salarios públicos. Además, se detectó la exposición de datos que pertenecen a la Dirección General de Aduanas, sin embargo, el Ministerio aseguró que la información que se divulgó no afecta las actuaciones operativas o de fiscalización. En la Tabla 2 se sintetizan y analizan los casos previamente expuestos:

Tabla 2. Síntesis de casos de divulgación de datos en Costa Rica

Empresa	Hallazgo	Consecuencias a la víctima	Fallo empresarial	Sanción
Caja Costarricense del Seguro Social	Filtración / Divulgación de información personal con respecto al paciente 0 de Covid en Costa Rica	Acoso, amenazas de muerte	Mala gestión de accesos a la información	No
Caja Costarricense del Seguro Social	Filtración / Divulgación de información personal y videos de sala quirúrgica en redes sociales	Acoso, daños al autoestima	Mala gestión de accesos a la información, incumplimiento de procedimientos	No
Tigo	Filtración / Divulgación de información personal y llamada telefónica	Daño y repercusiones en el ámbito profesional	Incumplimiento de reglamento	Sí (Demanda)

A partir de lo anterior se demuestra la necesidad de que las organizaciones mantengan seguros los datos de posibles ataques cibernéticos, pero también de tratar los datos de manera adecuada, debido a que el incumplimiento de los requisitos de la protección de datos puede dañar la reputación de una compañía,

del titular o hasta del Estado con respecto a la importancia que se le da a esta. Por esto, es necesario desarrollar una estrategia integral para la seguridad de la protección de datos con respaldo de un marco legal y reglamentario que debe actualizarse constantemente.

Discusión

Como es posible observar, la mala gestión empresarial de los datos personales y la poca atención hacia la aplicación de la ley han conducido a que los costarricenses sean víctimas de violaciones a sus derechos con repercusiones que atentan contra la autoestima, la dignidad y hasta la propia vida. Aunque existe la ley para el debido resguardo de la información, las denuncias que se han emitido en contra de este derecho son muy pocas, lo que deja en tela de duda la apropiación o conocimiento de la ley para los habitantes de Costa Rica, la falta de ética empresarial y la falta de prioridad ante el problema. Por este motivo, surge la interrogante sobre qué puede hacer Costa Rica para lograr un cambio ante la presencia de estas situaciones.

Algunas acciones pueden ser concientizar a la población costarricense de sus derechos como ciudadanos ante la filtración de información o datos confidenciales, como las llamadas telefónicas a empresas o servicios públicos, información personal con respecto a la salud e incluso el compartir información con algún servicio y que este mismo intercambie los datos que se brindan con otro servicio. El servicio de responsabilidad comienza en las empresas y las entidades a las cuales se les brindan los datos personales. Desde el momento en que se concientiza el brindar esta información los servicios deben mantener un trato de confidencialidad cliente-empresa, ya que, para brindar un buen servicio, no se debe dejar de lado el mejor manejo de la base de datos de cada entidad para proteger esta información.

De este modo, se puede educar a la población para que sea consciente de sus derechos ante las situaciones que atentan contra la privacidad de sus datos personales y así realizar un ambiente de confianza y respeto en las entidades en la que las personas ciudadanas confían para brindar su información.

Conclusiones

En Costa Rica el tema de seguridad informática es un área deficiente al que no se le da la prioridad que se debe. Por esto, los datos personales se publican sin autorización, en repetidas ocasiones.

A pesar de existir la Ley n.º 8968 hay mucho desconocimiento sobre esta a nivel sociedad fuera de empresas. Lo anterior afecta la manera en que las personas brindan sus datos, ya que desconocen el uso que se les deben dar y también provoca una ignorancia general sobre cómo actuar en caso de que alguna empresa divulgue los datos sin autorización.

Finalmente, a pesar de que en el ámbito empresarial sí es de conocimiento la ley que defiende los derechos de los datos personales, se presenta una práctica poco ética que es vender bases de datos entre sí por beneficios en común. Esto denota una ausencia del ente encargado de vigilar que estos hechos no sucedan.

Recomendaciones

Es importante que las personas ciudadanas lean y se informen sobre los deberes y derechos de sus datos personales, así como conocer cuáles corresponden y cuáles no. Además de saber cuáles acciones tomar ante una filtración de alguna empresa a la cual se tiene certeza que nunca se brindaron tales datos.

Es indispensable que haya una mejora en las entidades que controlan las bases de datos y sus reproducciones ilícitas, para generar un ambiente más seguro para las personas. De esta forma, pueden auditarse para reconocer los movimientos existentes y determinar si se ha extraído la *data* completa y a quien se envió.

Al existir tanta desinformación de las personas ciudadanas sobre el uso correcto de los datos según la Ley n.º 8968, se cree conveniente hacer esta información de conocimiento masivo. Lo anterior con el fin de que las personas puedan informarse de algo que ahora saben que existe, ya que no hay mucha información sobre esto en medios escritos o digitales.

Futuras líneas de investigación

Uno de los aspectos importantes que se debe tomar en cuenta para trabajos futuros es la importancia de la protección de los datos personales, con respecto al sector empresarial que hay en Costa Rica. Esto con el objetivo de llevar a cabo un estudio en profundidad sobre qué hace el país para lograr la regulación y reforzamiento de la protección de los datos en el ámbito digital y físico.

A partir de esto, se puede crear o impulsar la creación de una empresa que apoye a la población y concientice de esta manera a los trabajadores costarricenses a respetar y salvaguardar la información confidencial de los clientes. Lo anterior para generar ambientes de confianza en las personas que ingresarán datos sensibles en las empresas. La importancia de la ley de la persona frente al tratamiento de sus datos personales es aplicable a todo habitante en Costa Rica.

Referencias

Agencia de Protección de Datos de los Habitantes. (2019). *Informe de denuncias MCS*. https://drive.google.com/file/d/1I-gQyxDHkjMgytBfvsJYTNzjktujIP1_/view

Amorín, D. (2016). *Porque la información es el activo más importante de tu empresa: Backup Online*. LinkedIn. https://www.linkedin.com/pulse/porque-la-informaci%C3%B3n-es-el-activo-m%C3%A1s-importante-de-tu-david-amor%C3%ADn/?originalSubdomain=es

Barrantes, R. (2019). *Realidad sobre la privacidad de los datos personales en Costa Rica*. Scielo. https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1659-41422019000200068

Belluomo, R. (2022). *Personas: El activo más importante de la empresa*. Evaluando Software. https://www.evaluandosoftware.com/personas-activo-mas-importante-la-empresa/

Briancesco, M. (2021). *Costa Rica: reforma para protección de datos personales*. Ipandetec. https://www.ipandetec.org/2021/02/09/reforma-datos-personales/

Colaborador de DocuSign. (2021). ¿Qué son datos sensibles? La gran preocupación de la era de la información. DocuSign. https://www.docusign.mx/*blog*/datos-sensibles

Comisión Europea. (2018). ¿Qué son los datos personales? European Commission. https://ec.europa.eu/info/law/law-topic/*data*-protection/reform/what-personal-*data*_es

Contreras, M. (2015). *Así es como las grandes empresas venden tus datos en Internet*. El confidencial. https://www.elconfidencial.com/tecnologia/2015-09-14/asi-es-como-venden-tus-datos-personales-en-internet_1011071/

Cortés Ruiz, S. (2019). *Protección de datos: sus orígenes y la privacidad desde el diseño*. Asociación de mujeres en el sector público. https://mujeresenelsectorpublico.com/proteccion-de-datos-sus-origenes-y-la-privacidad-desde-el-diseno/

CrHoy. (2016). *Caja investigará quién difundió video y fotos de paciente*. https://archivo.crhoy.com/caja-investigara-quien-difundio-video-y-fotos-de-paciente/nacionales/

CrHoy. (2021). *La pesadilla de la primera familia tica con COVID19: en memoria del Dr. Albernas*. https://www.crhoy.com/nacionales/la-pesadilla-de-la-primera-familia-tica-con-covid-19-en-memoria-del-dr-albernas/

Deloitte. (2019). *Gobierno de TI en las empresas y su necesaria implementación*. https://www2.deloitte.com/cr/es/pages/risk/articles/gobierno-de-ti-en-las-empresas-y-su-necesaria-implementacion.html

Dhpedia. (2021). *Artículo 12 de la Declaración Universal de los Derechos Humanos*. https://dhpedia.wikis.cc/wiki/Art%C3%ADculo_12_de_la_Declaraci%C3%B3n_Universal_de_Derechos_Humanos#:%7E:text=%C2%ABNadie%20ser%C3%A1%20objeto%20de%20injerencias,contra%20tales%20injerencias%20o%20ataques.%C2%BB

Diccionario panhispánico del español jurídico. (2022). *Privacidad*. https://dpej.rae.es/lema/privacidad

Durango, E. (2021). *Protección de Datos Personales y su regulación en Costa Rica*. GoLegal. https://golegalcr.com/proteccion-de-datos-personales-en-costa-rica/#:%7E:text=La%20protecci%C3%B3n%20de%20datos%20personales%20en%20Costa%20Rica,al%20Tratamiento%20de%20sus%20Datos%20Personales%20N%C2%B0%2037554-JP

E-dea Networks. (s. f.). *Cómo implementar un buen gobierno de datos en una empresa*. E-dea. https://www.e-dea.co/blog/como-implementar-gobierno-de-datos-en-la-empresa

Editor. (2015). *Los datos, la nueva materia prima de la era*. Ibm. https://www.ibm.com/blogs/think/es-es/2015/07/15/los-datos-la-nueva-materia-prima-de-nuestra-era/

El Financiero. (2017). *En 3 años hubo 140 denuncias por violación de datos personales*. https://www.elfinancierocr.com/tecnologia/en-tres-anos-hubo-140-denuncias-por-violacion-de-datos-personales/3IYF7L5TMBHKZKIUGVFKO2MDZE/story/

Fernández, H. (2019). *¿Qué es el Capital humano y cómo influye en el éxito de las empresas?* Economía TIC. https://economiatic.com/capital-humano/

https://www.nacion.com/el-pais/servicios/eugenia-cartin-afectada-por-filtracion-de-llamada-de-tigo-para-mi-todo-esto-ha-sido-pavoroso/JN4LBH4CCBEKNMT2Y5QM7AVSUI/story/

Hurtado, J. (2008). *Guía para la comprensión holística de la ciencia*. Unidad III, Capítulo 3, 45-65. http://virtual.urbe.edu/tesispub/0092769/cap03.pdf

Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México. (2022). ¿Qué son los datos personales? https://infocdmx.org.mx/index.php/protege-tus-datos-personales/%C2%BFqu%C3%A9-son-los-datos-personales.html

La Nación. (2017). Eugenia Cartin reclama a Tigo $500,000 por filtración de llamada. https://www.nacion.com/el-pais/servicios/eugenia-cartin-reclama-a-tigo-500-000-por-filtracion-de-llamada/CJUYTJ2I3ZGVRDSRXCMFW6MHSQ/story/

La Nación. (2017). *Eugenia Cartín, afectada por filtración de llamada de Tigo: 'para mí todo esto ha sido pavoroso'*.

Medrano Melara, J. (2020). ¿Se pueden transferir bases de datos personales libremente entre instituciones del gobierno? Adalid Medrano. https://adalidmedrano.com/se-pueden-transferir-bases-de-datos-personales-libremente-entre-instituciones-del-gobierno/2020/

Naciones Unidas. (1948). *La Declaración Universal de los Derechos Humanos*. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Nelson Ulloa, J. (2016). *Solo 59 bases de datos de unas 5000 están inscritas en agencia de protección de información*. Amelia Rueda. https://www.ameliarueda.com/nota/bases-de-datos-inscripcion-informacion-datos

París, M. (2021). *Protección de datos personales: no perdamos la década siguiente*. La República. https://www.larepublica.net/noticia/proteccion-de-datos-personales-no-perdamos-la-siguiente-decada

Real Academia Española. (2022). *Confidencial*. https://dle.rae.es/confidencial

Remolina Angarita, N. (2012). *Revista Internacional de Protección de Datos Personales*. Habeas Data Colombia. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf

Revista Summa. (2020). *Costa Rica: ¿Qué se debe saber sobre la protección de datos?* https://revistasumma.com/costa-rica-que-debemos-saber-sobre-la-proteccion-de-datos/

Rodríguez, K. y Alimonti, V. (2020). *Un panorama retrospectivo y futuro de la protección de datos en*. Electronic Frontier Foundation. https://www.eff.org/es/deeplinks/2020/09/look-back-and-ahead-*data*-protection-latin-america-and-spain

Rodríguez, P. (2020). *Hay empresas que tiene extensos informes con tus datos personales recopilados en Internet y los venden*. Xataka. https://www.xataka.com/privacidad/hay-empresas-que-tiene-extensos-informes-tus-datos-personales-recopilados-internet-venden-cien-euros

Sánchez Pérez, G. y Rojas González, I. (2022) *leyes de protección de datos personales en el mundo y la protección de datos biométricos- parte i*. UNAM. https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93

Semanario Universidad. (2020). Nueve funcionarios de la Caja perdieron la batalla contra la COVID19. https://semanariouniversidad.com/ultima-hora/nueve-funcionarios-de-la-caja-perdieron-la-batalla-contra-el-covid-19/

Sempf, J. (2019). ¿Por qué tus datos son tan valiosos? Hornetsecurity. https://www.hornetsecurity.com/es/seguridad-de-la-información/la-era-de-la-información-por-que-tus-datos-son-tan-valiosos/?_adin=01833301559

Silva, I. (2022). *Costa Rica: elecciones entre denuncias, violación de datos personales y reformas de ley insuficientes*. Derechos Digitales. https://www.derechosdigitales.org/18043/costa-rica-elecciones-entre-denuncias-violacion-de-datos-personales-y-reformas-de-ley-insuficientes/

Sistema Costarricense de Información Jurídica. (2022). *Protección de la Persona Frente al Tratamiento de sus Datos Personales n.º 8968*. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989

SWI swissinfo.ch. (2022, 19 de abril). *El Ministerio de* Hacienda *de Costa Rica enfrenta un ciberataque*. https://www.swissinfo.ch/spa/costa-rica-ciberataque_el-ministerio-de-hacienda-de-costa-rica-enfrenta-un-cibertaque/47528790#:%7E:text=San%20Jos%C3%A9%2C%2019%20abr%20(EFE,el%20pago%20de%20salarios%20p%C3%BAblicos