Derecho al olvido e intimidad, protección de datos

Right to be forgotten and privacy, data protection

Itza López Spencer[1], Universidad Latinoamericana de Ciencia y Tecnología

2021

Resumen

El derecho a la intimidad es un derecho fundamental que se encuentra estipulado en la Constitución Política Costarricense, específicamente en el artículo 24 y hace referencia a que este garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Por lo tanto: "Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República" (Constitución Política de la República de Costa Rica, 1949). Asimismo, este fundamento se enlaza con el derecho al olvido, que se refiere a limitar a terceros el uso de datos de un particular. Se debe tener claro que cada persona tiene derecho a que se respeten sus datos, su información, publicaciones, entre otros elementos a los que se está susceptible en la Era de Datos y el flujo de información que se comparte en los diferentes medios de comunicación, como también a que no se publique información errónea. Por otra parte, que si se publica información en un caso concreto, que esta pueda eliminarse cuando ya no tenga ningún efecto. Por este motivo, en este artículo se desarrollan puntos sobre la aplicación del derecho al olvido en temas crediticios, en personas objeto de publicaciones periodísticas o casos como el del español Mario Costeja, quien logró que la justicia europea sentenciara al buscador (Google) a eliminar datos que violaban su privacidad. Todo esto enlazado al derecho de intimidad y los datos e información que circula constantemente.

Palabras clave: derecho, intimidad, olvido, datos, protección.

[1] La autora es estudiante de Licenciatura en Derecho en la Ulacit. Correo electrónico: itzalopez_12@yahoo.es

Abstract

The right to privacy is a fundamental right that is stipulated in the Costa Rican Political Constitution, specifically in its article 24 and refers to the fact that it guarantees the right to privacy, freedom and secrecy of communications. Therefore, private documents and written, oral or any other type of communications from the inhabitants of the Republic are inviolable. Likewise, this foundation is linked to the Right to be forgotten, which refers to being able to limit the use of an individual's data to third parties. It must be clear that each person has the right to respect for their data, information, publications, among others, elements to which we are susceptible in the Data Age and the flow of information that is shared by the different means of communication, as well as to ensure that erroneous information is not published. On the other hand, if any information published by a specific case can be eliminated when it no longer has any effect. That is why this article will develop points about the application of the Right to Forget in credible issues, in people who are the object of journalistic publications, or cases such as the Spanish, Mario Costeja, who managed to get the European Justice to sentence the search engine (Google) to eliminate data that violated their privacy, all linked to the right to privacy and the data and information that constantly circulate.

Keywords: right, privacy, forget, data, protection.

1. Introducción

Con el paso del tiempo es cada vez más común lidiar con un tema de gran relevancia como el derecho que tenemos a proteger nuestra información, ya que en el nuevo mundo de la globalización y los grandes avances tecnológicos se hace más cotidiano ver nuestros días, funciones y comunicaciones consumados en el uso de las tecnologías de información (TI), la Internet, aplicaciones, entre otros medios. Por lo tanto, es necesario preguntarnos qué información es privada/íntima, qué información dejamos en Internet y cuál de ella se elimina, se borra o se olvida. O mejor todavía, preguntarnos si nos detenemos a leer cada cláusula de un contrato, documento o factura cuando adquirimos algún bien en un lugar comercial o cuando abrimos por primera vez Facebook, Instagram o WhatsApp.

Probablemente estos medios tecnológicos son tan eficientes para comunicarnos que no nos cuestionamos ni un poco sobre la información privada que brindamos o si esta pudiera afectarnos

o eliminarse aplicando algún proceso legal. Por consiguiente, el objetivo de este documento es conocer y revisar la información proporcionada por diferentes medios, como leyes, normativas e Internet, sobre la protección de datos, el derecho a la intimidad y al olvido y conocer casos reales sobre esto.

El tema por desarrollar en este artículo es El derecho al olvido e intimidad, protección de datos, por lo que es importante mencionar lo que indica la Agencia Española de Protección de Datos (AEPD) (s. f.) referente a que:

> El internet y los servicios que a través de ella se prestan se han convertido en un elemento imprescindible para nuestras vidas. En cualquier lugar y a cualquier hora, estos servicios forman parte de nuestro día a día: cuando nos informamos, nos relacionamos compartiendo información con otras personas, publicamos fotos o vídeos.
>
> Sin embargo, en buena parte de los casos los servicios más usados en la red se prestan gracias a la cantidad de información y datos personales que los usuarios aportamos, tanto a las empresas que ofrecen los servicios como a otros usuarios, por lo que debemos ser conscientes de los riesgos que esto puede suponer para nuestra seguridad y privacidad (s. p.).

La forma exponencial en que circulan las imágenes, comentarios y noticias a través de las redes sociales (a menudo carentes de veracidad) diluye rápidamente la posibilidad de evitar que se produzcan conceptos erróneos, tanto sobre hechos como sobre temas. Además, vale la pena mencionar la tarea difícil y, muchas veces imposible, de revertir los efectos que pueden implicar un daño mental, emocional, material y relacional irreparable. A esto debe agregarse la interferencia constante en nuestras áreas de privacidad mediante el Internet de las cosas (siglas en inglés IoT), los separables, las aplicaciones y la inteligencia artificial, todo lo cual es la consecuencia de un empoderamiento global de *big data*.

2. Revisión bibliográfica

Según la Procuraduría General de la República (1994):

> el Derecho fundamental a la intimidad constituye un límite para el derecho de acceso a la información pública. Alcances. “IV.- El numeral 24 de la Constitución Política consagra el derecho fundamental a la intimidad. Se trata de un fuero de protección a la vida privada

> de los ciudadanos. La intimidad está formada por aquellos fenómenos, comportamientos, datos y situaciones de una persona que normalmente están sustraídos al conocimiento de extraños y cuyo conocimiento por éstos puede turbarla moralmente por afectar su pudor y su recato, a menos que esa misma persona asienta a ese conocimiento. Si bien, no puede menos que reputarse que lo que suceda dentro del hogar del ciudadano es vida privada, también puede ser que lo que suceda en oficinas, hogares de amigos y otros recintos privados, esté en ese ámbito. De esta manera los derechos constitucionales de inviolabilidad del domicilio, de los documentos privados y de las comunicaciones existen para proteger dicha intimidad, que es un derecho esencial de todo individuo. El domicilio y las comunicaciones solo ceden por una causa justa y concreta. Lo mismo debe suceder con la intimidad en general, pues como indica la Convención Americana de Derechos Humanos, "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación" (Resolución n.º 1026-1994).

Por ejemplo, en otro aspecto como:

> El salario bruto es dato de acceso público, salario neto es información de carácter privado. Las operaciones de crédito o ahorro u otras deducciones que tienen los funcionarios públicos con Bancos, cooperativas, u otros organismos es información confidencial. "No obstante, en este caso la información allí detallada, contiene información privada que únicamente le interesa al funcionario involucrado por cuanto indica las operaciones de crédito o ahorro u otras deducciones que tiene con Bancos, cooperativas, u otros organismos. La Sala entiende el carácter público y el derecho que tiene todo ciudadano a conocer en forma general cuál es el salario nominal de un funcionario que ocupa determinado puesto en la Administración Pública, pero para obtener el desglose y monto del salario devengado (salario neto) de un determinado funcionario en particular, tiene que demostrar un interés legítimo para poder acceder a tal información" (Resolución n.º 14997-2003).

Sobre el derecho al olvido es importante indicar que se considera como un avance del derecho a la intimidad[2], al desarrollar su contenido en sus resoluciones judiciales y establecer su carácter independiente del derecho a esta, con base en sus principios y el objeto de protección. Los principios de protección de datos, así como las garantías que posee su titular, fueron establecidos en las resoluciones de este Tribunal Constitucional, ante la ausencia de legislación expresa que regulara la materia. Es decir, la regulación de los principios de protección de los datos personales debe ser por la vía legal; es el legislador quien debe encargarse de dotar de contenido a estos (Bolaños Chaves, 2012).

Sin embargo, ante la ausencia de legislación protectora de datos personales, la Sala Constitucional los creó y dotó de contenido. Por lo tanto, se da el surgimiento vía jurisprudencia nacional, por lo que el derecho al olvido puede caracterizarse como un interés protegido jurídicamente, que tienen las personas para la eliminación de cualquier dato o información relativa a ellas, que no cumpla con el principio de calidad de los datos, en relación con su actualidad y finalidad. Es decir, este es el derecho de las personas a que se elimine de cualquier base de datos, información no actual o adecuada al fin para el cual se recolectó.

La Sala Constitucional ha sido la encargada de tratar el tema, conceptualizarlo y caracterizarlo, ante la ausencia de legislación expresa que lo regule. Este Tribunal ha definido el derecho al olvido como aquel que existe en los casos en los que los datos consignados en las bases de datos no son actuales ni cumplen con la finalidad para la cual se recolectaron (Bolaños Chaves, 2012). Estas dos circunstancias (falta de actualidad o cumplimiento de la finalidad) provocan que el almacenamiento de los datos sea perjudicial para su titular, dañando su honor, imagen o sus derechos fundamentales en general. Por esto, la Sala Constitucional ha afirmado que el derecho al olvido es un:

> Principio a tenor del cual ciertas informaciones deben ser eliminadas de los archivos oficiales transcurrido un determinado lapso desde el momento en que acaeció el hecho a

[2] Hernández Valle (s. f.) define el derecho a la intimidad como aquel que "garantiza un ámbito privado reservado a la propia persona y del que quedan excluidos los demás, salvo, desde luego, que el titular del derecho desee compartir esa zona de privacidad con otros semejantes (…) protege el entorno familiar de la persona, por lo que cada uno tiene el derecho de exigir respeto no sólo de sus actuaciones como ser individual, sino también como parte integrante de un núcleo familiar, dado que esos vínculos inciden en la propia esfera de la personalidad de cada uno" (s. p.).

> que se refieren, para evitar que el individuo quede prisionero de su pasado. En efecto, a juicio de esta Sala todo ser humano necesita que se le reconozca su capacidad para rectificar su vida, que es un ejercicio de la fuerza creadora de su libertad. Si al hecho negativo del error cometido se le agrega la imposibilidad de restauración y de una nueva creación, la vida de los seres humanos quedaría estancada y sin más posibilidades, en el momento de equivocarse (Sala Constitucional. Voto número 2004-04626).

A pesar del paso del tiempo Costa Rica no ha desarrollado normativa más allá de situaciones relacionadas con el uso de información de los ciudadanos en entidades públicas y privadas, el comercio, salud, entre otros. Por el contrario, en otros países se desarrollan temas en relación con los motores de búsqueda, editores originales y otros. Por ejemplo, sobre la retirada de URLs de la Búsqueda de Google por privacidad[3]:

> En una sentencia de mayo del 2014, el Tribunal de Justicia de la Unión Europea declaró que cualquier persona tiene derecho a solicitar a los motores de búsqueda, como Google, que retiren ciertos resultados de las consultas que hagan referencia a ella. Los motores de búsqueda deben aplicar esta decisión si los enlaces en cuestión son "inadecuados, irrelevantes", si "ya no son relevantes" o si son "excesivos", teniendo en cuenta factores de interés público, como el papel desempeñado por la persona en la vida pública. Solo se retiran páginas de los resultados como respuesta a solicitudes relacionadas con el nombre de una persona concreta. Bloqueamos las URL de todos los resultados de búsqueda europeos de Google (resultados de usuarios en Alemania, Francia, España, etc.) y utilizamos señales de geolocalización para restringir el acceso a la URL desde el país de la persona que ha solicitado la retirada (Herránz, 2018, s. p.).

En la Figura 1 se muestra el número total de solicitudes recibidas y el número total de URLs cuya retirada se ha solicitado desde el 29 de mayo del 2014:

[3] Uniform Resource Locator es la dirección única y específica que se asigna a cada uno de los recursos disponibles de la World Wide Web para que puedan ser localizados por el navegador y visitados por los usuarios.

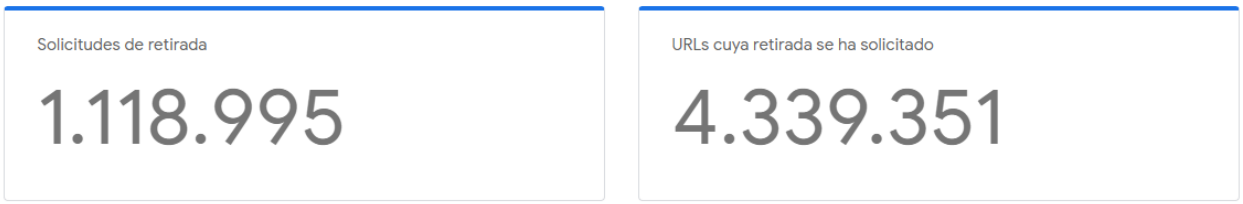

Figura 1
Solicitudes URLs

Fuente: Google (s. f.).

3. Metodología

Este artículo se desarrolla con el sistema de investigación cualitativa con un enfoque descriptivo, el cual estudia los fenómenos como aparecen en el presente, en el momento de llevar a cabo la investigación y tiene como objetivo describir situaciones y eventos. En cuanto a las fuentes, se utiliza la recolección de información escrita, como las leyes públicas, reglamentos nacionales e internacionales, normas, conversaciones con profesores con conocimiento en la materia, revisión de publicaciones relacionadas con interés y casos reales publicados. Lo anterior, con el objetivo de conocer y revisar el tratamiento existente sobre la protección de datos en relación con el derecho a la intimidad y el derecho al olvido, qué normativa se aplica, si existen actualizaciones de la normativa y cuáles han sido algunos criterios y resoluciones a favor de una persona. Por este motivo, se revisa y analiza la información encontrada.

Entre la normativa revisada e información analizada en el ámbito nacional, se cita la Constitución Política Costarricense, votos de la Sala Constitucional, información de la Procuraduría General de la República, Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, Ley 8968, Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, n.º 37554-JP y el Proyecto de Ley: Reforma Integral a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales. Asimismo, información extraída de la página *web* de la Agencia de Protección de Datos de los Habitantes (Prodhab) (s. f.), la cual: “Es una institución de desconcentración máxima adscrita al Ministerio de Justicia y Paz, con independencia de criterio y personalidad jurídica instrumental propia en el desempeño de las funciones” (s. p.). Además de conversaciones vía teléfono con el profesor universitario, Mauricio Garro Guillén, entre otra información conexa.

Entre la información internacional se puede mencionar el Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Información de la Agencia Española de Protección de Datos (AEPD). Asimismo, casos reales, por ejemplo, Cambridge Analytic y Mario Costeja.

La información obtenida se estudia con el propósito de conocer qué normativa existe en Costa Rica y en otros países. Asimismo, si en Costa Rica ha evolucionado la reglamentación al respecto y, en caso de que exista ausencia de legislación que proteja los derechos del ciudadano en referencia al derecho de intimidad y olvido, si se dan acciones del legislador para llenar esos vacíos legales.

4. Resultados

En este acápite se presentan varios conceptos, así como normativa nacional e internacional y otros resultados de la investigación sobre el derecho a la intimidad y derecho al olvido, en la protección de datos. Además, a pesar de que en la Constitución se establecen derechos fundamentales al respecto, se busca jurisprudencia y casos reales en los cuales se pueda observar su aplicación. En Costa Rica existe la Agencia de Protección de Datos de los Habitantes (Prodhab)[4] (s. f.), que es:

> Una institución de desconcentración máxima adscrita al Ministerio de Justicia y Paz, con independencia de criterio y personalidad jurídica instrumental propia en el desempeño de las funciones y en la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones (s. p.).

Además:

> Su principal objetivo es garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a su derecho a la autodeterminación

[4] La Prodhab se creó mediante la Ley 8968 del 7 de julio del 2011, publicada en el diario oficial La Gaceta N. °170 del 5 de setiembre del 2011. Sus funciones y procedimientos, además, son desarrollados mediante el Reglamento a dicha ley (en adelante RPDP), publicado en el Decreto Ejecutivo N. °37554-JP del 30 de octubre del 2012, y publicado en el alcance N. °42 de diario oficial La Gaceta, N. °45 del 05 de marzo del 2013.

> 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 (Prodhab, s. f., s. p.).

4.1. Concepto de derecho a la intimidad y derecho al olvido

Según Scanavino (2012): "El Derecho a la intimidad es la facultad que le reconoce el estado al hombre de mantener reservada la información que considere no comunicable" (s. p.). Por otra parte, el Art. 11 del Decreto Ejecutivo 37554 (2012) indica sobre el derecho al olvido:

> La conservación de los datos personales que puedan afectar a su titular, no deberá exceder el plazo de diez años, desde la fecha de terminación del objeto de tratamiento del dato, salvo disposición normativa especial que establezca otro plazo, que por el acuerdo de partes se haya establecido un plazo distinto, que exista una relación continuada entre las partes o que medie interés público para conservar el dato.

4.2. Constitución Política Costarricense - Derecho a la intimidad

La Constitución Política de la República de Costa Rica (1949) en el artículo 24 establece que se garantiza el derecho a la intimidad a la libertad y al secreto de las comunicaciones. Además, indica:

> Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.

De acuerdo con Salazar Fuentes (2014):

> La ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán

ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial.

No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación (p. 149).

4.3. Normativa de protección de datos en Costa Rica

A continuación, se presenta la información relevante sobre esta narrativa.

4.3.1. Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, n.º 8968 (2011)

Esta ley hace referencia a definiciones como:

Artículo 3. Definiciones.

a) Base de datos: cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.

b) Datos personales: cualquier dato relativo a una persona física identificada o identificable.

c) Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

d) Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.

Artículo 4.- Autodeterminación informativa.

Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección. Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias.

4.3.2. Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, n.º 37554-JP (2012)

Este reglamento, se basa en:

> Razón del riesgo a la intimidad o actividad privada del individuo, deviene necesario velar por la defensa de la libertad e igualdad del mismo con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona, cuando estos figuren en bases de datos de organismos públicos o privados (Decreto Ejecutivo 37554, 2012).

En el Art. 11 de este cuerpo normativo, se establece el Derecho al olvido:

> La conservación de los datos personales que puedan afectar a su titular, no deberá exceder el plazo de diez años, desde la fecha de terminación del objeto de tratamiento del dato, salvo disposición normativa especial que establezca otro plazo, que por el acuerdo de partes se haya establecido un plazo distinto, que exista una relación continuada entre las partes o que medie interés público para conservar el dato.

4.3.3. Proyecto de Ley: Reforma Integral a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (2021)

De este proyecto de ley se desprende lo siguiente:

> Datos sin protección, el reto de actualizar la normativa.
> El país cuenta con una Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales aprobada en 2011 -cuya discusión legislativa se remonta a inicios de los 2000- que establece regulaciones para el manejo y procesamiento de datos sensibles en las bases de instituciones públicas y empresas, y que fue considerada de avanzada al momento de su creación. Sin embargo, carece de varios conceptos actuales, lo que le da un alcance relativamente limitado para tutelar correctamente los derechos de la ciudadanía en la era de la información y las nuevas tecnologías de recolección y procesamiento de datos.
> El Reglamento General de Protección de Datos de la Unión Europea: un referente global.
> El derecho a la protección de los datos personales está relacionado con el derecho a la privacidad, pero sus alcances son distintos. Más de 160 países consagran el derecho a la privacidad en sus constituciones, pero el entendimiento de lo que implica varía de un país

a otro. Los estados miembros de la Unión Europea representan una excepción en este sentido, ya que reconocieron la protección de datos como un derecho fundamental en la Carta de 2001 de la UE.

Por todo lo descrito, el objetivo y fin de la actualización de esta ley de orden público es:

> Garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a 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 autonomía personal con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona (Proyecto de Ley: Reforma Integral a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, 2021).

4.4. Información Prodhab

En la *web* de Prodhab se muestra y pone a disposición del público información relacionada con los procedimientos (denuncias) de protección de derechos de datos, en lo que se observa el estado de la delación, los años, los sectores denunciados, los motivos, entre otros. Esto evidencia la inclinación de las situaciones que se materializan en el ámbito nacional, como se ha comentado en este artículo.

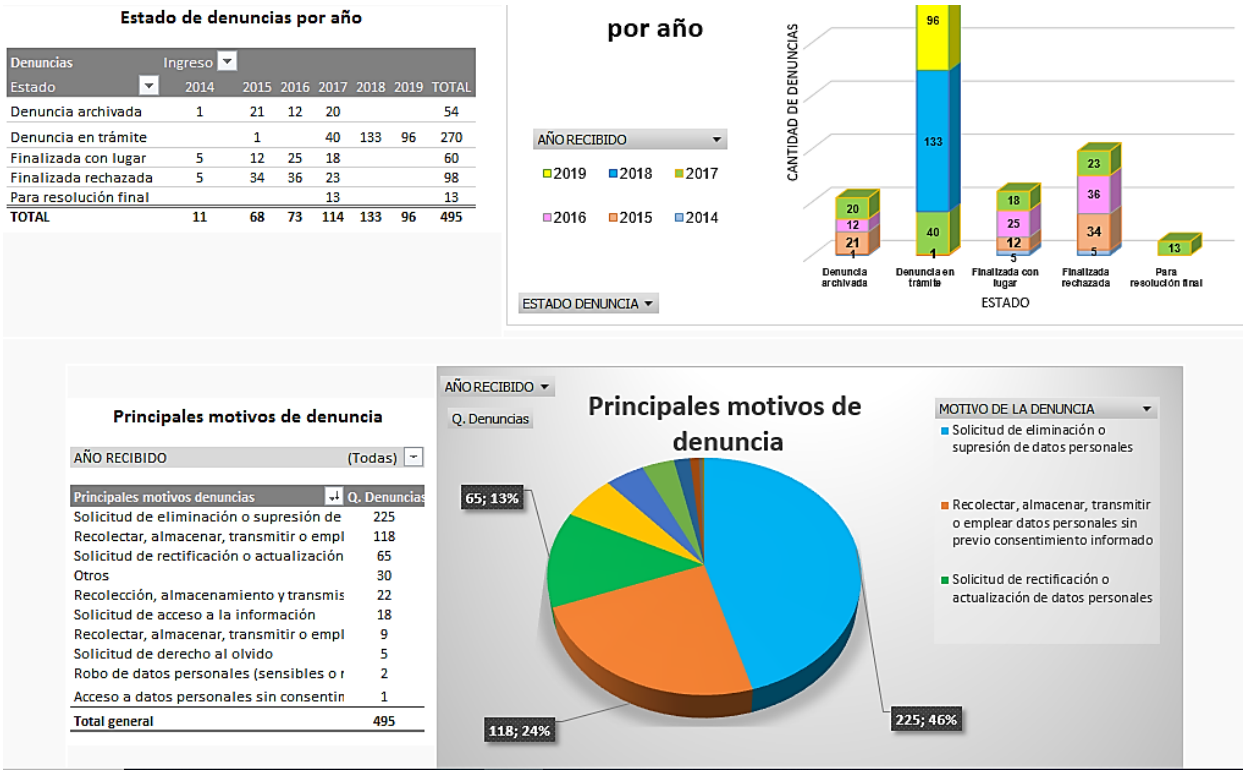

Figura 2
Estado de la delación, años, sectores denunciados y motivos (a)

Fuente: Prodhab (s. f.).

Sector Denunciado

Sector denunciado	Denuncias
Banca y finanzas	132
Varios	59
Comercial	56
Gestionadora de cobro	56
Buró de crédito	30
Gobierno	28
Persona física	22
Telecomunicaciones	19
Salud	17
Bufete/ Firma jurídica	15
Cooperativa	13
SD	13
Medio de comunicación	8
Superintendencia/ Entidad Reguladora	7
Administrador página web y/o app	5
Colegio profesional	3
Seguros	3
Tecnología	3
Fundación/ ONG/ ORG	2
Turismo	1
Bienes Inmuebles	1
Educativo	1
Asociación solidarista	1
TOTAL	**495**

Figura 3
Estado de la delación, años, sectores denunciados y motivos (b)

Fuente: Prodhab (s. f.).

4.5. Reglamentación e información internacional

La información se presenta en los siguientes apartados.

4.5.1. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Esta normativa relata:

> La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades (Reglamento [UE] 2016/679, 2016).

Además, su artículo 1, establece que:

> El Derecho de supresión («el derecho al olvido») 1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo (Reglamento [UE] 2016/679).

4.5.2. Agencia Española de Protección de Datos (AEPD)

Según la AEPD (2021) se destacan los siguientes temas:

> 1. ¿Qué es el derecho de supresión (“derecho al olvido”)?
> Es la manifestación del derecho de supresión aplicado a los buscadores de internet. El derecho de supresión ('derecho al olvido') hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa.
> 2. ¿Puedo ejercerlo frente al buscador sin acudir previamente a la fuente original?
> Sí. Los motores de búsqueda y los editores originales realizan dos tratamientos de datos diferenciados, con legitimaciones diferentes y también con un impacto diferente sobre la privacidad de las personas. Por eso puede suceder, y de hecho sucede con frecuencia, que no proceda conceder el derecho frente al editor y sí frente al motor de búsqueda, ya que la difusión universal que realiza el buscador, sumado a la información adicional que facilita sobre el mismo individuo cuando se busca por su nombre, puede tener un impacto desproporcionado sobre su privacidad.
> 3. Si lo ejerzo frente a un buscador, ¿la información desaparecerá de internet?
> No. La sentencia del Tribunal de Justicia de la UE de 13 de mayo de 2014 determina que sólo afecta a los resultados obtenidos en las búsquedas hechas mediante el nombre de la persona y no implica que la página deba ser suprimida de los índices del buscador ni de la fuente original. El enlace que se muestra en el buscador sólo dejará de ser visible cuando la búsqueda se realice a través del nombre de la persona que ejerció su derecho. Las fuentes permanecen inalteradas y el resultado se seguirá mostrando cuando la búsqueda se realice

por cualquier otra palabra o término distinta al nombre del afectado.

4. ¿Cómo puedo ejercerlo?

La normativa de protección de datos establece que para ejercer el derecho de supresión (y, por tanto, el 'derecho al olvido') es imprescindible que el ciudadano se dirija en primer lugar a la entidad que está tratando sus datos, en este caso al buscador. Los buscadores mayoritarios han habilitado sus propios formularios (Google, Bing o Yahoo!) para recibir las peticiones de ejercicio de este derecho en este ámbito. Si la entidad no responde a la petición realizada o el ciudadano considera que la respuesta que recibe no es la adecuada, puede interponer una reclamación ante la Agencia Española de Protección de Datos. En función de las circunstancias de cada caso concreto, la Agencia determinará si la estima o no. Esta decisión de la Agencia, a su vez, es recurrible ante los Tribunales (s. p.).

4.6. Casos / situaciones en las que se aplica el derecho al olvido

En los siguientes apartados se detallan las situaciones.

4.6.1. Votos de la Sala Constitucional, sobre el derecho al olvido en temas crediticios

En este acápite se habla de datos personales, es decir, aquella información que permite conocer el comportamiento crediticio de una persona como deudora. Por lo tanto, se trata de la información que existe sobre una persona en relación con sus deudas, si estas han sido incumplidas o, por el contrario, han sido canceladas a tiempo.

> La Sala Constitucional ha desarrollado jurisprudencia sobre el derecho de autodeterminación informativa y sobre el "*derecho al olvido*" en materia crediticia, principio al tenor del cual ciertas informaciones deben ser eliminadas de los archivos oficiales transcurrido un determinado tiempo. Al respecto la Sala Constitucional ha establecido un límite de cuatro años para el almacenamiento de datos referentes al historial de incumplimientos crediticios, por lo que es necesario adecuar el plazo de los antecedentes crediticios previstos en el "Reglamento para la Calificación de Deudores" (Voto 8895, 2005).

Además:

> Dicho plazo deberá ser computado a partir del momento en que se declaró incobrable el

crédito, o bien desde que se dio su efectiva cancelación, luego de efectuado un proceso cobratorio. La idea es que dicho término ocurra una vez transcurridos cuatros años a partir del momento en que el crédito en cuestión dejó ser cobrable. De esta forma, se trata de lograr un adecuado equilibrio entre el legítimo interés de las instituciones financieras de valorar el riesgo de sus potenciales clientes y el derecho de la persona a que la sanción por su incumplimiento crediticio no lo afecte indefinidamente, en consonancia con su derecho a la autodeterminación informativa" (Resolución 8894-2005 de 5 de julio del 2005).

4.6.2. El derecho al olvido a favor de las personas objeto de publicaciones periodísticas

En el caso de la notoriedad de un personaje público, esta incide directamente en la actualidad de la información de interés público que se da a conocer. Lo anterior por lo que, si esta información trata acerca de una persona con mucha notoriedad pública, sujeto constante de publicaciones periodísticas a raíz de su cargo, oficio, profesión o carrera, la actualidad de la información dada a conocer pierde relevancia como criterio definidor del interés público.

Por lo anterior, por ejemplo, un excandidato presidencial, un expresidente, un exdiputado, una exestrella de fútbol, entre otros, serán siempre personas de interés público con mayor notoriedad que los demás ciudadanos. Por lo tanto, la información relativa a un acontecimiento o evento no actual, que tiene como personaje principal esta persona con notoriedad pública, será de interés público a pesar de la no actualidad de esta. Por este motivo, es necesario analizar caso por caso, para determinar la importancia de la actualidad del hecho o evento informado, como elemento definidor del interés público (Bolaños Chaves, 2012).

4.7. Casos sobre protección de datos a nivel internacional

Los casos se plantean a continuación.

4.7.1. Caso Cambridge Analytica y Facebook

De acuerdo con el Proyecto de Ley: Reforma Integral a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (2021):

Cambridge Analytica estuvo en el centro del escándalo desde marzo de 2018, cuando los

diarios The Guardian, The New York Times y The Observer, revelaron que la consultora política accedió a los datos personales de 50 millones de usuarios de Facebook sin su autorización, y que fueron usados por la campaña del expresidente de los Estados Unidos, Donald Trump, con una estrategia digital prácticamente idéntica a la ejecutada en el Brexit (Graham y Cadwalladr, 2019).

En este caso el énfasis también estuvo en la política migratoria y en divulgar noticias falsas sobre la candidata demócrata, Hillary Clinton. La revelación la hizo uno de los creadores del sistema, Christopher Wylie, quien relató que los datos surgieron de un test de personalidad desarrollado por el profesor de la Universidad de Cambridge, Aleksandr Kogan, que, como muchas aplicaciones, requería a los usuarios iniciar sesión en Facebook y otorgar algunos permisos de acceso. 270 mil personas hicieron el test, sin saber que al hacerlo estaban autorizando a la aplicación recopilar toda su información y la de todos sus amigos de la red social, sumando alrededor de 87 millones de personas. Tampoco sabían que esa información iba a ser vendida a CA por 800 mil dólares. El ex empleado de CA también reveló que Facebook supo lo que estaba pasando con los datos de sus usuarios muchos meses antes de que fuera divulgado por los medios de comunicación. Fue hasta después del escándalo, y de que las acciones de la red social tuvieran una millonaria caída, que su fundador y CEO, Mark Zuckerberg, reconoció públicamente los fallos en la seguridad (BBC Mundo, 2018).

Tiempo después, la Comisión Federal de Comercio de Estados Unidos ordenó a la red social a pagar US$5.000 millones como sanción por las malas prácticas en el manejo de la seguridad de los datos de los usuarios. En Reino Unido, la red social fue condenada a pagar una multa de 500.000 libras (US $600.000) ante la Oficina del Comisionado de Información del Reino Unido por el mismo caso. La Resolución del Parlamento Europeo contra Facebook, del 25 de octubre de 2018, confirmó que se utilizaron datos personales de forma irregular por parte de Cambridge Analytica, dentro de los que se encontraban los datos de 2,7 millones de ciudadanos de la Unión.

4.7.2. Caso Mario Costeja, el español que venció al todopoderoso Google

Según La Vanguardia (2014):

Este gallego ha logrado que la Justicia Europea sentencie al buscador a eliminar datos que

violen la ley de privacidad.

El Tribunal de Justicia de la Unión Europea (TJUE) reconoció, por primera vez, el denominado “derecho al olvido” en Internet: el derecho a que se elimine de la red una información personal antigua que perjudica a un individuo.

La sentencia de Luxemburgo abre las puertas a que los ciudadanos puedan reclamar a Google y a otros buscadores la eliminación de enlaces que conducen a páginas donde aparece información personal, convirtiéndose en un hito en la defensa de la privacidad.

Es lo que pidió hace ya cinco años Costeja, el abogado español que se convirtió en promotor involuntario del derecho al olvido digital e impulsó, desde un caso personal, el establecimiento de unas reglas del juego para que multinacionales como Google cumplan con la normativa europea de protección de datos.

La corte europea considera que el operador de Internet “es responsable del procesamiento que hace de los datos personales que aparecen en sus páginas web”, incluido el material publicado en medios de comunicación.

“Para Google sigo siendo deudor y casado”, se quejaba Costeja hace unos meses al diario El País. El abogado se había divorciado ya hacía años y sus deudas estaban saldadas, pero su pasado volvía como un fantasma cada vez que introducía su nombre en el buscador.

Todo comenzó en 1998, cuando su nombre apareció en dos anuncios publicados en La Vanguardia como dueño de una propiedad sacada a subasta por un embargo a causa de deudas. El buscador indexó su nombre cuando se digitalizó la hemeroteca y este fue el comienzo de una larga historia, con triunfos, algún que otro revés y, ahora, la victoria definitiva.

En 2009, intentó sin éxito que Google suprimiera el enlace que re direccionaba a esa información. Un año después, la agencia de protección de datos española le dio la razón y ordenó al gigante de Internet su retirada. Pero Google recurrió y la Justicia española remitió el caso al Tribunal europeo.

La multinacional estadounidense, sin embargo, calificó el fallo judicial de decepcionante para los buscadores y en general, para quienes publican contenidos en Internet (s. p.).

Tabla 1
Variables

Variables que se utilizan		
Variable 1	Marco regulatorio	Leyes, reglamentos y normas sobre interés
Variable 2	Narrativa	Conversación con profesor que brinda y colabora con conocimiento en el tema, como guía y aporte de información.
Variable 3	Casos reales	Caso internacional “Mario Costeja”

Tabla 2
Abreviaturas o acrónimos

Nombre	Abre/acron
Costa Rica	CR
Agencia Española de Protección de Datos	(AEPD)
Unión Europea	UE
El Tribunal de Justicia de la Unión Europea	TJUE
Agencia de Protección de Datos de los Habitantes	Prodhab
Uniform Resource Locator	URLs
Internet Of Things	IoT
Tecnologías de información	TI
Macro Datos	*Big data*

Según lo detallado en el acápite de resultados, se puede observar que a pesar cuánto en lo nacional, como en lo internacional, existe normativa y reglamentaciones en relación con el derecho de intimidad y olvido para la protección de datos, nacionalmente estas normas están más enfocadas en situaciones de información sensible, manejada por empresas e instituciones y situaciones crediticitas. Sin embargo, se hacen los esfuerzos para actualizar el cuerpo normativo existente y su aplicación. Asimismo, mantener a la vanguardia con conceptos aplicados en países de Europa, España y otros, que observan muy detenidamente:

> La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales, y que la tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin

> precedentes a la hora de realizar sus actividades (Reglamento general de protección de datos, 2016).

Por consiguiente, se inclinan por llevar a cabo avances que requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta.

5. Discusión

De la información recabada, revisada y analizada se puede afirmar que en el ámbito mundial existen casos que evidencian los riesgos y las consecuencias de la información deliberada que brindamos o que por medio de terceros se ingresa al Internet y a otros medios de comunicación. Los seres humanos han creado la tecnología por años para acortar distancias, estar más cerca de las familias, mejorar la calidad de vida, acelerar tareas, mantenernos informados, entre otros muchos puntos de gran relevancia.

Sin embargo, conforme crece ese desarrollo tecnológico de la mano con mucha información de los usuarios, nos volvemos dependientes de esta, sin dar vuelta atrás, sin detenernos a observar, de manera amplia, los riesgos inherentes a esta innovación. Además, sin percatarnos al menos de que existen personas que podrían utilizar esos datos para beneficio personal o para dañar nuestra imagen. Existen casos populares, como el de Mario Costeja, en el cual:

> El Tribunal de Justicia de la Unión Europea (TJUE) reconoció, por primera vez, el denominado derecho al olvido en Internet: el derecho a que se elimine de la red una información personal antigua que perjudica a un individuo. En este caso, la agencia de protección de datos española le dio la razón y ordenó al gigante Google de Internet la retirada de la información (La Vanguardia, 2014, s. p.).

De igual forma, el de Cambridge Analytic, que:

> Estuvo en el centro del escándalo desde marzo de 2018, cuando los diarios The Guardian, The New York Times y The Observer, revelaron que la consultora política accedió a los datos personales de 50 millones de usuarios de Facebook sin su autorización, y que fueron usados por la campaña del expresidente de los Estados Unidos, Donald Trump (Asamblea Legislativa de Costa Rica, 2021, s. p.).

Estas noticias y casos muestran el gran desafío que implica mantener nuestra intimidad y a la larga que la información pueda eliminarse de las fuentes. En el ámbito nacional se pueden observar situaciones relacionadas con los derechos de intimidad y olvido en los temas crediticios que a pesar de normas y resoluciones establecen plazos para exponer la situación de un ciudadano, muchas entidades no lo eliminan de sus bases, lo que perjudica al particular. Al respecto la Sala Constitucional ha establecido un límite de cuatro años para el almacenamiento de datos referentes al historial de incumplimientos crediticios.

Otros casos son los de las instituciones públicas, que comparten información sensible sin limitarse a la privacidad y derecho de confidencialidad. Al respecto, la Procuraduría General de la República (2002), ha indicado:

> El Derecho a la intimidad como límite del derecho de acceso a la información pública, Límites de acceso a documentos de carácter privado que se encuentren en oficinas públicas, Datos personales, Archivos médicos, Datos privados de funcionarios públicos, Salario neto de funcionarios públicos, Obligación de Administración de proteger datos privados, Fotografía, Comunicaciones de carácter público, Discriminación de información protegida para dar acceso a información pública.

Por lo anterior, los datos íntimos o sensibles, por ejemplo, la orientación ideológica, fe religiosa, preferencias sexuales, entre otros, no son de acceso público.

> El Estado debe procurar que los datos íntimos (también llamados sensibles) de las personas no sean siquiera accedidos sin su expreso consentimiento, tales como su orientación ideológica, fe religiosa, preferencias sexuales, es decir, aquellos aspectos propios de su personalidad, y que como tales escapan del dominio público, integrando parte de su intimidad del mismo modo que su domicilio y sus comunicaciones escritas, electrónicas, y otras (Procuraduría General de República, 2002).

Por lo tanto, como se indicó en párrafos anteriores, la Sala Constitucional se ha encargado de tratar la protección de datos, conceptualizarla y caracterizarla, ante la ausencia de legislación expresa que la regule. Además, define el derecho al olvido como aquel que existe en los casos en los que los datos consignados en las bases de datos no son actuales ni cumplen con la finalidad para la cual

se recolectaron. A partir de esto es necesario indicar que la información debe cumplir ciertos parámetros para que se mantenga en vigencia, como:

> 1.-Actualidad: Los datos de carácter personal deberán ser actuales. El responsable de la base de datos eliminará los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados. 2. Veracidad: Los datos de carácter personal deberán ser veraces. La persona responsable de la base de datos está obligado a modificar o suprimir los datos que falten a la verdad. De la misma manera, velará por que los datos sean tratados de manera leal y lícita. 3.- Exactitud: Los datos de carácter personal deberán ser exactos. La persona responsable de la base de datos tomará las medidas necesarias para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados. 4.- Adecuación al fin: Los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines (Ley 8.968, 2011).

Sin embargo, por mucho tiempo Costa Rica ha mantenido reglamentaciones y normativa que se limita a temas como el derecho a la intimidad, privacidad y olvido en relación con empresas, Sector Público, información crediticia y otros, no directamente enfocándose, de manera amplia, en el tema. Esto según la información recabada de Prodhab, en la que se observa que los temas tratados principalmente en el área de las denuncias consisten en supresión de datos personales, emplear datos sin previo conocimiento, entre otros.

Por lo anterior, las entidades objeto de denuncias han sido bancos, comercio, gobierno, salud, entre otros. Es decir, las regulaciones para el manejo y procesamiento de datos sensibles que fueron considerados en el momento de avanzada carecen de: “Varios conceptos actuales, lo que le da un alcance relativamente limitado para tutelar correctamente los derechos de la ciudadanía en la era de la información y las nuevas tecnologías de recolección y procesamiento de datos” (Asamblea Legislativa de Costa Rica, 2021, s. p.).

Además, es necesario mencionar que el actual Proyecto de Ley denominado Reforma Integral a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, que tiene como objetivo fortalecer ese vacío legal y está alineado con reglamentación europea, plantea que:

> La normativa que ha desarrollado la Unión Europea en materia de protección de datos ha servido de referente en para el resto del mundo, aunque ciertamente desde su aprobación también se han encontrado diversas oportunidades de mejora. En 2016, entró en vigor el Reglamento General de Protección de Datos (RGPD) y fue de aplicación en 2018 y que una de sus virtudes fue el desarrollo de principios claros bajo los cuales debe realizarse cualquier tratamiento de datos personales, comprendiendo así que más allá de la tecnología (Asamblea Legislativa de Costa Rica, 2021, s. p.).

Como se desprende del Proyecto de Ley de marras:

> Ya en la década de los noventa muchos países del mundo contaban con leyes para la protección de los datos personales de sus ciudadanos, esas normativas no contemplaron un contexto como el descrito anteriormente: la era del Big Data y el desarrollo de tecnologías que tienden a que las personas pierdan el control y algunas veces hasta prácticamente la propiedad, sobre sus datos. Costa Rica, en definitiva, no escapa a este panorama (Asamblea Legislativa de Costa Rica, 2021, s. p.).

La reglamentación costarricense tiene áreas de mejora en puntos como:

> Actualización de conceptos base utilizados en la legislación, desarrollo de los principios que rigen el tratamiento de datos personales, así como de los derechos que le asisten a las personas titulares, limitación tajante de las excepciones a la autodeterminación informativa de la persona interesada, y clarificación de las excepciones al consentimiento informado, fortalecimiento institucional de la Autoridad Nacional, la Prodhab, entre otros puntos (Asamblea Legislativa de Costa Rica, 2021, s. p.).

Por lo tanto, se debe ser consciente de que el tema tratado en esta investigación es sumamente amplio y se extiende más allá de nuestras fronteras, sin embargo, se necesita de un plazo mayor para revisar y concluir en grandes rasgos todos sus puntos. Por lo tanto, el factor tiempo es una limitante que inhibe profundizar en el tópico.

En este artículo se llega a conclusiones y hallazgos importantes y, sobre todo, se enriquece el conocimiento sobre lo tratado en el ámbito nacional e internacional y asimilación y desarrollo de este en ambos círculos. Más allá de lo expuesto, se cumple el objetivo de conocer y revisar datos

para entender la importancia de la información de las personas y el trato que pueden darle terceros para fines de conveniencia personal y estratégica sin un debido consentimiento.

6. Conclusiones y recomendaciones

De lo expuesto en este artículo se puede concluir que el ser humano ha desarrollado numerosa tecnología con el propósito de mantener comunicadas e informadas a las personas alrededor del mundo y con esto se ha creado una dependencia a los medios electrónicos y tecnológicos. Por lo tanto, la mayoría de información de cualquier persona la encontramos en estos medios, por lo que se puede afirmar que:

- "Gran parte de los servicios más usados en la red se prestan gracias a la cantidad de información y datos personales que las personas usuarias aportamos" (AEPD, 2021b, s. p.).
- "El Internet y los servicios que a través de ella se prestan se han convertido en un elemento imprescindible para nuestras vidas" (Infante Caballero, 2019, s. p.).
- Se debe concientizar sobre los riesgos que el uso inadecuado de la información puede suponer para nuestra seguridad y privacidad.
- Parte de la ciudadanía pasa desapercibida de los riesgos de la información que ingresa a las redes, aplicaciones de Internet, entre otras, obviando las consecuencias del uso sin autorización.
- La información que se replica en el Internet puede tener vicios, como ser errónea o inexacta y no siempre se garantiza que la misma va a ratificarse con rapidez y agilidad.
- Deben respetarse los datos como lo indican las normas al efecto, en el sentido que estos deberán ser actuales, veraces, exactos y adecuados al fin y el responsable de la base de datos deberá eliminarlos cuando ya estos: "hayan dejado de ser pertinentes o necesarios, en razón de su finalidad para la cual fueron recibidos y registrados. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados de su titular" (Ley 8968, 2011, Art. 9).

- Existen procesos legales, aunque no inmediatos, que pueden liberar o ejercer el derecho de que se olvide esta información, lo que le permite a la persona afectada materializar su derecho a la intimidad y al olvido. Además, hay casos populares en el ámbito mundial que exponen el riesgo del uso de la información como el Caso Cambridge Analytic-Facebook y Mario Costeja.

- El país cuenta con normativa con temas relacionados con la protección de datos, pero estos abarcan una porción limitada del tema tan amplio que desarrolla este tópico. Por ejemplo:

  Establece regulaciones para el manejo y procesamiento de datos sensibles en las bases de instituciones públicas y empresas. Sin embargo, carece de varios conceptos actuales, lo que le da un alcance relativamente limitado para tutelar correctamente los derechos de la ciudadanía (Asamblea Legislativa de Costa Rica, 2021, s. p.).

- Costa Rica, con el propósito de establecer una normativa legal apegada a la actualidad y al nivel de países europeos que poseen normativa con los conceptos y temas modernos, presentó el Proyecto de Ley Reforma integral a la Ley de protección de la persona frente al tratamiento de sus datos personales.

Entre las recomendaciones que se derivan de esta investigación se encuentran las siguientes:

- Es necesario que las personas tomen consciencia de la información que por voluntad propia aportan a las diferentes aplicaciones de Internet.

- Se debe divulgar e informar masivamente sobre la existencia de leyes y normas que permiten ejercer la defensa de los derechos de intimidad, privacidad, olvido, consentimiento y otros, es decir, brindar mayor publicidad.

- Costa Rica debe implementar estrategias para mantenerse en vanguardia con la normativa y métodos que permitan tutelar correctamente los derechos de la ciudadanía en el nuevo mundo de la información y las tecnologías de recolección y procesamiento de datos.

- Desde nuestros hogares debemos empezar a ser conscientes de que la información y el Internet son dos mundos inmensos y que al descuidar lo que editamos o subimos puede cobrarnos una cara factura.
- Asimismo, las leyes han sido creadas por la existencia de necesidad en la sociedad y con el propósito de hacer valer los derechos que en ellas se consagran, por lo que es nuestro deber como ciudadanos ejercerlos por los medios competentes.

Referencias

Agencia de Protección de Datos de los Habitantes. (s. f.a). *¿Quiénes sómos?* http://prodhab.go.cr/quienesomos/

Agencia de Protección de Datos de los Habitantes. (s. f.b). *Datos abiertos*. http://www.prodhab.go.cr/datosabiertos/

Agencia Española de Protección de Datos (AEPD). (2021). *Internet y redes sociales*. https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales

Agencia Española de Protección de Datos (AEPD). (s. f.). https://www.aepd.es/es

Asamblea Legislativa de Costa Rica. (2021). *Proyecto de Ley: Reforma Integral a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales. Alcance n.º 33 de la Gaceta 30 del 12 de febrero de 2021*. https://www.informatica-juridica.com/etiqueta/datos-personales/

BBC Mundo. (2018). *El hombre que obligó a Google a eliminar su pasado criminal del buscador*. https://www.bbc.com/mundo/noticias-43754550

Bolaños Chaves, E. (2012). *El Derecho al Olvido en la Internet, una aplicación a las hemerotecas digitales* (Tesis para optar por el grado de Licenciatura en Derecho). https://iij.ucr.ac.cr/wp-content/uploads/bsk-pdf-manager/2017/10/El-Derecho-al-Olvido-en-la-Internet.pdf

Cijul en línea. (s. f.). https://cijulenlinea.ucr.ac.cr

Comisión Europea. (s. f.). *La protección de datos en la UE*. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es#legislacin

Constitución Política de la República de Costa Rica. (1949). https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=871

Decreto Ejecutivo 37554. (2012). *Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales*. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74352&nValor3=106487&strTipM=TC

Dictamen 123. (2012). Dictamen: 123 del 18/05/2012. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/pronunciamiento/pro_ficha.aspx?param1=PRD&param6=1&nDictamen=17218&strTipM=T

Google. (s. f.). *Retiradas de resultados de búsqueda en aplicación de la normativa europea sobre privacidad*. https://transparencyreport.google.com/eu-privacy/overview

Hernández Valle, R. (s. f.). *Prerrogativa y garantía*. https://books.google.co.cr/books?id=uREZSw2MEcoC&pg=PA74&lpg=PA74&dq=#v=onepage&q&f=false

Herránz, A. (2018). *Unos 65.000 españoles han reclamado a Google su derecho al olvido. El Comercio*. https://www.elcomercio.es/tecnologia/internet/65000-espanoles-reclamado-Google-derecho-olvido-20180305231534-ntrc.html

Infante Caballero, A. (2019). *¿Es legal compartir un contacto en WhatsApp en redes sociales? ¿Es legal que las compañías de redes sociales hagan negocio con nuestros datos?* https://elblogdelabogadoblog.com/2019/10/20/es-legal-compartir-un-contacto-en-whatsapp-en-redes-sociales-es-legal-que-las-companias-de-redes-sociales-hagan-negocio-con-nuestros-datos/

La Vanguardia. (2014). *Mario Costeja, el español que venció al todopoderoso Google*. https://www.lavanguardia.com/tecnologia/internet/20140514/54407896513/mario-

costeja-google.html

Ley 8968. (2011). *Ley de Protección de la persona frente al tratamiento de sus datos personales. La Gaceta nº 170*. https://www.informatica-juridica.com/etiqueta/datos-personales/

Procuraduría General de República. (1994). *Resolución n.º 1026-1994 del 18 de febrero de 199*4. Criterio reiterado.

Procuraduría General de República. (2002). *Resolución n.° 8996-2002 del 13 de septiembre del 2002*.

Procuraduría General de República. (2003). *Resolución n.º 14997-2003 del 17 de diciembre de 2003*.

Procuraduría General de República. (2005). *Resolución n.° 8894-2005 de 5 de julio del 2005*. https://www.pgr.go.cr/wp-content/uploads/2017/05/Comportamiento_crediticio.pdf

Procuraduría General de República. (s. f.). *Derecho a la intimidad*. https://www.pgr.go.cr/wp-content/uploads/2017/05/Derecho_a_la_intimidad.pdf

Reglamento 607. (2006). *Reforma Reglamento para la Calificación de Deudores*. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=58248&nValor3=64382&strTipM=TC

Sala Constitucional. (2004). *Voto 04626*.

Sala Constitucional. (2005). *Voto 8895*.

Salazar Fuentes, M. (2014). *¿Existe una protección real de los datos personales en Costa Rica? Análisis de la Ley 8968 y el habeas data*. Universidad de Costa Rica. http://repositorio.sibdi.ucr.ac.cr:8080/jspui/bitstream/123456789/2297/1/37204.pdf

Scanavino, F. (2012). *Derecho a la intimidad vs Derecho a la información. Antagonismo o complementariedad*. http://www.saij.gob.ar/doctrina/dacf120207-scanavino-derecho_intimidad_vs_derecho.htm

Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*. https://www.boe.es/doue/2016/119/L00001-00088.pdf