Hacia la Sociedad de la Información y el Conocimiento

2022

PROSIC

Programa Institucional
Sociedad de la Información y el Conocimiento

UNIVERSIDAD DE COSTA RICA

Capítulo 7

Hacia el reconocimiento de los derechos digitales en Costa Rica

José Adalid Medrano Melara

El mundo está viviendo una transformación social, sin precedentes, la cual se encuentra impulsada por una reducción de la brecha digital y la pandemia. Esta la cual nos obligó a tener una mayor convivencia en los entornos digitales, los cuales carecen de fronteras en el ciberespacio propiciado por internet. Un espacio interconectado requiere de un constante análisis que tome en cuenta las oportunidades y riesgos que representa para las personas. En dicho espacio las personas a través del uso de herramientas digitales en las cuales requieren se respeten sus derechos, libertades y su dignidad para un libre desarrollo de su personalidad.

Las Tecnologías de la Información y la Comunicación (TIC) tienen la capacidad de darle la posibilidad de violar masivamente derechos fundamentales de los ciudadanos, lo que suele ser aprovechado por gobiernos, organizaciones o empresas, sin que los ciudadanos sean conscientes de que se está dando una afectación e inclusive sin que consideren necesario que se les proteja. Esto se debe a que los procesos de transformación digital que estamos experimentando son tan acelerados que no nos da tiempo de detenernos y evaluar cuáles son las condiciones mínimas que requerimos como sociedad para la interacción digital.

De acuerdo con el Informe Hacia la Sociedad de la Información y el Conocimiento del Programa Sociedad de la Información y el Conocimiento (Prosic) del 2021, el teléfono móvil se encuentra presente en casi la totalidad de los hogares costarricenses (96,3%) y la tenencia de computadora está presente en casi la mitad (48.3%) de estos (Amador, 2021). Esto muestra que nos encontramos en una situación en donde casi toda la población hace usos de la tecnología por lo que podría estar en indefensión debido a la falta de educación sobre cómo protegerse, así como por falta de regulación que le proteja.

Debido a lo anterior, se requiere reconocer como un derecho digital la educación básica sobre cómo estar seguro en estos nuevos entornos en donde nos toca realizar gran parte de nuestras interacciones sociales y laborales. Sin embargo, el camino hacia el reconocimiento de los nuevos derechos digitales requiere un análisis de las amenazas emergentes contra los ciudadanos cuando interactúan con medios tecnológicos, con el fin de que exista una correcta comprensión de los riesgos y las oportunidades, las cuales están estrictamente relacionadas.

El camino más adecuado para incorporar en nuestra regulación estos derechos es a través de un extensivo análisis de riesgos y oportunidades que nos presenta la tecnología, junto con un intenso debate regulatorio que tome en cuenta los avances de otras naciones en esta materia. A este efecto, el presente capítulo pretende analizar los riesgos a los que se expone las personas usuarias en el ciberespacio, con el fin de brindar una guía hacia el reconocimiento de derechos digitales en Costa Rica.

7.1 ¿QUÉ ES UN DERECHO DIGITAL?

Los derechos digitales son aquellos sustentados en la protección de la dignidad, la libertad y las oportunidades de las personas frente a la tecnología, en relación con sus actividades en entornos digitales o el mundo físico. Muchos de ellos se encuentran sustentados en derechos fundamentales reconocidos por distintas constituciones políticas y tratados internacionales, pero principalmente han sido desarrollados por leyes creadas para garantizar su respeto ante las constantes amenazas propiciadas por las TIC.

Con el fin de elevar el nivel de protección frente a la tecnología, diversos autores discuten sobre la necesidad de dotarles de reconocimiento internacional, por lo que se habla de una cuarta ola de derechos humanos que son necesarios para el nuevo mundo digital. En esa misma línea, muchos señalan a **la dignidad digital como el núcleo de estos nuevos derechos**, en donde se busca proteger esta en los nuevos entornos digitales en donde el ser humano tiene presencia. El autor español Moisés Barrio, destaca la importancia de estos derechos para maximizar la calidad de la democracia y los derechos:

> El concepto de «derechos digitales» engloba los derechos de los ciudadanos en el entorno digital, ya sean derechos fundamentales o derechos ordinarios. Esta categoría es especialmente relevante porque **la transformación digital debe tener como principio estructural maximizar la calidad de la democracia y los derechos**. El Derecho tiene que garantizar que estos derechos pueden ejercerse y están asegurados en el entorno digital con la misma eficacia que fuera de él, lo que plantea el problema de cómo protegerlos adecuadamente dadas las especiales características del mundo digital. (Barrio, 2021, p. 207)

Quiere decir que los derechos tradicionales, fundamentales o no, pueden resultar insuficientes para proteger a las personas de los nuevos desafíos que traen las TIC y que los abusos de estas pueden erosionar la democracia, la libertad y la oportunidad de las personas, convirtiéndose en un óbstáculo para su desarrollo presonal, cuando deberían estar ahí para servirles. En este sentido, vale la pena destacar lo que indicaba en 1978 la Ley francesa relativa a la informática, ficheros y libertades sobre cuál debería ser el papel de la informática en la sociedad:

> Art. 1**. La informática debe estar al servicio de todos los ciudadanos**. Su desarrollo debe producirse en el marco de la cooperación internacional. **No debe atentar contra la identidad humana, los derechos humanos, la intimidad o las libertades individuales o públicas**. (Ley № 78-17,1978, artículo 1).

En línea similar la Constitución Española, busca limitar los alcances de la informática con respecto al impacto sobre los derechos fundamentales:

> La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (Articulo 18.4, Constitución Española, 1978).

Si tuviésemos dudas con respecto al carácter visionario del senador constituyente español, el señor Isaías Zarazaga, quien advertía en 1978 de la era de cambios a los que la tecnología emergente sometería a la sociedad:

> «Tenemos que situarnos en el futuro [...] vendrán otras muchas técnicas —no solo la informática—, y resulta imprescindible prevenir y prepararnos para ellas adecuadamente y no quedarnos desplazados en la carrera [...]. **Hay que evitar la traición de la tecnología; hay que arbitrar nuevos sistemas de valores»** (Lombarte, 2020, p. 103).

El legislador español a través de la ley española de protección de datos personales del año 1992, mantiene que la informática genera un impacto que por mandato constitucional debe regular:

> La Constitución española, en su artículo 18.4, emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos.
>
> El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos **ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida**.
>
> Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución[1] y por las leyes que los desarrollan, **la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.**
>
> Ello es así porque, hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. **El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona**.
>
> Uno y otro límite han desaparecido hoy: Las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos.
>
> [...]
>
> **Se hace preciso, pues, delimitar una nueva frontera de la intimidad y del honor una**

1 El artículo 18 de la Constitución Española reza de la siguiente manera:
1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. (Constitución Política, 1978, artículo 18).

> **frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes;** una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley. (Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, España, párr. 1-5 y 7).

La amenaza de la informática sobre distintos derechos fundamentales es un tema actual y el reconocimiento de nuevos derechos digitales a los ciudadanos digitales está pendiente y requiere una discusión profunda. Nuestra Sala Constitucional en 1998, analizó, con gran visión de futuro, el impacto de la informática sobre la vida de las personas:

> Lo que hoy conocemos como "sociedad informatizada" plantea nuevos retos al concepto clásico del derecho a la intimidad. **En la década de los ochenta y noventa, en nuestro país, la libertad individual, la personal y la colectiva, estaban relativamente lejos de la influencia de la tecnología.** Así por ejemplo, el ciudadano no se cuestionaba con qué fin le eran solicitados sus datos personales, quienes tienen acceso a ellos y con cual objeto.
>
> **La informática, no sólo representa uno de los más grandes avances del presente siglo, sino que pone en evidencia las posibilidades de inspección de la vida interior de las personas,** desde este punto de vista**, la personalidad de los ciudadanos y su fuero interno cada vez se hacen más trasparentes**. **Esta situación hace necesario que los derechos fundamentales amplíen también su esfera de protección.**
>
> La esfera privada ya no se reduce al domicilio o a las comunicaciones, sino que es factible preguntarse si es comprensible incluir "la protección de la información" para reconocerle al ciudadano una tutela a la intimidad que implique la posibilidad de controlar la información que lo pueda afectar. (Sala Constitucional, Resolución No 01345-1998).

Como hemos visto, en nuestro país, la Sala Constitucional ha sido punta de lanza y baluarte de los derechos digitales, pero en el siglo XXI el avance tecnológico paulatínamente le ha venido superando, por lo que como sociedad debemos analizar el impacto de la tecnología -presente y futura- sobre los derechos individuales y colectivos, la dignidad y la libertad del individuo; con el fin de propiciar un desarrollo tecnológico que ayude a fortalecer un sistema democrático que garantice oportunidades para todos.

Por lo anterior, para que Costa Rica pueda avanzar hacia un correcto reconocimiento de los derechos digitales, se requiere de la valentía y la constante actualización por parte de los jueces constitucionales, gobernantes, legisladores, academia y sociedad civil. Sin embargo, para dar ese paso la educación no es el único requisito, ya que se requiere una sociedad con pensamiento crítico y visionario para poder anticiparse a distintos escenarios que puede generar la tecnología.

7.2 RIESGOS EN ENTORNOS DIGITALES

El desarrollo tecnológico conlleva oportunidades y riesgos, para los ciudadanos, empresas, organizaciones y gobiernos, por lo que es necesario un constante análisis de las posibilidades de las tecnologías para aprovecharlas de la mejor manera en respeto de los derechos fundamentales de las personas, la libertad y la dignidad del individuo.

Dicho análisis debe aprovecharse para impulsar una política pública más agresiva con respecto a la

educación de toda la población, con el objetivo de construir conocimientos adecuados para aprovechar la tecnología y dotar al individuo de conocimientos digitales que le permitirán prosperar en un mundo digitalizado. De lo contrario, la falta de habilidades tecnológicas y de cultura de respeto de estos nuevos derechos se convertirán en obstáculos para vivir en un mundo que se dirige a entornos que requieren cada vez más de estos conocimientos.

En este apartado realizaremos un análisis de los riesgos emergentes que deben ser tomados en cuenta en este proceso y posteriormente analizaremos el camino que han tomado otras naciones con respecto al reconocimiento de derechos digitales.

7.2.1 El Metaverso

El entorno digital que más titulares está acaparando a nivel mundial -y el que representa mayores riesgos para las oportunidades, vida privada y derechos digitales de las personas- es el metaverso. Al ser un concepto en constante evolución lo vamos a presentar desde la descripción que hacen del mismo distintos autores:

1. "Un metaverso es un entorno donde los humanos interactúan social y económicamente como avatares en un ciberespacio, que actúa como una metáfora del mundo real pero sin sus limitaciones físicas o económicas" (Orellana, 2022, párr. 2).
2. La expresión "metaverso" combina el prefijo griego "meta" -más allá- y del apócope "verso" -derivado de universo- y no es un concepto nuevo: apareció por primera vez en la influyente novela de ciencia ficción "Snow Cash", de Neal Stephenson, en la que un repartidor en la vida real llamado Hiroaki Hiro se transformaba en un guerrero samurai en el ciberespacio. **Tres décadas después, los expertos explican el "metaverso" como un entorno inmersivo tridimensional compartido por múltiples "usuarios", en el que se puede interactuar a través de una interpretación digital de la imagen física, conocida como avatar.** Una "nueva era de internet" a la que se accede a través de las redes sociales, que ya es una realidad en los juegos en línea y que avanza hacia el entorno laboral en busca de sustituir las relaciones físicas por experiencias de realidad virtual y aumentada, y el intercambio económico por las criptomonedas en un espacio de marcos legales difusos, alejado de instituciones y gobiernos. (EFE, 2022, párr. 2-4).
3. "Quizás podamos comprar ropa virtual, vivir en un apartamento virtual, mantener relaciones virtuales o ir a reuniones de trabajo virtuales. Esta es la idea que subyace tras el Metaverso, **la de crear una extensión del mundo real. Una red de entornos virtuales en los que cualquier persona pueda interactuar con otros usuarios y objetos digitales mediante representaciones virtuales de sí mismos. O dicho de otra forma, no utilizaremos Internet... estaremos dentro de Internet.** Será un universo paralelo completamente virtual e inmersivo. Donde eliminaremos cualquier tipo de limitación espacial y donde podremos interactuar de tú a tú con cualquier persona del planeta." Y de una forma cada vez más realista.
4. Porque, si en solo unos años, los **dispositivos de realidad virtual,** como las gafas virtuales, se han perfeccionado tanto que nos permiten sumergirnos en un escenario en tres dimensiones y sentirnos dentro de él; convendría que nos planteásemos hasta qué punto estas tecnologías podrían tener potencial. Al fin y al cabo, **esto es solo el principio**, y todavía queda mucho camino por recorrer. En estos momentos ya se está trabajando en diferentes tecnologías que permitirán -por ejemplo- **leer los movimientos de nuestro rostro**, para que

nuestro avatar gesticule al unísono que nosotros; o unos **guantes que permitirán sentir lo que está sucediendo** en el entorno digital. (Herrera, 2022, párr. 4-5).

5. Técnicamente, el metaverso es una fusión de múltiples tecnologías emergentes como el 5G, la inteligencia artificial (IA), la realidad extendida y los gemelos digitales. El metaverso se apoya en tres elementos clave: presencia, interoperabilidad y estandarización. La «presencia» es la sensación de estar realmente en un espacio virtual, con otros elementos virtuales. Este efecto se consigue con un dispositivo hardware inmersivo habilitado para la realidad virtual, como son unas gafas del tipo de las Oculus de Facebook o las Hololens de Microsoft.
6. La «interoperabilidad» significa poder transitar sin problemas entre espacios físicos y virtuales con los mismos activos virtuales, como los avatares y los objetos digitales. Por ejemplo, la plataforma ReadyPlayerMe permite a los interesados crear un avatar que pueden utilizar en algunos mundos virtuales, incluso en reuniones de Zoom.
7. Mientras tanto, tecnologías como «blockchain», las criptomonedas y los «tokens» no fungibles (los NFT) facilitan la transferencia de bienes digitales a través de los metaversos.
8. La «estandarización» es lo que permite la interoperabilidad de las plataformas y los servicios en todo el metaverso. Se trata de uno de sus mayores desafíos. (Barrio, párr. 11-16).

Como puede verse, a nivel jurídico no es lo mismo analizar el metaverso con la tecnología de los noventa, con la actual o con la que se contará en el futuro. Por esto debe hacerse el difícil ejercicio de futurismo -al menos para los próximos diez años- de cómo será la tecnología que permite el metaverso, ya que para el año 2030 muchos expertos esperan que gran porcentaje de la humanidad participe ya de manera activa en el metaverso.

Y si hacemos este ejercicio, podemos esperar que, si el ser humano interactúa en un entorno con mayores capacidades de generar un espejo con nuestro mundo físico y la posibilidad de capturar mayor cantidad de datos, dentro de las que se encuentran nuestras microexpresiones, emociones y hasta nuestro estado de salud, el asunto requiere un urgente debate regulatorio en busca de proteger la dignidad del individuo en estos entornos.

No es un tema menor que Facebook -una empresa estadounidense, que no se ha caracterizado por ser un defensor de derechos digitales- es quien busca ser quien lidere el salto hacia el metaverso y que en la actualidad es la responsable por todo el posicionamiento que está teniendo el metaverso desde que Mark Zuckerberg presentara sus planes en esta materia:

> Tras tener a casi la mitad de la humanidad pendiente de sus redes sociales, el joven magnate considera que hace falta darle una vuelta de tuerca a su proyecto. El metaverso, aseguró Zuckerberg el jueves en el evento anual de desarrolladores de su empresa, es la evolución lógica de la red, que no da más de sí. Es llevar a Facebook al siguiente nivel. **Hasta ahora, nuestra experiencia en el ciberespacio se limitaba a navegar en webs o manejar aplicaciones.** El mundo digital existía en las pantallas de nuestros dispositivos; al despegar la mirada del móvil o el ordenador, ese mundo se apagaba. **El metaverso es meterse en él. En un universo**, eso sí, diseñado y modelado por Facebook (o Meta), **donde todo lo que veamos, oigamos y toquemos sea una experiencia de realidad virtual**. Un gigantesco desafío tecnológico al que la compañía liga también su futuro financiero. Según Zuckerberg, **este mundo paralelo moverá "centenares de miles de millones de dólares" en los próximos diez años**. Bloomberg Intelligence cifra el ne-

> gocio en unos 800.000 millones para 2024. (Pascual, 2021, párr.1).

Como puede verse, Facebook y otras empresas invierten fuertemente en la tecnología que servirá como base para el desarrollo de un metaverso omnipresente, en el cual su éxito depende de que los ciudadanos del mundo decidan hacerlo parte de sus vidas personales y/o profesionales. A partir de esto deberán someterse a nuevas reglas y cederán algunos aspectos de su vida privada, por lo que la educación de estos y la normativa que rija el metaverso será crucial para que como humanidad demos este paso.

Sin embargo, como sociedad debemos tomar en cuenta que en la actualidad no contamos con educación digital necesaria para tomar decisiones informadas. Por ejemplo, se reporta que el 74% de los españoles piensan que si quisieran podrían borrar toda su huella digital en internet:

> La mayoría de los españoles no son conscientes o no están seguros del control que tienen sobre su presencia en la red o de lo que podrían hacer si quisieran gestionar su identidad digital, y de forma extendida, existe la idea errónea de que la información difundida a través de redes sociales puede eliminarse completamente.
>
> Se trata de las conclusiones de un reciente estudio realizado por la compañía de ciberseguridad **Kaspersky**, 'Right to be Forgotten' (Derecho al Olvido), que se centra la presencia 'online' de los internautas y las consecuencias de huella digital, y en el que han participado más de 8.500 usuarios en once países europeos, incluido España. (Europa Press, 2022).

Tampoco existe una conciencia real de cómo se siguen nuestras huellas en el ciberespacio y la existencia de mercados que lucran con nuestra información personal con fines publicitarios. Por ello, si los distintos gobiernos no educan a sus ciudadanos sobre los derechos digitales y los riesgos en entorno digitales, la población se encontrará nuevamente en desventaja ante una tecnología cuya naturaleza genera mayores capacidades de vigilancia.

7.2.2 ¿Qué es la huella digital del dispositivo?

Nuestros dispositivos tienen información que les hace identificables, lo que facilita el seguimiento de nuestro rastro a través de la red, lo que genera un grave problema para la privacidad global. Debido a esto la Agencia Española de Protección de Datos realizó un estudio en el cual definen el "fingerprinting":

> La huella digital del dispositivo es una recopilación sistemática de información sobre un determinado dispositivo remoto **con el objetivo de identificarlo, singularizarlo y, de esa forma, poder hacer un seguimiento de la actividad del usuario del mismo con el propósito de perfilarlo**.
>
> El Comité Europeo de Protección de Datos, en su documento "Dictamen 9/2014 sobre la aplicación de la Directiva 2002/58/CE a la toma de fingerprinting de dispositivos" asume la definición de la RFC 69732 que define la huella como "**un conjunto de elementos de información que identifica un dispositivo o una instancia de aplicación**".
>
> Dicho en términos más comprensibles, la huella digital del dispositivo es un conjunto de datos extraídos del terminal del usuario que permiten individualizar de forma unívoca dicho terminal. Dado que lo habitual es que las personas no compartan sus equipos, ya sea este un teléfono móvil, tableta, portátil u ordenador de trabajo, **individualizar el terminal supone individualizar a la persona que lo utiliza.** Las entidades que utilizan los mecanismos de huella digital realizan una recopilación sistemática de información de todos los terminales que se conecten a sus

servidores con el objetivo de singularizarlos y poder hacer un seguimiento de la navegación del usuario para construir un perfil.

Contrariamente a lo que pueda pensar, el perfilado no se limita a recopilar y analizar los hábitos de navegación del usuario o las búsquedas que realiza en servidores. **Las técnicas más avanzadas permiten registrar los movimientos que realiza el usuario a través de la página web con el ratón, examinando en que partes de la pantalla se detiene por más tiempo.** Por otro lado, los desarrollos de software para dispositivos, como por ejemplo JavaScript o Flash, facilitan la implementación de procedimientos para recoger información muy concreta del dispositivo, como por ejemplo el modelo de navegador, tipo y versión de sistema operativo, resolución de la pantalla, arquitectura de procesador, listas de fuentes de texto, plugins o dispositivos instalados, direcciones IP, etc. **La combinación apropiada de toda esta información permite confeccionar una suerte de huella digital única del dispositivo que lo singulariza y, por lo tanto, diferencia de forma univoca a cada usuario en internet.** (Agencia Española de Protección de Datos, 2019, pp. 4-5).

7.2.3 Las pujas en tiempo real con su Información personal

Este tipo de subastas llegó al mercado en 2014, con el fin de mejorar la efectividad de la publicidad en línea al permitir mayor precisión a la hora mostrarle anuncios publicitarios en línea. Por esto con algunas aplicaciones que usted tiene instaladas en su teléfono se pueden crear perfiles sobre usted, las cuales se complementan con la información de su navegación para mostrarle publicidad, por lo que cuando llega a un sitio o abre su aplicación se puede dar una impresión que inicia el proceso.

Esto lo detalla Hessie Jones en un artículo para Forbes (2021) quien nos indica que **cuando se carga una impresión en el navegador de un usuario, la información sobre ese usuario y la página en la que se encuentra se transmite a un intercambio de anuncios que permite a los anunciantes pujar en tiempo real por esas impresiones**. Lo que ha hecho que esto sea más atractivo para el anunciante es el proceso de subasta que ha expuesto al anunciante a la información del flujo de ofertas sobre los usuarios, independientemente de que hayan sido el adjudicatario. Estos datos enviados revelan información identificativa de las personas, como la dirección IP, el código postal, la ubicación GPS, el historial de navegación y los identificadores del dispositivo, como el tipo de aparato, la marca, el modelo, el tipo de pantalla, el tipo de conexión, el sistema operativo y la velocidad de la CPU.

Es preocupante comprender, que todos los datos del flujo de ofertas que se intercambien se almacenarán en la base de datos del anunciante y del editor hasta que se eliminen manualmente, lo que como indican en Forbes (2021) la evolución de la publicidad digital ha ido más allá de los principios aceptados para encontrar al cliente adecuado para el producto adecuado hasta la vigilancia absoluta de las personas.

Como lo indica la Electronic Frontier Foundation (2020), Google controla aproximadamente el 62% de los navegadores de móviles, el 69% de los navegadores de escritorio y los sistemas operativos del 71% de los dispositivos móviles del mundo. El 92% de las búsquedas en Internet se realizan a través de Google y el 73% de los adultos estadounidenses utilizan YouTube. Google ejecuta código en aproximadamente el 85% de los sitios de la web y en el 94% de las aplicaciones de la tienda Play. Recoge datos sobre cada clic, toque, consulta y movimiento de los usuarios a partir de todas esas fuentes y más. Como lo indica esta organización norteamericana Google monetiza lo que observa sobre las personas principalmente de dos maneras:

- Utiliza los datos para crear perfiles individuales con datos demográficos e intereses, y luego permite a los anunciantes dirigirse a grupos de personas en función de esos rasgos.
- Comparte los datos con los anunciantes directamente y les pide que pujen por anuncios individuales.

En el caso de las pujas en tiempo real (también conocidas como "pujas RTB"), nos indica la EFF (2020) que los datos de los usuarios suelen pasar por tres niveles diferentes de empresas en su camino desde un dispositivo hasta un anunciante:

1. Las plataformas del lado de la oferta (o SSP) recogen los datos de los usuarios para venderlos.
2. Empresas de intercambio de anuncios organizan subastas entre ellos y los anunciantes.
3. Las plataformas del lado de la demanda (o DSP) "pujan" en nombre de los anunciantes para decidir qué anuncios mostrar a qué personas.

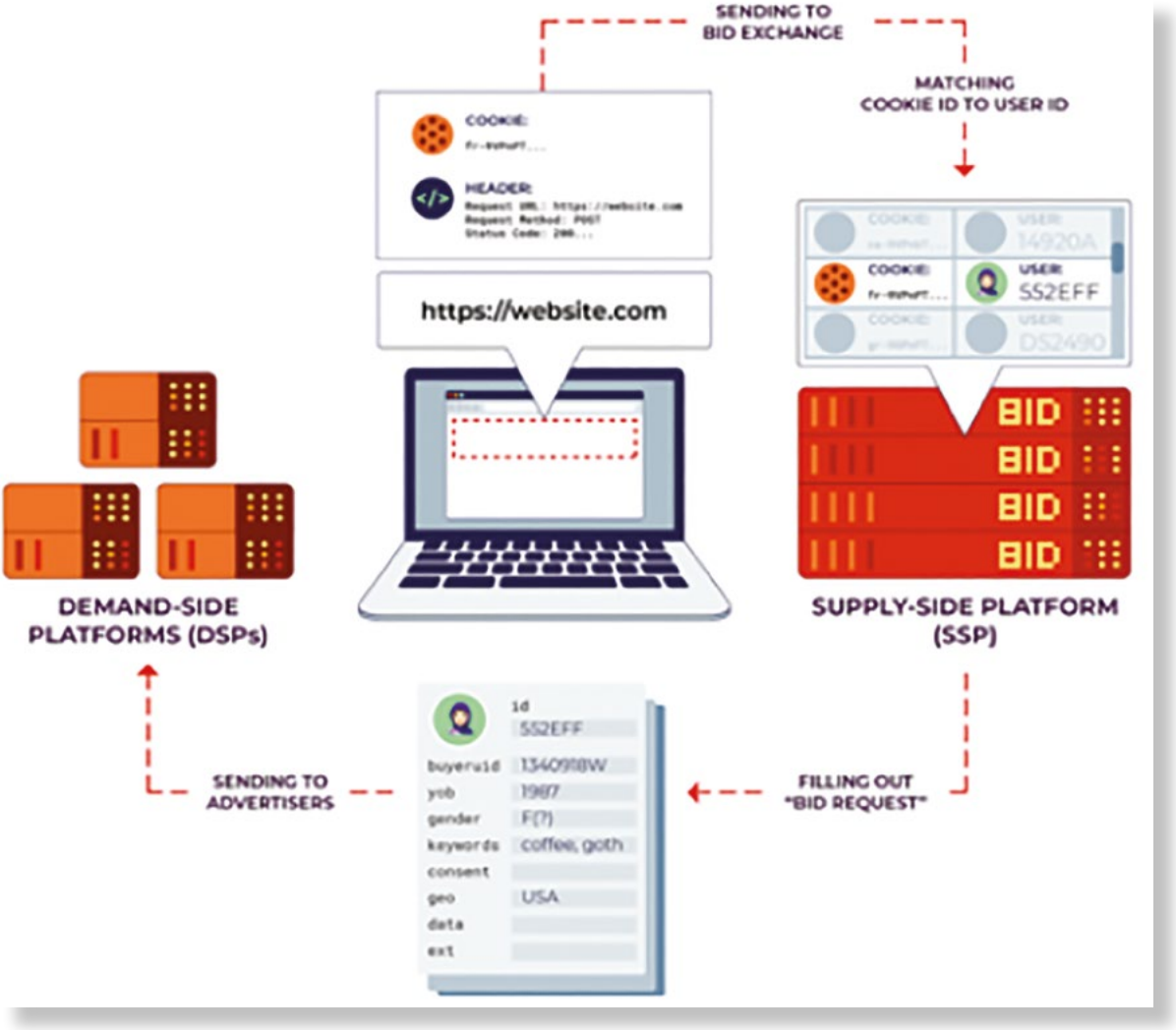


Figura 7.1. Flujos de datos en un sistema típico de pujas en tiempo real

Fuente: EFF, 2020.

Como si esto no fuese suficientemente preocupante, Google a través de su programa de segmentación por lista de clientes (Customer Match) le permite a sus anunciantes subir una lista con los datos que comprenden la huella de un dispositivo para realizar publicidad en entornos digitales distintos. En su sitio web, Google lo explica de la siguiente manera:

> Con la segmentación por lista de clientes, puedes usar tus datos online y offline para llegar a tus clientes y volver a captar su atención en la Búsqueda, la pestaña Shopping, Gmail, YouTube y Display. Con este tipo de segmentación, la información que los clientes te han facilitado se usa para mostrar anuncios a esos mismos clientes y a otros similares a ellos. (Google, 2022).

7.2.4 El impacto de la Subasta en Tiempo Real (RTB) sobre la privacidad

En mayo del 2022, el Consejo Irlandés de Libertades Civiles (ICCL, por sus siglas en inglés), una organización sin fines de lucro que lucha por libertades individuales y derechos humanos desde 1976, presentó un informe llamado "La mayor filtración de datos". La investigación de ICCL refleja escalofriantes datos sobre este mercado de datos, la cual se realiza a través del mecanismo de Subasta en Tiempo Real (RTB, por sus siglas en inglés), que utilizan empresas como Facebook, Google y Microsoft. Este sistema opera de manera sigilosa entre sitios web y aplicaciones, sin que el usuario promedio se percate, ya que no se leen las políticas de privacidad para poder avanzar rápido hacia el contenido.

Esta práctica permite que se rastree todo lo que el usuario mira e inclusive su ubicación. Todos los días estos datos se transmiten entre distintas empresas, con lo cual se puede creer un perfil suyo para fines publicitarios y entre los datos más interesantes del reporte están los siguientes:

- La Subasta en Tiempo Real (RTB) es la mayor violación de datos jamás registrada, rastrea y comparte lo que la gente ve en línea y su ubicación en el mundo real 178 billones de veces cada año en Estados Unidos y Europa.
- De media, una persona en Estados Unidos ve expuesta su actividad en línea y su ubicación 747 veces al día por la industria del RTB.
- 4.698 empresas están autorizadas por Google a recibir datos de RTB sobre personas en Estados Unidos.
- En Europa, el RTB expone los datos de las personas 376 veces al día.
- Google envía 19,6 millones de transmisiones sobre el comportamiento en línea de los internautas alemanes cada minuto que están conectados.
- Los datos privados de los internautas europeos y estadounidenses se envían a empresas de todo el mundo, incluidas Rusia y China, sin ningún medio para controlar lo que se hace después con los datos.
- El sector del RTB generó más de 117.000 millones de dólares en Estados Unidos y Europa en 2021.
- El valor del mercado de RTB (gasto estimado en "publicidad programática") fue de 91.000 millones de dólares en Estados Unidos en 2021 y de 23.000 millones de euros (26.000 millones de dólares) en Europa en 2019.
- Miles de empresas (1.058 en Europa y 4.698 en Estados Unidos) reciben datos RTB de Google.
- Google difunde datos como lo que la gente está viendo o haciendo en un sitio web o una aplicación y su ubicación "hiperlocal " 42.000 millones de veces al día en Europa, o 31.000 millones en Estados Unidos. (Consejo Irlandés de Libertades Civiles (ICCL), 2022).

7.2.5 La vigilancia en línea puede usarse para vigilancia en exteriores

Si los hallazgos de ICCL nos sorprenden, podría generar un impacto mayor el caso de empresas que recopilan fotografías que los usuarios comparten para alimentar una base de datos que tiene fines de identificación biométrica de reconocimiento facial. Este es el caso de la empresa estadounidense ClearView AI que rastrea todas las fotografías que suben los cibernautas en el mundo para venderle esta información a empresas y gobiernos para que puedan potenciar la identificación de personas con las cámaras de reconocimiento facial que se instalan a nivel mundial. Esta tecnología se reportaba en el año 2020 que era utilizada por 2400 policías en todo el mundo:

> El fundador de esta plataforma, cuyo algoritmo permite relacionar una fotografía de una persona con otras imágenes publicadas de esta en varias plataformas de internet —entre ellos imágenes extraídas de Facebook, YouTube y otras plataformas, con lo que podrían haber quebrado sus condiciones de privacidad—, aseguró en esta entrevista que **un usuario de Clearview cuesta unos 2.000 dólares anuales (1.690 euros) y es mayoritariamente utilizada por detectives.** «Son bastante asequibles, comparadas con lo que había antes en el mercado», añadió Ton-That Clearview AI, una pequeña startup fundada en 2017, saltó a la luz pública después de que el New York Times publicara un reportaje en enero de 2020 en el que alertaba de que su tecnología podía ser una amenaza para la privacidad. En **él se explicaba que la herramienta se estaba aplicando combinada con tecnología de realidad aumentada, lo que permitiría a un oficial de seguridad equipado con unas gafas con esta tecnología identificar de forma casi instantánea a una persona con solo verla, e incluso acceder a otros datos**. (Moreno, 2020, párr. 2-3).

La situación es tan grave que empresas como Twitter, LinkedIn, Facebook le han indicado a la empresa norteamericana ClearView AI que deje de extraer información de los usuarios desde dichas plataformas. Como lo reporta The Verge, inclusive varios países ya le han ordenado a dicha empresa borrar la información de sus ciudadanos:

> La polémica empresa de reconocimiento facial Clearview AI ha recibido la orden de eliminar todos los datos pertenecientes a residentes en el Reino Unido por parte del organismo de control de la privacidad del país, la Oficina del Comisionado de Información (ICO). La ICO también ha multado a Clearview con 7,5 millones de libras esterlinas (9,4 millones de dólares) por no respetar las leyes de protección de datos del Reino Unido.
>
> Es la cuarta vez que se ordena a Clearview que elimine datos nacionales de esta manera, tras órdenes y multas similares emitidas en Australia, Francia e Italia.
>
> Clearview afirma que su base de datos de reconocimiento facial contiene unos 20.000 millones de imágenes extraídas de fuentes públicas como Facebook e Instagram. Anteriormente vendía su software a una serie de usuarios privados y empresas, pero recientemente aceptó limitarse en Estados Unidos a venderlo a agencias federales y departamentos de policía tras una demanda presentada por la Unión Americana de Libertades Civiles (ACLU). (Vincent, 2022).

Esta controversial tecnología no solo ha sido utilizada por fuerzas policiales en distintos países del mundo, sino que también ha empezado usarse en la guerra, como es el caso del gobierno de Ucrania:

> El Ministerio de Defensa de Ucrania ha estado utilizando el software de reconocimiento facial Clearview AI desde marzo de 2022 con la intención de verificar crímenes de guerra

mediante la identificación de los muertos, tanto rusos como ucranianos.

El Ministerio de Transformación Digital de Ucrania ha expresado que está utilizando la tecnología Clearview AI para ofrecer a los rusos la oportunidad de experimentar el "verdadero coste de la guerra" y para que las familias sepan que, si quieren encontrar los cuerpos de sus seres queridos fallecidos, serán "bienvenidos a Ucrania". (Romero, 2022, párr. 2-3).

Como puede verse los datos de todo lo que hacemos en línea se vende y puede tener impacto en la seguridad física de la persona, por lo que si este modelo se replica en el metaverso nos encontraríamos ante una circunstancia más grave ya que cuando nuestro avatar se alimenta de nuestros datos podríamos estar transmitiendo más información de la que estamos conscientes. Como se reportó en el artículo el Delito de Violación de Datos Personales para la Revista Tribuna Libre, en nuestro país esta venta de datos es delito, pero es poco lo que se puede hacer desde Costa Rica ante un tráfico de datos de este tipo:

Quiere decir, que conforme se avance en la incorporación de más sensores que alimenten la apariencia y comportamiento de nuestro avatar muchas más utilidades puede representar para una industria que busca sacarle un provecho publicitario a toda nuestra información.

En California, Estados Unidos, siendo conscientes que este es un problema real que se da sin el consentimiento de los usuarios y sin la intención de que se requiera su consentimiento para que funcionen estas subastas se le permite al usuario requerir de forma activa que no se venda su información. En este sentido, la Ley de Privacidad del Consumidor de California de 2018 (C.P.P.A., por sus siglas en inglés) obliga a las empresas que se dediquen a estas prácticas a darle hasta tres opciones de exclusión a los usuarios:

(I) Exclusión global de la venta e intercambio de información personal, incluyendo una dirección para limitar el uso de información personal sensible.

(II) Opción de "Limitar el uso de mi información personal sensible".

(III) Elección titulada "No vender/no compartir mi información personal para la publicidad conductual cruzada". Ley de Privacidad del Consumidor de California de 2018, Estados Unidos, artículo 1798.185. (19.a.iv).

En Costa Rica, por otro lado, desde el año 2012 [2] sancionamos penalmente la violación de los datos personales, mientras en Estados Unidos -que es el país donde residen la mayoría de empresas tecnológicas cuyos servicios usamos- el comercio de los datos personales de los consumidores, inclusive sin su consentimiento, es una práctica permitida. A pesar de lo anterior, estamos lejos de ser una autoridad en esta materia, ya que, a pesar de la estricta regulación, es claro el comercio ilegal de datos personales en nuestro país se hace a vista y paciencia de todos, lo que alimenta el cibercrimen organizado local de estafas informáticas y tradicionales. (Medrano, 2021, p.48)

7.2.6. Ventas de datos personales con fines defraudatorios

La venta de datos personales para la realización de fraudes es una tendencia mundial en donde los mercados negros se alimentan de las constantes brechas de seguridad que se dan en distintos servicios electrónicos, entre otros métodos, se logran identificar.

7.2.6.1 Ventas de tarjetas bancarias

Las tarjetas de crédito de las personas se venden todos los días en internet y los precios no son tan altos

2 *Delito de violación de datos personales, incluido en el Código Penal costarricense a través de la Ley* № *9048.*

como podría pensarse. En un estudio de NordVPN[3] donde se analiza una base de datos correspondientes a 4.47 millones de tarjetas que estaban siendo vendidos en la darkweb[4]. De ese total, se determinó que unos 9393 correspondían a la región centroamericana de los cuales eran tarjetas de Costa Rica, con un costo aproximado de $6.6 por tarjeta y de acuerdo a dicha empresa Costa Rica tiene un riesgo medio, al establecer un índice de riesgo de 0.5, siendo el máximo un 1[5]. Por otro lado, de acuerdo a los números extraídos de esta base de datos, la mayoría de tarjetas que se filtran en Costa Rica son de débito, lo que genera una enorme necesidad de que las personas cuenten con seguros contra este tipo de fraudes.

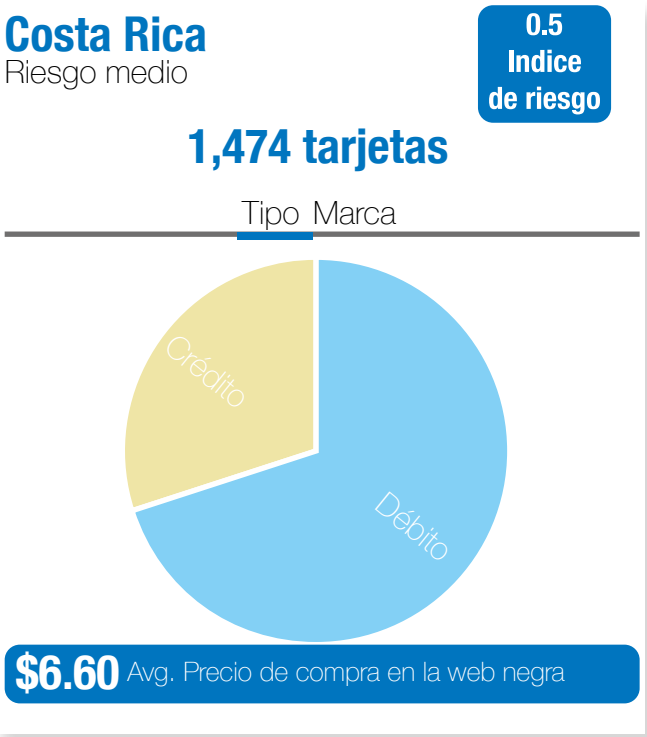


Figura 7.2. Mapa de los detalles de la tarjeta de pago hackeada por NordVPN

Fuente: Tomado de NordVPN.

También es interesante subrayar que la única fuente de la obtención de estos datos no son las filtraciones de bases de datos, sino que también los delincuentes pueden aplicar la fuerza bruta para adivinarlas.

En la región centroamericana, son interesantes los siguientes datos:

1. Guatemala es quien tiene la mayor cantidad de tarjetas filtradas en dicha base de datos,
2. Las tarjetas bancarias de Panamá son las que tienen mayor valor ($18.42, y en su mayoría son de crédito), mientras que las de Honduras son las que menor valor ($0.85 y en su mayoría so de débito).
3. Costa Rica es a la que colocan con el mayor índice de riesgo (0.5).

3 Los datos fueron recopilados por NordVPN en colaboración con investigadores independientes especializados en la investigación de incidentes de ciberseguridad. Evaluaron una base de datos que contenía los detalles de 4.478.908 tarjetas en total, incluyendo detalles del tipo de tarjeta (crédito o débito), banco emisor y si era reembolsable.

4 ¿Qué es la darkweb? La Dark Web es el conjunto oculto de sitios de Internet a los que solo se puede acceder mediante un navegador web especializado. Se utiliza para mantener la actividad de Internet privada y en el anonimato, lo que puede ser útil tanto en aplicaciones legales como ilegales. Si bien algunos la utilizan para evadir la censura del gobierno, también se sabe que se utiliza para actividades altamente ilegales. (Kaspersky, 2022, párr.1). Como lo destacan en Xakata, es el contenido que puedes encontrar en diferentes Darknets, que son cada una de las redes a las que sólo puedes acceder con programas específico. La más popular es TOR, pero también tienes a Freenet, I2P o ZeroNet. Cada una de estas es una Darknet, pero cuando nos referimos a todas en general utilizamos el término Dark Web (Fernández, 2021, párr.7).

5 El Índice de Riesgo fue calculado tomando en cuenta los siguientes elementos: 1) Número de tarjetas en la base de datos per cápita para ese país; 2) Número de tarjetas en circulación para ese país (basado en datos nacionales o regionales de Visa, Mastercard y American Express); 3) La proporción de tarjetas no reembolsables en la base de datos para ese país, con una influencia reducida en el índice general. A continuación, normalizaron logarítmicamente estas cifras para obtener calificaciones escaladas entre 0 y 1.

4. Nicaragua y Belice no aparecen en dicha base de datos, lo que no significa que esos países no cuenten con ese problema, sino que en esta base de datos analizada por esta empresa tecnológica no aparecían.

Tabla 7.1. Resultados del Informe NordVPN en países centroamericanos

	País	Índice de Riesgo	Número de tarjetas filtradas	Tipo de tarjeta bancaria más filtrada	Precio promedio
1	Guatemala	0.4	5106	Débito	$3.56
2	Honduras	0.4	1721	Débito	$0.85
3	Costa Rica	0.5	1474	Débito	$6.6
4	Panamá	0.4	816	Crédito	$18.42
5	El Salvador	0.3	276	Débito	$8.82

Fuente: Tomado del Informe NordVPN.

7.2.6.2 Ventas de datos personales del usuario financiero

Costa Rica tiene su propio cibercrimen organizado vinculado con las estafas informáticas, cuya técnica predilecta es la del phishing[6], *la cual utilizan* para defraudar al usuario financiero nacional. Los delincuentes locales utilizan mayoritariamente las llamadas telefónicas para engañar al usuario, aprovechándose de información de este, no solo de contacto, sino también para generar la confianza sobre la legitimidad de la llamada y de esta manera obtener la información confidencial. Por lo anterior, requieren información proveniente de diferentes fuentes, no solo bancarias, pero que las autoridades judiciales ya están investigando:

> La compra de bases de datos con información personal de clientes bancarios permite a los estafadores tener todas las herramientas necesarias para crear confianza con sus potenciales víctimas, todo esto con el fin de saquearles las cuentas.
>
> El Organismo de Investigación Judicial (OIJ) ha detectado, **por medio de diversas investigaciones, que los documentos que llegan a manos de los delincuentes son tanto lícitos**

6 El phishing es una de las estafas más antiguas y mejor conocidas de Internet. Podemos definirlo como un tipo de fraude en las telecomunicaciones que emplea trucos de ingeniería social para obtener datos privados de sus víctimas. Un ataque de phishing tiene tres componentes: 1) El ataque se realiza mediante comunicaciones electrónicas, como un correo electrónico o una llamada de teléfono, 2) El atacante se hace pasar por una persona u organización de confianza y 3) El objetivo es obtener información personal confidencial, como credenciales de inicio de sesión o números de tarjeta de crédito.
Este es el engaño del que el phishing obtiene su nombre: el ciberdelincuente sale de «pesca» («fishing», en inglés, con la misma pronunciación que «phishing») con un «cebo» atractivo para ver si alguna víctima pica en el vasto «océano» de los usuarios de Internet. Las letras ph de «phishing» proceden de una afición de mediados del siglo XX, el llamado «phone phreaking», que consistía en experimentar con las redes de telecomunicaciones para averiguar su funcionamiento. Phreaking + fishing = phishing. (Belcic, 2020, párr.1-3).

> **como ilícitos.** Sin embargo, hasta ahora desconocen cuánto pueden pagar los hampones para obtenerlos. (Jiménez, 2022, párr.1-2).

Los ataques de phishing han resultado ser efectivos con usuarios con escasos conocimientos sobre ciberseguridad por lo que es importante que el sector bancario les proteja con tecnologías algoritmos inteligentes que aprovechen los datos en su poder. En ese sentido es revelador el informe de la Organización de Estados Americanos (OEA) con respecto a la Ciberseguridad en el Sector Bancario en América Latina y el Caribe:

> Resulta significativo que **el 49% de las entidades bancarias aún no están implementando herramientas, controles o procesos usando Tecnologías Digitales Emergentes, tales como Big Data, Machine Learning o Inteligencia Artificial**, las cuales resultan muy importantes a la hora de prevenir ciberataques o **determinar patrones sospechosos asociados a fraude, entre otras capacidades de detección**. (OEA, 2018, p.8).

Lo anterior es importante para proteger al usuario financiero aun cuando este caiga ante un *phishing*.

7.3 LA AMENAZA DEL RANSOMWARE

Después del ataque de ransomware que sufrió el país a inicios de año, este es un aspecto al que se le debe prestar atención porque este tipo de ciberdelitos no solo afectan la integridad de la información, sino que también su disponibilidad y confidencialidad. A nivel global este es un tema que debe verse con detenimiento ya que cada vez que una organización es afectada hay datos que pueden ser publicados y ser utilizados con fines delictivos por ciberdelincuentes de diferentes áreas. En un informe de Sekoia (2022) se reporta que al menos 88 países se vieron afectados en todo el mundo, con las tasas más altas en América del Norte (incluyendo el 37% de las víctimas reveladas ubicadas en los EE.UU.), y Europa. De acuerdo con Sophos (2022), en su reporte **El Estado del Ransomware 2022**, el 66% de las organizaciones fueron atacadas por ransomware en el último año, frente al 37% que lo fueron en el año 2020. Lo anterior supone un aumento del 78 %, lo que demuestra que los adversarios se han vuelto considerablemente más capaces de ejecutar los ataques más importantes a escala. De este informe podemos extraer importantes datos sobre el año 2021:

- 65% resultados en encriptación de los datos. En el 2020, solo el 54% de los casos los ciberdelincuentes lo lograban con éxito.
- 4% de casos donde los delincuentes extorsionaron a la empresa bajo la amenaza de publicaron la información, aunque no encriptaron los datos. En el 2020, esta cifra era de un 7%, lo que representa una reducción en este método.
- 72% de las organizaciones experimentó un incremento en el volumen, complejidad e impacto de los ciberataques.
- 99% de las organizaciones lograron recuperar alguna de la información encriptada. Los respaldos son el método más efectivo para esto (73%).
- 46% de las organizaciones realizó algún pago al grupo cibercriminal. De media, las organizaciones que pagaron solo recuperaron el 61% de sus datos, frente al 65% de 2020. Asimismo, solo el 4% de las que pagaron el rescate recuperaron TODOS sus datos en 2021, frente al 8% de 2020.
- 90% de los ataques lograron afectar la operación de la organización. Y un mes es el promedio de recuperación luego de un ataque.

A esta industria cibercriminal se le debe dar constante seguimiento ya que cada grupo que aparezca puede tener formas de operar que deben ser estudiadas para

prevenir ataques. En ese sentido, Sekoia (2022) reporta que en el primer semestre de 2022 aparecieron 20 nuevos grupos de ransomware e inclusive se sospecha que algunos grupos son marcas nuevas, como Axxes (de Midas, según Cloudsek) y Pandora (de Rook, según Cyble), o bien nuevas variantes de familias de ransomware existentes, como YourCyanide, Yashma y Onyx. De interés para Costa Rica sería la nueva marca Black Basta, la cual ha suscitado dudas entre los analistas de amenazas sobre su posible vinculación con Conti, la cual atacó a Costa Rica.

7.3.1. Los grupos de ransomware utilizan nuevas formas de extorsión

De acuerdo con Sekoia (2022) los grupos de ransomware mejoran constantemente sus técnicas para añadir presión y hacer que la víctima pague el rescate. Por ejemplo, el grupo cibercriminal ALPHV/BlackCat comenzó a publicar los datos que robaron a una empresa no sólo en su sitio web en la *darkweb*, sino también en un sitio web accesible por cualquiera, el cual estaba específicamente diseñado con un dominio denominado según el nombre de la víctima. En dicho caso, el ransomware incluía un formulario de búsqueda, lo que permitía a los empleados o clientes buscar directamente si aparecían en la filtración, lo que eleva el nivel de presión.

7.3.2. Riesgos en el teletrabajo

Con esta modalidad de trabajo se generan riesgos para los derechos de los trabajadores, pero también para los intereses de las empresas debido a que los entornos de los hogares pueden estar menos protegidos.

Vigilancia al trabajador desde la casa

Con los empleados teletrabajando se eleva la tentación para los empleadores de utilizar las facilidades de las nuevas tecnologías para monitorearles y verificar que se encuentren realizando su trabajo. En Reino Unido, el sindicato Prospect (2022) denuncia que se ha elevado la cantidad de empleados que están siendo vigilados ilegalmente mientras trabajan. En una encuesta que realizaron llegaron a las siguientes conclusiones:

1. **El uso de la tecnología de cámaras para vigilar a las personas que trabajan desde casa se ha duplicado,** según los datos: el 13% de los trabajadores a domicilio están siendo vigilados por cámaras, frente al 5% de hace seis meses.
2. **Los trabajadores más jóvenes son mucho más propensos a ser vigilados que sus colegas de más edad**, según el sondeo: casi la mitad (48%) de los encuestados de entre 18 y 34 años dijeron que eran vigilados en el trabajo.
3. **El 52% opina que el uso de cámaras web para vigilar a los trabajadores a distancia debería estar prohibido. Un 28% considera que esta práctica debería estar** fuertemente regulada y sólo el 8% de los trabajadores piensa que los empresarios deberían poder decidir unilateralmente cuándo utilizar las cámaras para vigilar a las personas que trabajan en su propia casa.

La seguridad en la casa puede ser deficiente

Los teletrabajadores pueden poner en riesgo la información de sus patronos, no solo porque las redes internas de las casas no están debidamente aseguradas, sino también porque pueden saltarse protocolos de seguridad de la información en el trabajo.

> Un estudio de Goshred detectó que el 66% de los teletrabajadores corren el riesgo de infringir el Reglamento General de Protección de Datos de la Unión Europea[7] al imprimir

7 Para cumplir con dicha normativa las empresas que tratan datos personales deben tener un proceso eficaz, documentado y auditable para la recopilación,

información confidencial personal en sus casas. Como lo indica Hill (2021), para InfoSecurity Magazine, entre estos documentos se incluyen notas y órdenes del día de reuniones (42%), documentos internos como manuales de procedimientos (32%), contratos y documentos comerciales (30%) y recibos y formularios de gastos (27%).

Debido a la falta de medidas de seguridad, inclusive, como reportó el New York Times, grupos criminales han dirigido sus ataques de manera específica contra teletrabajadores, durante la pandemia, e intentando entrar en sus redes con malware destinado a paralizar sus operaciones (Sanger, 2020, párr. 2).

Amenazas a la democracia a través de la creación de leyes sobre delitos informáticos que pueden restringir la libertad de expresión

A nivel internacional se han visto avances regulatorios vinculados con las TIC que pueden convertirse en serias amenazas para las libertades individuales y la democracia. De manera especial algunas representan graves riesgos a la libertad de expresión, al poder ser utilizadas para limitar a disidentes de un gobierno de poder expresarse en el ciberespacio. Ejemplos de esto se pueden observar en el accionar de gobiernos de países como Rusia, Nicaragua y El Salvador.

En el caso de Rusia, se aprobó en el año 2019 una regulación que viene a sancionar noticias falsas, que tres años después fue utilizada para controlar la información relacionada con la invasión a Ucrania:

> El parlamento ruso dio el primer paso para aprobar dos normas que **prohíben la "falta de respeto"** a las autoridades y la difusión de lo que el gobierno considera como **"noticias falsas".**
>
> La primera prohibición se refiere a la "falta de respeto evidente" al Estado, sus funcionarios y la sociedad rusa, y los delincuentes reincidentes se enfrentan a una pena de **hasta 15 días de cárcel.**
>
> El segundo proyecto de ley prohíbe distribuir "información falsa de interés público, compartida bajo el pretexto de noticias falsas", informó la agencia estatal de noticias TASS. (BBC News, 2020).

De manera similar, Nicaragua dentro de la legislación sobre delitos informáticos, sancionó a su vez las noticias falsas:

> El Gobierno de Daniel Ortega sigue avasallando la libertad de expresión en Nicaragua. Este martes, el Parlamento leal al sandinismo aprobó la denominada Ley Especial de Ciberdelitos, cuyo objetivo principal es la criminalización de publicaciones en medios de comunicación independientes y redes sociales de contenido considerado por el Gobierno como falso con penas de cárcel que oscilan entre uno y diez años. La normativa, conocida como *ley*, no solo afecta a periodistas, sino también a cualquier ciudadano que vierta críticas contra la Administración de Ortega en plataformas digitales. La Ley Especial de Ciberdelitos es parte de un tridente legislativo promovido por el régimen de Ortega y que, según sus críticos, está ideado para acallar las voces disidentes que denuncian las constantes violaciones de derechos humanos que se cometen en este país centroamericano. Lo que más ha llamado la atención con la aprobación de la ley de ciberdelitos es que es el mismo Gobierno quien determinará cuándo un periodista, medio de comunicación o un ciudadano publique una noticia falsa (Miranda, 2020)

Por otro lado, El Salvador, tan solo dos años después, aprobó una ley que ha sido señalada como mordaza. No solo se le acusa de utilizar lenguaje

el almacenamiento y la destrucción de la información personal.

ambiguo, que en un país con una institucionalidad débil puede utilizarse en contra de periodistas, sino que también permite medidas cautelares que pueden censurar sitios web, por lo que distintas organizaciones internacionales que defienden los derechos digitales le hicieron una carta abierta al presidente salvadoreño refiriéndose a esta reforma.

> La ambigüedad, imprecisión y amplitud de las reformas puede favorecer el abuso y la criminalización de actividades en ejercicio legítimo de derechos, así como poner en riesgo la privacidad y la libertad de expresión en el país, con graves consecuencias para su democracia. En un contexto en que hemos conocido situaciones de vulneración grave de derechos mediante la instalación de malware para la vigilancia de activistas y periodistas, cualquier reforma legislativa debe apuntar a mejorar las garantías de protección, defensa, debido proceso y acceso a la información y no aumentar las capacidades estatales para perseguir actividades legítimas mediante la vigilancia.
>
> Por un lado, las reformas a la Ley de Delitos Informáticos y Conexos son imprecisas y deficientes en técnica legislativa. Uno de los artículos criminalizaría la mera obtención y transferencia de información considerada confidencial (artículo 25), estableciendo una sanción de 5 a 8 años de prisión. La medida pone en riesgo el ejercicio periodístico, la libertad de expresión, así como la protección de empleados de gobierno qué revelan irregularidades en el gobierno (…)
>
> La norma permitiría de manera amplia que el Ministerio Público solicite medidas cautelares al juez competente, consistente en el bloqueo de sitios, redes sociales y plataformas digitales de cualquier persona natural o jurídica en la fase de instrucción del proceso penal, sin hacer referencia expresa al deber de ponderar la necesidad o proporcionalidad de esa medida en casos concretos (Derechos Digitales, América Latina, 2022, párr. 3-5).

Todo lo anterior es sumamente grave, ya que impone límites a la libertad de prensa, la cual puede requerir alimentarse de información confidencial para hacer denuncias de interés público que pueden afectar al gobierno, lo que se debería poder hacer, sin tener que preocuparse porque le denuncien penalmente. La inseguridad jurídica que tendría un periodista en ese contexto se agrava cuando se ha acusado al gobierno salvadoreño de utilizar programas informáticos maliciosos para vigilar periodistas pertenecientes a medios no afines al gobierno. Estas acusaciones han sido confirmadas por organizaciones internacionales como Amnistía Internacional:

> Amnistía Internacional (AI) indicó este miércoles (12.01.2022) que verificó el "uso del programa Pegasus para vigilancia de periodistas" y activistas de derechos humanos en El Salvador.
>
> "Una investigación conjunta de Access Now y Citizen Lab ha identificado el uso a gran escala del programa espía Pegasus de NSO Group contra periodistas y miembros de organizaciones de la sociedad civil en El Salvador", dijo el organismo en un comunicado de prensa.
>
> La fuente añadió que "expertos técnicos del Laboratorio de Seguridad de Amnistía Internacional han revisado el informe y verificado de forma independiente las pruebas forenses que demuestran el uso abusivo de Pegasus en el país (…)
>
> El informe de Citizen Lab asegura que logró confirmar "35 casos de periodistas y miembros de la sociedad civil cuyos teléfonos se infectaron con éxito con el software espía Pegasus de NSO entre julio de 2020 y noviembre de 2021" detalló que "los objetivos

> incluyeron periodistas de El Faro, GatoEncerrado, La Prensa Gráfica, Revista Digital Disruptiva, Diario El Mundo, El Diario de Hoy y dos periodistas independientes", además de miembros de las organizaciones Fundación DTJ, Cristosal y otra ONG. (DW, 2022, párr. 2-5)

Como si lo anterior no fuese lo suficientemente grave, la reforma sobre delitos informáticos permite imponer medidas cautelares para bloquear sitios web que transmitan información cuando el Estado considere que incurre en algún hecho delictivo. Esto resulta problemático cuando se combina con tipos penales abiertos que pueden servir para abrir causas contra periodistas y eliminar contenido disidente. En la práctica se crean herramientas que pueden servir como una especie de muro informativo que controla la información que recibe el pueblo salvadoreño, siendo en pequeña escala lo que pasa en naciones como China.

La experiencia sobre la supuesta "Ley Mordaza" sobre delitos informáticos en Costa Rica

No debemos olvidar que en nuestro país se acusó al gobierno de Laura Chinchilla de impulsar una "ley mordaza" (Ley №9048). A diferencia de los casos anteriores, la crítica se basaba principalmente en desafortunadas imprecisiones de la ley que junto con el desconocimiento en derecho penal informático de la prensa, dio la receta perfecta para la desconfianza. En ese sentido, el Dr. Marlon Mora, en nombre del Colegio de Periodistas, uno de los principales detractores de la norma, en una mesa redonda sobre este proyecto de ley, organizada por el Programa Sociedad de la Información y el Conocimiento de la Universidad de Costa Rica (PROSIC), manifestó lo siguiente:

> Para el Dr. Mora, Costa Rica es un país democrático donde el uso de los secretos de Estado debería ser limitado para asegurar la transparencia política. Además, la Ley de Delitos Informáticos debería armonizar el término de informaciones secretas políticas con el de secretos de Estado que se presenta en la Constitución Política.
>
> "A mí me preocupa muchísimo que al final una interpretación que hacen los comunicadores al respecto de la ley, permita que nosotros apliquemos una autocensura y un temor a seguir investigando sobre temas específicos en el caso que caigan en esas tres palabras (informaciones secretas políticas)", mencionó el periodista. (Velázquez, 2012, párr. 14-15).

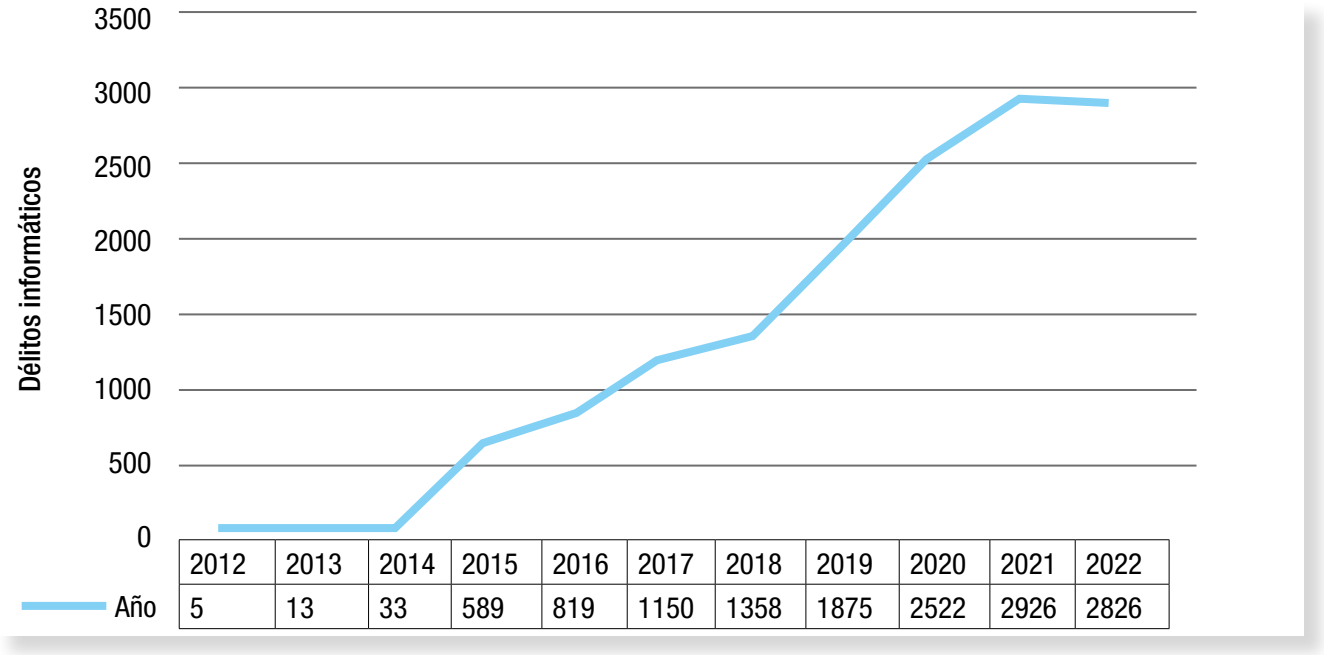
Pocos meses después de dicho evento, principalmente debido a la presión de los medios de comunicación y otros actores, se logró realizar una reforma relámpago (Ley №9135), que vino a corregir el error que contenía el Código Penal de 1970. Además, se realizaron reformas en temas de libertad de expresión que le brindan mayor seguridad jurídica a los periodistas en su trabajo, que a diferencia del caso salvadoreño y nicaragüense, pueden hacer uso de contenidos obtenidos de ilícitos penales informáticos, si la publicación de los mismos tiene un interés público.

Quiere decir que la democracia costarricense permitió el escenario donde libremente se expusieran puntos de vista y más allá de cuál era el criterio técnico más acertado, se realizó una reforma que vino a traer tranquilidad a los medios de comunicación, lo que terminó fortaleciendo la democracia misma.

Eso sí, esto nos deja la experiencia que cuando se trata de reformas vinculadas con las Tecnologías de la Información y la Comunicación (TIC) **hay que hacer una consulta extensiva a la sociedad civil, academia y empresas tecnológicas, y generar mesas de conversación para escuchar el criterio de profesionales en comunicación, ciberseguridad, derecho informático y de profesiones afines**.

7.4 EL AUMENTO DE LOS DELITOS INFORMÁTICOS EN COSTA RICA

La denuncia de los delitos informáticos se ha incrementado de manera importante en los últimos siete años, en donde solo la mitad del año 2022 ya casi se ha logrado a la totalidad cometida desde el año pasado. Los datos estadísticos que se reflejan a continuación son tomados del informe estadístico que brinda el OIJ con respecto a denuncias recibidas, el cual presenta diferencias con respecto a la información que maneja el Ministerio Público, como se verá más adelante.



	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Año	5	13	33	589	819	1150	1358	1875	2522	2926	2826

Figura 7.3. Denuncias de delitos informáticos en Costa Rica 2012-2022

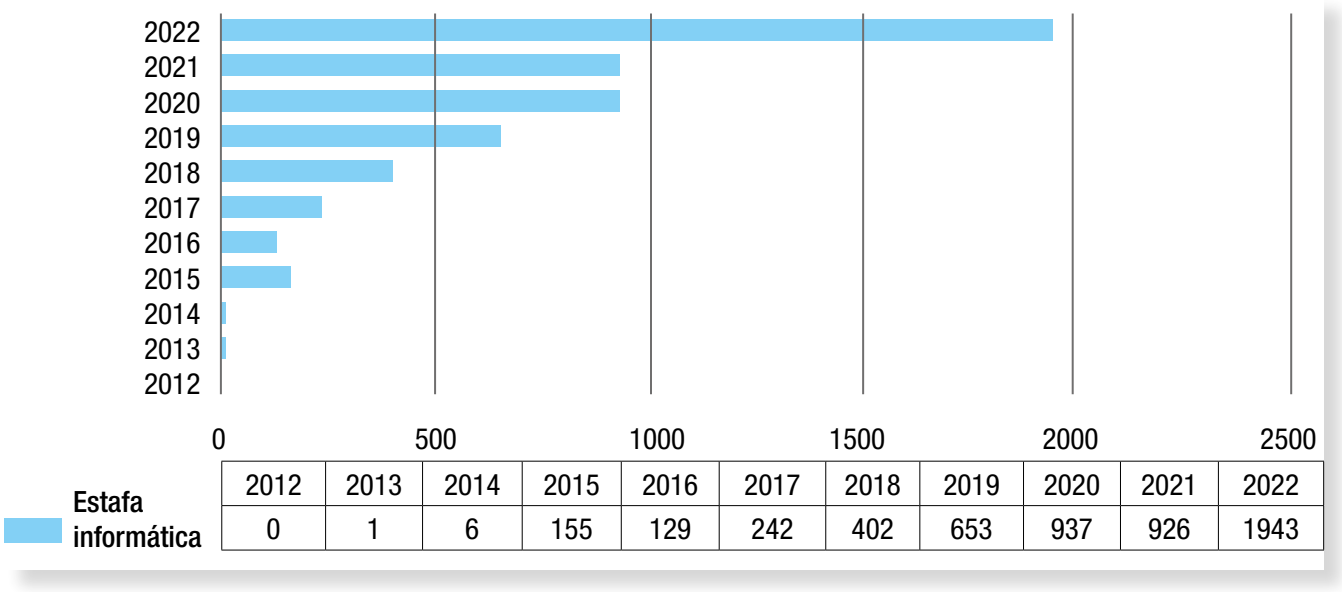
Fuente: Solicitud de información 1182-OPO/UAC/S-2022. (Desde el año 2012 hasta el 30 de junio del 2022)

Con respecto al cómputo de las estadísticas sobre cibercrimen el país presenta grandes problemas que inclusive fueron señalados por el Consejo de Europa al evaluar al país en esta materia en el año 2018:

> La identificación y control estadístico de los procedimientos relacionados con la investigación del ciberdelito constituye un factor esencial de cara a conocer cuáles son las tendencias de este fenómeno criminal. El establecimiento por parte de los Estados de sistemas adecuados para el registro, producción y puesta a disposición de los datos sobre cibercrimen, constituye un factor esencial para, a partir de su análisis, combatir de forma más eficaz estos delitos, como se viene afirmando reiteradamente desde distintas Instancias dedicadas a la prevención y lucha contra la ciberdelincuencia. Costa Rica, como otros muchos países de la región, **no dispone de un sistema de registro integrado que permita cruzar datos entre las distintas instituciones encargadas de investigar el ciberdelito, reflejando de forma global y única la incidencia de la ciberdelincuencia dentro del país**. (Consejo de Europa, 2018).

7.4.1 La estafa informática es la reina de los delitos informáticos

En Costa Rica, el delito informático que más se denuncia es el de la Estafa Informática, el cual por sí solo representa el 38% de todas las denuncias relacionadas con esta clase de delitos. Lo anterior, es revelador si tomamos en cuenta que muchas de las denuncias por suplantación de páginas electrónicas (5%), suplantación de identidad (28%), instalación o propagación de programas informáticos maliciosos (2%), facilitación del delito informático (3%) y la difusión de información falsa (5%) por un error al recibir la denuncia podrían ser también estafas informáticas. Lo anterior es parte del problema señalado al inicio de este apartado y es un elemento que debe solucionarse para contar con mejores datos para luchar contra este flagelo.



2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
0	1	6	155	129	242	402	653	937	926	1943

Figura 7.5. Denuncias por estafa informática en Costa Rica (2012-junio del 2022)

Fuente: Solicitud de información 1182-OPO/UAC/S-2022.

Las estadísticas de denuncias sobre delitos informáticos por poco más de una década (2012-2022) son:

Tabla 7.2. Delitos informáticos en Costa Rica (2012-2022)[8]

	Delito	Denuncias (2012-2022)	Denuncias (2017-2022)	Denuncias (2020-2022)
1	Estafa informática	5394	5103	3806
2	Suplantación de identidad	4003	3504	2133
3	Difusión de pornografía infantil	1383	1164	579

8 Hasta el 30 de junio del 2022.

	Delito	Denuncias (2012-2022)	Denuncias (2017-2022)	Denuncias (2020-2022)
4	Difusión de información falsa	706	567	371
5	Suplantación de páginas electrónicas	643	539	
6	Espionaje informático	439	412	302
7	Facilitación del delito informático	424	419	245
8	Seducción o encuentros con menores por medios electrónicos (Child Grooming)	396	332	147
9	Instalación o propagación de programas informáticos maliciosos	224	220	206
10	Sabotaje informático	175	140	73
11	Daño informático	119	97	54
12	Fabricación, producción, o reproducción de pornografía infantil	86	73	43
13	Producción de material audiovisual (acoso callejero)	37	37	37
14	Tenencia de material pornográfico	22	17	9
15	Captación indebida de manifestaciones verbales	5	5	1

Fuente: Solicitud de información 1182-OPO/UAC/S-2022.

7.4.2. Explosión de las estafas informáticas en Pandemia

Las estafas informáticas tuvieron una explosión durante la pandemia (2020-2022), ya que durante este período se realizaron 3806 denuncias al OIJ, lo que corresponde al 71% de las que se han recibido desde el año 2012 sobre este delito. Este incremento tan exponencial se ha venido presentado en los últimos cinco años, con un incremento importante antes y durante la pandemia. De acuerdo con las estadísticas que el Ministerio Público maneja el impacto del cibercrimen organizado de estafas informáticas es todavía más grave de lo que reflejan las estadísticas del OIJ, ya que solo en el año 2021 manejaron 9800 causas.

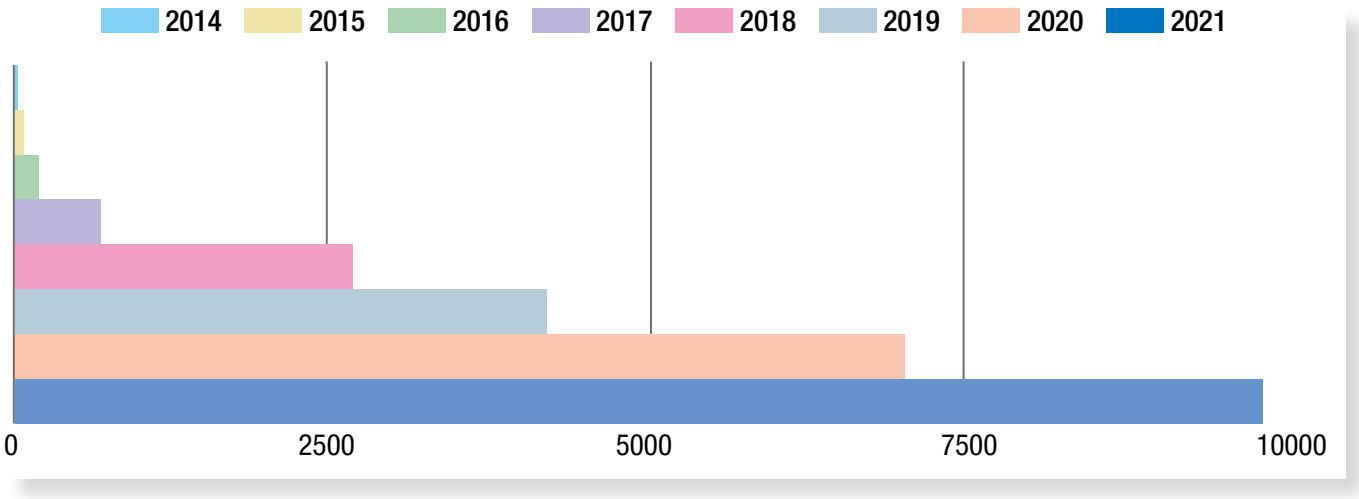


Figura 7.6. Estafas informáticas. Causas penales a cargo de la Fiscalía Adjunta de Fraudes y Cibercrimen (2014-2021)

Fuente: Solicitud de información 1182-OPO/UAC/S-2022.

7.5. HACIA EL RECONOCIMIENTO DE LOS DERECHOS DIGITALES

El Estado costarricense tiene la obligación de desarrollar política pública y promover reformas legales que brinden mayores garantías a las personas en la utilización de estos entornos digitales. Sin embargo, cuando se habla de la protección de nuevos derechos digitales o de libertades en el ciberespacio muchos consideran que es un área en donde se establecen obstáculos a la innovación, cuando lo que realmente debe generar es una adecuada confianza en los medios tecnológicos para convertir a la tecnología en un motor de innovación y cambio social.

7.5.1 La libertad en el ciberespacio y democracia

La privacidad y la libertad están estrictamente relacionadas, ya que la intromisión sobre una representa una injerencia sobre la otra, lo que resulta preocupante cuando comprendemos que de la autonomía individual depende nuestro sistema democrático. Cuando pensamos que la recopilación, análisis y uso indiscriminado de nuestros datos personales pueden tener impacto en nuestra toma de decisiones es un buen momento para hacer una pausa y buscar un mejor entendimiento del problema. Sobre este tema, es importante destacar el comentario del autor español Juan A. Hernández Corchete, sobre el impacto del tratamiento de los datos sobre la autonomía personal:

> es susceptible de resultar afectada no solo de manera coercitiva, sino también por medio de condicionantes que, principalmente sin la conciencia del sujeto, alcancen a manipular sus decisiones, guiándolas sin su voluntad efectiva en determinadas direcciones. Los tratamientos de datos personales ligados al desarrollo de la sociedad digital pueden, suministrar información significativa de la persona y porque lo hacen sin que ésta repare en esta realidad ni en que se usa para influirle, producir esta incidencia manipulativa y consecuentemente pueden mermar o incluso anular la privacidad del sujeto entendida como espacio de libre decisión o, dicho con otras palabras, de autonomía personal. (Hernández, 2018, p. 282).

Sobre el vínculo de la autonomía individual y la privacidad vale la pena destacar la obra Conceptualizando la privacidad (Solove, 2002), en la cual sobre misma materia nos explica que el filósofo Stanley Benn también desarrolla una concepción de la privacidad desde la personalidad, **señalando que la privacidad equivale al respeto por los individuos como personas que eligen: "El respeto a alguien como persona, como persona que elige, implica el respeto por él como alguien que participa en una especie de empresa autocreativa, que podría verse interrumpida, distorsionada o frustrada incluso por una intrusión tan limitada como la de observar**. Basándose en El ser y la nada de Jean Paul Sartre, Benn explica que ser "objeto de escrutinio, como foco de la atención de otro, le lleva a uno a una nueva conciencia de sí mismo, como algo visto a través de los ojos de otro". **El observado "toma conciencia de sí mismo como objeto, conocible, que tiene un carácter determinado**".

La privacidad y el reconocimiento de nuevos derechos digitales será lo que nosotros como sociedad decidamos que debe ser, por lo que para concluir este tema cito nuevamente a Hernández: la privacidad como espacio de libre decisión de la persona es un bien jurídico básico en cualquier Estado de Derecho, pero depende de cada ordenamiento jurídico la forma en que se garantiza" (Hernández, 2018, p. 285). Por lo anterior, podemos concluir que la construcción de nuevos derechos digitales que le permitan a los individuos ser libres es uno de los fundamentos de todo Estado democrático.

7.5.2 El desarrollo de política pública y el respeto de los derechos digitales

Un país puede desarrollar política dirigida a la protección de nuevos derechos o puede incluir el respeto de los derechos digitales en toda aquella que involucre a las TIC. En el caso de Costa Rica, en el Gobierno de Luis Guillermo Solís, cuando se desarrolló la **Estrategia de Ciberseguridad** se procuró incluir el respeto de los derechos humanos y particularmente el de la privacidad, en su apartado 4.2:

> 1.2. **Respeto a los Derechos Humanos y la Privacidad:** Garantizar el respeto a los derechos humanos, especialmente los relacionados con el acceso a las TIC, el acceso a la información y el respeto a la privacidad, es fundamental. Las medidas y acciones que resulten de esta estrategia deberán en todo momento salvaguardar los derechos humanos y la privacidad de la información de los habitantes del país.
>
> Por lo tanto, esta estrategia se ha desarrollado teniendo en cuenta la necesidad de equilibrar la protección de todos los habitantes y el respeto de los derechos humanos básicos y fundamentales, con la necesidad de implementar medidas para mantenerlos seguros en línea. Esto incluye el respeto a la libertad de expresión, la libertad de palabra, el derecho a la privacidad, la libertad de opinión y la libertad de asociación. (Micitt, 2017, p. 36).

Pocos meses después, con el cambio de gobierno, el Micitt publica su **Estrategia para la Transformación Digital hacia la Costa Rica del Bicentenario 4.0,** la cual como se señaló en el informe anterior (Medrano, 2020) el diseño y accionar de dicha estrategia está basado en cinco principios esenciales de los cuales **llama la atención que ninguno se refiera al tema de la privacidad en el manejo de datos personales**. Esto resulta relevante pues no se puede obviar la ausencia de la privacidad como un principio rector de una estrategia que busca aprovechar las ventajas de la cuarta revolución industrial ya que al involucrar tecnologías sustentadas en la inteligencia artificial y similares, se generan importantes retos para la privacidad de la ciudadanía.

Lo más grave de dicha estrategia es que indica de manera expresa que la transformación digital debía propiciar los cambios sustantivos en materia de la normativa nacional vigente para permitir el apro-

vechamiento de las tecnologías digitales disruptivas en el quehacer de los diversos sectores de la sociedad costarricense. El documento señala de forma expresa la normativa para la gestión de la información ciudadana (habeas data, privacidad), como un elemento que debería cambiarse, que aunque incluía la fiscalización ciudadana y la discusión sobre la normativa vigente, lo cierto es que cuando se dio el escándalo UPAD, el gobierno fundamentó el famoso decreto en dicha estrategia para crearla.

No solo esto, sino que también se basó en el derecho de acceso a la información pública y en la limitación del derecho de autodeterminación informativa (art. 8, ley №8968), **lo que nos llevaba más en la ruta de una ciudanía más transparente hacia el Estado y aunque era un cambio importante, no se propició ninguna clase de fiscalización.** La fiscalización se realizó una vez el decreto era de conocimiento público y fue importante la labor del Colegio de Abogados y Abogadas, cuyo Informe Técnico de la Comisión Ad Hoc para el Análisis sobre la Creación de la UPAD dio luz al debate público con respecto a la ilegalidad e inconstitucionalidad del decreto, ya que para este momento la Prodhab se había pronunciado con respecto a que no había acto ilegal alguno, como se reportó en el informe Hacia la Sociedad de la Información y el Conocimiento 2020:

> A pesar de la gravedad de los hechos, **la Prodhab en un comunicado de prensa, manifestó que no existe ninguna limitación legal para que se compartieran estos datos**, en contravención del artículo 14 de la ley e inclusive en contradicción de criterios de la agencia en el pasado (Medrano, 2020, p. 349).

Como puede verse, esto es un reflejo de la necesidad de independencia de la Prodhab, sino también la importancia de la participación de la sociedad civil, la academia y los distintos sectores para la fiscalización sobre el respeto de los derechos digitales de los ciudadanos. De hecho, en el 2020, a falta de una organización costarricense especializada en defender la privacidad o derechos digitales fue el Colegio de Abogados y Abogadas quien se encargó de realizar esta labor. Como veremos a continuación, debido a este vacío nace una organización con este fin.

7.5.3 Sociedad civil en la defensa de los derechos digitales

En nuestro país hacen falta más organizaciones que de manera especializada se dediquen en la defensa de los derechos digitales de los costarricenses ya que el avance tecnológico requiere esfuerzos enormes de fiscalización, monitorización y capacitación que es difícil que se logre de manera solitaria.

7.5.4. Fundación PRIDAT

A finales del 2020, impulsada por el caso UPAD distintos ciudadanos crearon la Fundación de Privacidad y Datos (Pridat), que de acuerdo a su sitio web es una organización sin fines de lucro cuya misión es la protección de los datos personales de los costarricenses. Además, de promover una cultura de privacidad digital e incidir en el diseño de políticas públicas informadas que permitan al país alinear las bondades de la tecnología con el respeto a la democracia y los derechos fundamentales (Pridat, 2022). Desde su fundación han generado los siguientes comunicados y reportes:

- Comunicado sobre ataque de ransomware a Ministerio de Hacienda (19 abril 2022). Pronunciamiento: Recopilación de Datos Sensibles mediante Pruebas FARO - Ministerio de Educación. (13 de noviembre de 2021).
- Posición sobre el Pasaporte Biométrico.
- Entrevistas y participación en eventos sobre medios de comunicación sobre el proyecto de ley №22.388 sobre Protección de datos personales.

- Presentación de proyecto de ley №23.097 sobre protección de datos personales y un proyecto de ley № 22.063 que reforma el artículo 24 constitucional.

7.5.5. Comisión de Innovación Regulatoria del Colegio de Abogados y Abogadas

Como se ha destacado anteriormente, las comisiones de este colegio profesional han tenido gran importancia en la discusión de temas de alta relevancia nacional como lo es la defensa de los derechos digitales. A través de la Comisión de Innovación Regulatoria se ha montado una estructura de defensa por los derechos humanos, en particular, los digitales. El señor Julio Córdoba, miembro fundador de dicha comisión, en un artículo para Diario Extra indica lo siguiente:

> La normativa vigente debe velar para que desde la instrucción básica nos formemos más alineados con las necesidades del presente y del futuro, por lo que hasta el cómo aprendemos debe mejorarse. De la misma manera, para nuestra sociedad es esencial una cultura de ciberseguridad y privacidad que nos proteja a todos, pero principalmente a la niñez, de los peligros de internet.
>
> De igual manera, las empresas deben desarrollar su cultura de seguridad, privacidad y derechos digitales, que le permitan a sus colaboradores ser más eficientes y felices, en una sociedad que cada vez vive más conectada, bien haríamos con permitirles desconectarse…
>
> **El Colegio de Abogados y Abogadas se ha apuntado al reto de la innovación regulatoria a través de la discusión de temas que deberán ser discutidos pronto en la Asamblea Legislativa, si nuestro país no se quiere quedar atrás.**
>
> Los diputados están ante el desafío de construir, de la mano de la sociedad civil, legislación que le permita a Costa Rica crecer integrada de una forma competitiva a un mundo donde la digitalización de procesos, uso de monedas electrónicas, interacción con inteligencia artificial, internet de las cosas y hasta la nueva vida que ofrece el metaverso pueda ser disfrutada con plenitud, prosperidad y seguridad jurídica, porque las sociedades que no se adapten entrarán en rezago de oscuridad, desestímulo a la innovación, expulsión de la inversión y fuga masiva de cerebros. (Córdoba, 2022, párr. 3-4 y 8-9).

En febrero de 2021, la Comisión de Innovación Regulatoria le solicita al Colegio de Abogados y Abogadas la creación de observatorios, con la idea de **generar mecanismos de detección rápida de temas que requieren debate urgente debido a alguna iniciativa regulatoria.** Dentro de estos observatorios, se encuentra el de privacidad. Hasta la fecha el proceso se ha iniciado debido a 3 temas puntuales:

- **Proyecto de ley 22.388:** Un proyecto de ley que contenía importantes avances para la regulación de protección de datos personales, a la vez que peligros. Estos últimos fueron discutidos a través de 4 jornadas de discusión con especialistas en derecho informático, con el fin de analizar los puntos de mejora que presentaba el proyecto[9]. El riesgo más grave se encontraba en el texto sustitutivo de octubre de 2021, en donde se buscaba regular la forma como operó el gobierno en el caso UPAD. En la discusión de este proyecto de ley participaron distintos especialistas, incluyendo los de Fundación Pridat mencionados anteriormente.

9 Las I Jornadas de Debate Regulatorio sobre Protección de Datos Personales se pueden encontrar en https://youtube.com/playlist?list=PLtUSK-C_-80Zpl4ddfyeZ4ktHlZ7xcbJJX

-Discusión sobre propuestas regulatorias sobre criptoeconomía en Costa Rica y la región[10]: este evento obedeció a la presentación del proyecto de ley 22.837 que podría a impactar la criptoeconomía local de manera importante. El evento trascendió a medios, por lo que crhoy.com lo destacó de la siguiente manera: "**Expertos en Derecho e Informática criticaron un proyecto** de ley que **pretende regular la actividad de criptoactivos** en el país", Sin embargo, consideran que **pese a los cuestionamientos, la actividad se trata de una gran oportunidad de negocios**. Así se desprende de la mesa redonda "Propuestas Regulatorias sobre la criptoeconomía en Costa Rica y la región", organizada por el Colegio de Abogados (Murillo, 2022, párr.1).

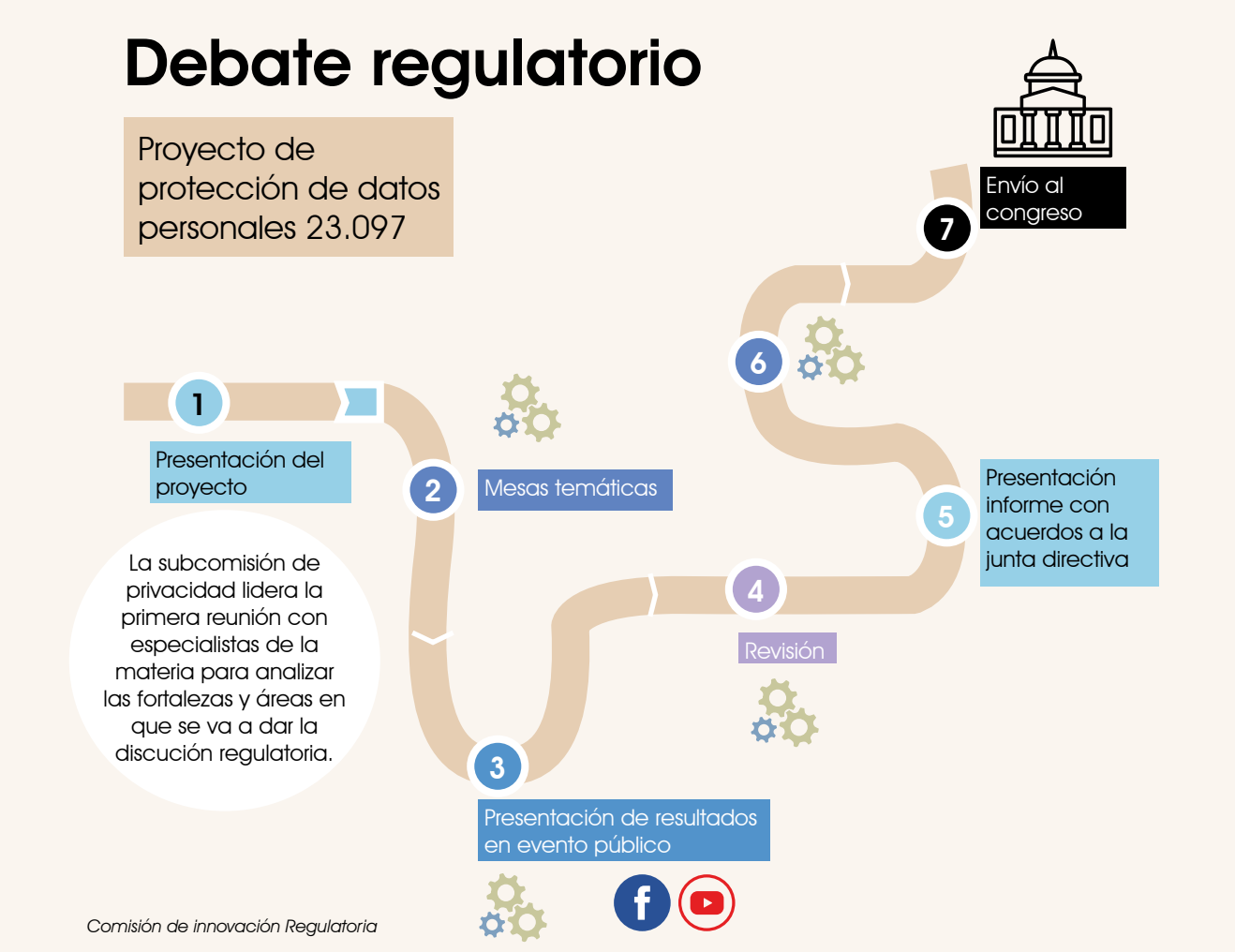


Figura 7.7. Proceso de debate regulatorio al que será sometido el proyecto de Ley 23.097

Fuente: Comisión de Innovación Regulatoria.

10 El evento puede verse en https://youtu.be/Dsa9oYG-WObQ

- **Proyecto de ley № 23.097 y № 22.063:** tanto el proyecto de ley que presentó el Partido Liberal Progresista (PLP) y el que presentó el Partido Liberación Nacional (PLN), con la ayuda de la Fundación Pridat sobre la Protección de Datos Personales serán sometidos a un proceso de debate regulatorio donde participarán distintos especialistas en derecho informático, con el fin de brindarle insumos a la Asamblea Legislativa para el proceso legislativo.

El proyecto de ley № 23.097, a diferencia del presentado por el Partido Acción ciudadana, viene a imponer una regulación más restrictiva con respecto a la transferencia de datos personales entre instituciones públicas, impidiendo que se transfieran bases de datos personales de ciudadanos completas entre ciudadanos, lo cual es uno de los graves problemas que contenía el proyecto del PAC. Al igual que el proyecto № 22.388, se encuentran inspirados en el Reglamento General de Protección de Datos de la Unión Europea (RGPD[11]) y aunque no presenta mayores riesgos para la población sí que cuenta elementos que merecen un profundo debate regulatorio, así como la inclusión de derechos digitales en dicha legislación, de manera similar a como lo hizo España, como se analizará más adelante.

7.5.6. Abriendo datos Costa Rica

Es una organización de sociedad civil sin fines de lucro cuyo objetivo es contribuir a fomentar la cultura de datos abiertos. La organización realiza capacitaciones y desarrolla proyectos dirigidos al acceso a la información pública, para el ejercicio ciudadano en todas sus facetas. Con respecto al escándalo UPAD, la organización también tuvo su participación desde un enfoque distinto. En entrevista para Semanario Universidad indicaron lo siguiente:

> Susana Soto e Ignacio Alfaro, de la organización Abriendo Datos, señalaron que la iniciativa representa amenazas a la privacidad de los costarricenses y contradice el proceso participativo de apertura de datos que se venían realizando desde las administraciones anteriores. Tras la revisión de los datos publicados por la Presidencia, los activistas indicaron que la herramienta usada (Tableau) no permite el acceso a los datos, sino sólo a su representación gráfica, lo que deja duda sobre el nivel de sensibilidad de la información que se está utilizando. Según la filosofía de datos abiertos, la información de las instituciones (debidamente anonimizada) debe ser accesible vía Internet, en formato digital, interoperable (para ser leída, usada y reutilizada), y tener una licencia para libre uso y distribución. La activista, que participa en la Comisión Nacional de Datos Abiertos, comentó que en la primera sesión del año el Ministerio de Comunicación informó que no había presupuesto, a pesar de que ya estaba funcionando la UPAD. (Muñoz, 2020, párr. 3-6).

7.6. EXPERIENCIAS INTERNACIONALES EN EL RECONOCIMIENTO DE LOS DERECHOS DIGITALES

Para incorporar nuevos derechos en el ciberespacio, es importante que aprendamos de las experiencias de otras naciones que llevan mucho más tiempo discutiendo esta materia. Por temas de espacio, vamos a limitar el estudio a lo acontecido en el continente europeo.

7.6.1. El Consejo de Europa promueve la garantía los derechos humanos y libertades de los usuarios de internet

El Consejo de Europa en el año 2014, publicó la Recomendación CM/Rec(2014)6, que contiene **la Guía**

11 GDPR, por sus siglas en inglés.

de los derechos humanos para los usuarios de Internet[12]**, del cual vamos a destacar distintos elementos para su estudio.** En esta se establece que todos los Estados miembros tienen la obligación de garantizar a todas las personas de su jurisdicción los derechos humanos y las libertades fundamentales consagrados en el Convenio Europeo de Derechos Humanos, lo que incluye la supervisión de las empresas privadas. A su vez, de manera expresa indica que esta obligación aplica en el contexto del uso de Internet, por lo que otros convenios y instrumentos del Consejo de Europa que tratan los siguientes derechos son aplicables:

1. Protección del derecho a la libertad de expresión.
2. Acceso a la información.
3. El derecho a la libertad de reunión.
4. La protección frente a la ciberdelincuencia.
5. El derecho al respeto a la vida privada.
6. La protección de los datos personales.

Con el fin de poder garantizar que los derechos humanos y las libertades fundamentales reconocidos se apliquen por igual dentro y fuera de la red, el Consejo de Europa (2014) recomienda que los Estados promuevan activamente la Guía de los derechos humanos para los usuarios de Internet entre los ciudadanos, las autoridades públicas y los actores del sector privado, y emprendan acciones específicas para su aplicación a fin de permitir a los usuarios ejercer plenamente sus derechos humanos y libertades fundamentales en línea**.**

Tabla 7.3. Guía de los derechos humanos para los usuarios de Internet

Acceso y no discriminación	Libertad de expresión e información
El acceso a Internet es un medio importante para que usted ejerza sus derechos y libertades y participe en la democracia. Por lo tanto, usted no debería quedar desconectado de Internet contra su voluntad, salvo por decisión judicial. En ciertos casos, el servicio podría descontinuarse debido a acuerdos contractuales, pero esta debería ser una medida de último recurso. 2. Su acceso debería ser asequible y no discriminatorio. Usted debería tener el mayor acceso posible al contenido, las aplicaciones y los servicios de Internet desde los dispositivos de su elección. 3. Si vive en una zona rural o alejada geográfcamente, dispone de bajos ingresos, tiene alguna discapacidad o tiene necesidades especiales, debería tener la expectativa de que las autoridades públicas hagan esfuerzos razonables y tomen medidas específcas para facilitar su acceso a Internet.	Usted tiene derecho a buscar, recibir y comunicar información e ideas de su elección, sin injerencia y sin consideración de fronteras. Esto significa que: 1. usted tiene la libertad de expresarse en línea y de acceder a la información y las opiniones y expresiones de otros. Esto incluye discursos políticos, puntos de vista sobre religión y opiniones u expresiones que tengan una acogida favorable o se consideren inofensivas, así como también aquellas que puedan ofender, chocar o perturbar a otros. Usted debe tomar debidamente en consideración la reputación y los derechos de los demás, inclusive el derecho al respeto a la vida privada; 2. pueden aplicarse restricciones a las expresiones que incitan a la discriminación, el odio o la violencia. Estas restricciones deben ser lícitas, estar definidas de manera estricta y ejecutarse bajo supervisión judicial;

Fuente: Tomado del Consejo de Europa, 2020.

12 Adoptada por el Consejo de Ministros el 16 de abril de 2014, en la 1197a reunión de Delegados de los Ministros.

Reunión, asociación y participación

Usted tiene derecho a reunirse y asociarse pacífcamente con otras personas usando Internet. En la práctica, esto significa que:

1. usted tiene la libertad de elegir cualquier sitio web, aplicación u otro servicio para formar o movilizar grupos sociales o asociaciones, o para su ingreso o participación en estos, independientemente de que estén o no reconocidos de manera formal por las autoridades públicas. Usted también debería poder utilizar Internet para ejercer su derecho a constituir sindicatos y formar parte de los mismos;

2. usted tiene derecho a protestar pacífcamente en línea. Sin embargo, debe tener en cuenta que se expone a consecuencias jurídicas si su protesta en la red causa bloqueos, interrupción de servicios o daños a los bienes de terceros;

Protección de la vida privada y de los datos personales

Usted tiene derecho al respeto de su vida privada y familiar en Internet, lo cual abarca la protección de sus datos personales y el respeto de la confidencialidad de su correspondencia y sus comunicaciones. Esto signifca que:

1. usted debería tener en cuenta que, al utilizar Internet, sus datos personales son objeto de un tratamiento constante. Esto ocurre cuando utiliza servicios tales como navegadores, correo electrónico, mensajes instantáneos, protocolos de transmisión de voz por Internet, redes sociales, motores de búsqueda y servicios de almacenamiento de datos en la nube;

2. las autoridades públicas y las empresas privadas tienen la obligación de respetar normas y procedimientos específicos cuando tratan sus datos personales;

Educación y conocimientos básicos

Usted tiene derecho a la educación, lo cual abarca el acceso al conocimiento. Esto signifca que:

1. usted debería tener acceso en línea a la educación, así como a contenidos culturales, científcos, académicos y de otra índole en lenguas ofciales. En relación con tal acceso, podrían aplicarse condiciones a fn de remunerar a los titulares de derechos por el trabajo que realizan. Usted también debería poder acceder libremente en Internet a las investigaciones y obras culturales de dominio público que sean fnanciadas con fondos públicos, cuando estén disponibles;

2. como parte del conocimiento básico de Internet y de los medios de comunicación, y con el objetivo de ejercer sus derechos y libertades en Internet, usted debería tener acceso a la educación y el saber digital, que abarca las competencias para comprender una amplia gama de herramientas de Internet, así como para usarlas y trabajar con ellas. Esto debería permitirle evaluar con una mirada crítica la exactitud y la fabilidad de los contenidos, aplicaciones y servicios a los que tiene acceso o a los que le gustaría acceder.

Niños y jóvenes

Como niño(a) o joven, tienes todos los derechos y las libertades que se describen en esta guía. En particular, debido a tu edad, tienes derecho a recibir protección y orientación especial al utilizar Internet. Esto signifca que:

1. tienes derecho a expresar libremente tus puntos de vista y a participar en la sociedad, a que se te escuche y a contribuir en la toma de decisiones sobre los asuntos que te afecten. Se debe dar a tus opiniones la consideración adecuada en función de tu edad y madurez, sin discriminación;

2. puedes tener la expectativa de recibir información en un lenguaje apropiado para tu edad y de que tus profesores, educadores, padres o tutores te orienten sobre el uso seguro de Internet, incluida la manera de proteger tu vida privada;

3. debes tener en cuenta que tanto el contenido creado por ti en Internet como el contenido creado por otros usuarios en relación contigo pueden ser accesibles en todo el mundo y podrían poner en peligro tu dignidad, tu seguridad y tu vida privada, o ser de otro modo perjudiciales para ti o para tus derechos, ahora o en una etapa posterior de tu vida. Si lo solicitas, tal contenido debe ser retirado o eliminado dentro de un plazo razonable;

Recursos efectivos	
1. Usted tiene derecho a un recurso efectivo cuando sus derechos humanos y libertades fundamentales sean objeto de restricción o violación. Para disponer de un recurso, no debería ser necesario que inicie directamente una acción legal. Las vías de recurso deberían estar disponibles, ser conocidas, accesibles y asequibles, y ser aptas para brindar una reparación adecuada. Deben poder obtenerse recursos efectivos directamente de los proveedores de servicios de Internet, las autoridades públicas o las instituciones nacionales de derechos humanos. Dependiendo de la violación de que se trate, los recursos efectivos pueden dar lugar a: la investigación, la explicación, la respuesta, la corrección, la petición de disculpas, el restablecimiento, la reconexión y la compensación. En la práctica, esto significa que:	1.2. las autoridades públicas, instituciones nacionales de derechos humanos (tales como mediadores), autoridades de protección de datos, ofcinas de asesoramiento a los ciudadanos, asociaciones de derechos humanos o derechos digitales, u organizaciones de consumidores deberían poner a disposición información y orientación adicional;
1.1. su proveedor de servicios de Internet, los proveedores de acceso a contenidos y servicios en línea, u otras compañías o autoridades públicas deberían informarle sobre sus derechos y libertades, así como sobre los recursos posibles y el modo de obtenerlos. Esto incluye información fácilmente accesible sobre la manera de denunciar injerencias en sus derechos, de presentar quejas al respecto y de buscar reparación;	1.3. las autoridades nacionales tienen la obligación de protegerle de actividades ilícitas o delitos cometidos en Internet o mediante el uso de Internet, en particular cuando están relacionados con el acceso ilícito, la interferencia, la falsifcación u otros manejos fraudulentos de su identidad digital, su ordenador o los datos allí contenidos. Las autoridades de orden público competentes tienen la obligación de investigar y tomar medidas adecuadas, lo cual incluye sanciones, si usted presenta una queja por perjuicio o injerencia en relación con su identidad personal y su propiedad en línea.
	2. En lo que respecta a la determinación de sus derechos y obligaciones o de cualquier acusación penal contra usted en relación con Internet:
	2.1. usted tiene derecho a un proceso equitativo, dentro de un plazo razonable, por un tribunal independiente e imparcial;
	2.2. usted tiene derecho a interponer un recurso individual ante el Tribunal Europeo de Derechos Humanos después de haber agotado todos los recursos nacionales disponibles.

7.6.2 La ley orgánica española de protección de datos personales y garantía de derechos digitales (LOPD-GDD)

Esta ley que entró en vigor en el año 2018 tiene por objeto adaptar la normativa de protección de datos personales al Reglamento Europeo de Protección de Datos Personales (RGPD) y en donde el legislador español decidió incursionar en la inclusión de derechos digitales. Como lo señala Moisés Barrio (2020) es la primera vez que un Estado europeo garantizará por ley derechos digitales en todos ámbitos individuales y colectivos afectados por la tecnología. Y la nueva norma impone obligaciones a los poderes públicos para posibilitar un acceso pleno de los ciudadanos a las herramientas y posibilidades tecnológicas.

De acuerdo al preámbulo de la LOPD-GDD, destaca la realidad omnipresente del internet en nuestra vida personal como colectiva, lo que genera una necesidad de reconocer los derechos digitales y la responsabilidad de los poderes públicos de desarrollar política pública que los garanticen:

Ya en los años noventa, y conscientes del impacto que iba a producir Internet en nuestras vidas, los pioneros de la Red propusieron elaborar una Declaración de los Derechos del Hombre y del Ciudadano en Internet.

Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. **Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital.** La transformación digital de nuestra sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía.

Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. **Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales**. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.

En el Título X de la LOPD-GDD, el legislador español decidió incluir la garantía de los derechos digitales, en su artículo 74, el cual se encuentra en armonía con lo indicado por el Consejo de Europa en la Recomendación CM/Rec (2014) 6:

> **Artículo 79. Los derechos en la Era digital.**
>
> **Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales** en que España sea parte **son plenamente aplicables en Internet**. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación (Artículo 79, 2018, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, España).

Los derechos reconocidos por esta innovadora legislación, junto con una pequeña descripción son:

1. **Derecho a la neutralidad de Internet.** Los proveedores de servicios de Internet deben proporcionar una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.
2. **Derecho de acceso universal a Internet.** Todos tienen derecho a acceder a Internet de forma asequible y de calidad, independientemente de su condición personal, social, económica o geográfica.
3. **Derecho a la seguridad digital**: Este derecho aplica sobre las comunicaciones que los usuarios transmitan y reciban a través de Internet, que deberán ser seguras.
4. **Derecho a la educación digital:** El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales.
5. **Protección de los menores en Internet.** Este derecho le impone el deber a los padres, madres, tutores, curadores o representantes legales de procurar que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales. A su vez, la utilización o difu-

sión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección establecidas en la ley.

6. **Derecho de rectificación en Internet**. Obliga a los responsables de redes sociales y servicios equivalentes a adoptar protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz. Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo.
7. **Derecho a la actualización de informaciones en medios de comunicación digitales:** Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.
8. **Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.** Reconoce el derecho a la intimidad del trabajador, pero le permite al empleador acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos. Todo lo anterior en un marco de respeto de sus derechos fundamentales, según los criterios de utilización de los dispositivos digitales y en todo caso los estándares mínimos de protección de su intimidad según los usos sociales y los derechos reconocidos constitucional y legalmente.
9. **Derecho a la desconexión digital en el ámbito laboral:** Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar. El empleador deberá elaborar una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática.
10. **Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo:** se les permite a los empleadores dicho tratamiento, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

11. **Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.** Se le permite a los empleadores este tratamiento, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.
12. **Protección de datos de los menores en Internet:** Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información. Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales.
13. **Derecho al olvido en búsquedas de Internet.** Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información. Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet. Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

    Derecho al olvido en servicios de redes sociales y servicios equivalentes: Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes. La norma contiene regulación para cuando los datos han sido facilitados por terceros y cuando corresponden a un menor de edad.
14. **Derecho de portabilidad en servicios de redes sociales y servicios equivalentes:** Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.
15. **Derecho al testamento digital:** Permite el acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas. Este apartado también establece de forma expresa que a través de convenciones colectivas, se reconocen garantías adicionales.

7.6.3. La Carta de Derechos Digitales

El 15 de julio del 2021, el Gobierno de España adoptó la Carta de Derechos Digitales, la cual fue elaborada a partir del trabajo realizado por el Grupo

asesor de expertos constituido por la Secretaria de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital. Esta carta que no tiene carácter normativo y por tanto debe verse como una guía que tiene como objetivo:

a. Ser un marco de referencia para garantizar los derechos de la ciudadanía en la nueva realidad digital.

b. Reconocer los retos que plantea la adaptación de los derechos actuales al entorno virtual y digital.

Como lo indica el Gobierno de España (2021) el texto recoge un conjunto de principios y derechos para guiar futuros proyectos normativos y el desarrollo de las políticas públicas de forma que se garantice la protección de los derechos individuales y colectivos en los nuevos escenarios digitales.

> El objetivo de la Carta es descriptivo, prospectivo y asertivo. Descriptivo de los contextos y escenarios digitales que dan lugar a nuevos conflictos y situaciones que deben resolverse; prospectivo al anticipar futuros escenarios que pueden ya predecirse; y asertivo porque revalida y legitima los principios, técnicas y políticas que deberían aplicarse en los entornos y espacios digitales presentes y futuros. (Gobierno de España, 2021).

Como lo indica de manera expresa la carta, esta no trata de crear nuevos derechos fundamentales, sino que busca perfilar los más relevantes en el entorno y los espacios digitales o describir derechos instrumentales o auxiliares de los primeros. Por cuestiones de espacio, se van a citar con una pequeña descripción a los derechos digitales que contiene, pero que son distintos a los contenidos en la LOPD-GDD:

1. **Derechos de Libertad**

Derecho a la identidad en el entorno digital. El derecho a la propia identidad es exigible en el entorno digital. Esta identidad vendrá determinada por el nombre y por los demás elementos que la configuran de acuerdo con el ordenamiento jurídico nacional, europeo e internacional. Debe garantizarse, con arreglo a nuestro ordenamiento jurídico, el derecho a la gestión de la propia identidad, sus atributos y acreditaciones.

Derecho al pseudonimato. De acuerdo con las posibilidades técnicas disponibles y la legislación vigente, se permitirá el acceso a los entornos digitales en condiciones de pseudonimidad, siempre y cuando no sea necesaria la identificación personal para el desarrollo de las tareas propias de dicho entorno.

Derecho de la persona a no ser localizada y perfilada. La localización y los sistemas de análisis de personalidad o conducta que impliquen la toma de decisiones automatizadas o el perfilado de individuos, o grupos de individuos, únicamente podrán realizarse en los casos permitidos por la normativa vigente y con las garantías adecuadas en ella dispuestas.

2. **Derechos de Igualdad**

Derecho a la igualdad y a la no discriminación en el entorno digital. El derecho y el principio a la igualdad inherente a las personas será aplicable en los entornos digitales, incluyendo la no discriminación y la no exclusión. En particular, se promoverá la igualdad efectiva de mujeres y hombres en entornos digitales. Además, se fomentará que los procesos de transformación digital apliquen la perspectiva de género adoptando, en su caso, medidas específicas para garantizar la ausencia de sesgos de género en los datos y algoritmos usados**.**

Accesibilidad universal en el entorno digital: Se promoverán las condiciones necesarias para garantizar la accesibilidad universal de los entornos digitales, en particular a las personas con discapacidad, tanto desde el punto de vista del diseño tecnológico como respecto de sus contenidos, asegurando especialmente que la información relativa a las condiciones legales del servicio resulte accesible y comprensible.

Brechas de acceso al entorno digital. Se fomentará y facilitará el acceso de todos los colectivos a los entornos digitales y su uso y la capacitación para el mismo**.**

3. **Derechos de participación y de conformación del espacio público**

Libertad de expresión y libertad de información: A quienes ejerzan su libertad de expresión e información a través de los servicios intermediarios de la sociedad de la información les corresponden las eventuales responsabilidades como autores por los contenidos ilícitos o que lesionen bienes o derechos de un tercero susceptibles de indemnización.

Derecho a recibir libremente información veraz: Se promoverá la adopción, por parte de los prestadores de servicios intermediarios a través de los cuales directamente se ejerzan libertades de expresión e información, de protocolos adecuados que garanticen a los usuarios su derecho a recibir información veraz.

Derecho a la participación ciudadana por medios digitales: De acuerdo con las leyes, se promoverán entornos digitales que contribuyan a un derecho de acceso efectivo a la información pública, la transparencia, la rendición de cuentas, así como a la propuesta de iniciativas y a la implicación de las personas en las actuaciones de las Administraciones públicas en sus respectivos ámbitos competenciales, de acuerdo con la Constitución Española.

Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas: El derecho a la igualdad de las personas se extiende al acceso a los servicios públicos y en las relaciones digitales con las Administraciones públicas. A tal fin se promoverán políticas públicas activas que garanticen el acceso a los servicios públicos, a los sistemas y los procedimientos a todos los sujetos y la asistencia en tales procedimientos.

Derechos del Entorno Laboral y empresarial: Se garantizarán la dignidad y los derechos fundamentales de las personas trabajadoras en los entornos digitales

a. La desconexión digital, al descanso y a la conciliación de la vida personal y familiar.
b. La protección de sus derechos a la intimidad personal y familiar, el honor, la propia imagen, la protección de datos y el secreto de las comunicaciones en el uso de dispositivos digitales, así como frente al uso de dispositivos de videovigilancia, de grabación de sonidos, y en el caso de la utilización de herramientas de monitoreo, analítica y procesos de toma de decisión en materia de recursos humanos y relaciones laborales, y en particular, la analítica de redes sociales.
c. La protección de los derechos de la letra anterior en la utilización de sistemas biométricos y de geolocalización.
d. La garantía de sus derechos frente al uso por la entidad empleadora de procedimientos de analítica de datos, inteligencia artificial y, en particular, los previstos en la legislación respecto del empleo de decisiones automatizadas en los procesos de selección de personal.
e. El uso licito, leal, proporcionado y transparente de los controles empresariales digitales. [entre otros..] (Gobierno de España, 2021, p.22).

La empresa en el entorno digital: La libertad de empresa reconocida en la Constitución Española es aplicable en los entornos digitales en el marco de la economía de mercado, en el que quede asegurada la defensa y promoción de una competencia efectiva, evitando abusos de posición de dominio, que garantice igualmente la compatibilidad, seguridad, transparencia y equidad de sistemas, dispositivos y aplicaciones.

1. **Derechos digitales en entornos específicos**
    a. Derecho de acceso a datos con fines de archivo en interés público, fines de investigación científica o histórica, fines estadísticos, y fines de innovación y desarrollo.

b. Derecho a un desarrollo tecnológico y a un entorno digital sostenible

c. Derecho a la protección de la salud en el entorno digital.

d. Libertad de creación y derecho de acceso a la cultura en el entorno digital Derechos ante la inteligencia artificial.

2. **Derechos digitales en el empleo de las neurotecnologías**[13]

   Garantía y Eficacia: Todas las personas tienen derecho a la tutela administrativa y judicial de sus derechos en los entornos digitales de acuerdo con lo dispuesto en la legislación vigente.

7.7. EL DESARROLLO DE DERECHOS DIGITALES EN COSTA RICA

Costa Rica ha tenido un avance importante en la protección de derechos digitales, principalmente en el Código Penal, resoluciones de la Sala Constitucional y algunas leyes especiales. Sin embargo, nos encontramos ante esfuerzos aislados carentes de una estrategia país hacia el reconocimiento de nuevos derechos para las necesidades de la Costa Rica del futuro. Debemos acordarnos que más bien la Estrategia de Transformación Digital del gobierno de Carlos Alvarado omitía por completo alguna ruta hacia algún reconocimiento de derechos digitales. A continuación, vamos a abordar algunos derechos digitales que han sido incluidos dentro de nuestro ordenamiento jurídico, en relación con el contexto de los riesgos detallados en el presente capítulo.

7.7.1 El derecho a la seguridad digital

El reconocimiento de la seguridad digital como un derecho de las personas es altamente necesario para poder proteger al ciudadano ya no solo sobre la violación de sus datos personales, sino por la gran posibilidad de afectar su patrimonio y otros bienes jurídicos. En Costa Rica, el legislador optó por proteger la información personal obligando al responsable de la base de los datos a garantizar la seguridad de estos, con lo cual se busca que este le brinde una garantía de confidencialidad e inalterabilidad de la información personal, como reza en el numeral 10, titulado **seguridad de los datos**:

> El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.
>
> Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.
>
> No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas.
>
> Por vía de reglamento se establecerán los requisitos y las condiciones que deban

13 En ese mismo sentido, Chile ha avanzado en una reforma constitucional bastante innovadora:
En 2021 el Senado chileno (link is external) aprobó por votación unánime un proyecto de ley que modifica la Constitución para proteger los derechos del cerebro o "neuroderechos". La Cámara de Diputados revisó y votó esta legislación en septiembre de este año. Ahora tiene que ser promulgada por el presidente de la República.
Si el proceso llega a su fin, Chile se convertirá en el primer país que se dota de una legislación encaminada a proteger la integridad mental, el libre albedrío y la no discriminación en el acceso de los ciudadanos a las neurotecnologías. Su objetivo es dar el estatuto de órgano a los datos personales para que no puedan ser objeto de tráfico o de manipulación. (Unesco, 2021).

reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos (Ley №8968, 2011, artículo 10).

Este derecho se encuentra estrictamente relacionado con la garantía de confidencialidad que contiene la ley de manera atípica, dentro del derecho de rectificación que tiene que otorgarle todo responsable de datos a los titulares. Lo anterior, permite que la persona pueda solicitar que se respete este derecho, el cual deberá ir de la mano con el desarrollo tecnológico. De la manera como quedó regulado, el responsable deberá hacer todas las acciones necesarias para evitar que se realicen delitos informáticos cuyo objeto sea la información y otras acciones que contravengan la ley de protección de datos personales. De acuerdo con el reglamento, el responsable deberá tomar en cuenta lo siguiente para determinar la seguridad datos:

a. La sensibilidad de los datos personales tratados, en los casos que la ley lo permita.
b. El desarrollo tecnológico.
c. Las posibles consecuencias de una vulneración para los titulares de sus datos personales.
d. El número de titulares de datos personales.
e. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento o almacenamiento.
f. El riesgo por el valor, cuantitativo o cualitativo, que pudieran tener los datos personales; y
g. Demás factores que resulten de otras leyes o regulación aplicable al responsable.

Siendo uno de los derechos de mayor relevancia para proteger la confidencialidad de los datos, se podría esperar que sea un derecho cuyo ejercicio suele ser utilizado de manera frecuente. Sin embargo, ante la Prodhab, hasta la fecha solo se han establecido 401 denuncias relacionadas con el derecho de seguridad de los datos.

7.7.2 La Prodhab y la seguridad digital

Con respecto a esta obligación se puede hacer una diferenciación, entre el sector privado y el sector público, ya que sobre el último la Agencia de Protección de Datos de los Habitantes (Prodhab) deberá tener un papel más activo para garantizar la seguridad digital y la garantía de confidencialidad de los habitantes. Debido a esto es importante analizar las atribuciones que le otorga la ley №8968 a la Prodhab y que se encuentran vinculadas con la seguridad de la información.

Son atribuciones de la Prodhab, además de las otras que le impongan esta u otras normas, las siguientes:

a. Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos.
b. Llevar un registro de las bases de datos reguladas por esta ley.
c. Requerir, de quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo, entre ellas, los protocolos utilizados…
d. **Dictar las directrices necesarias**, las cuales deberán ser publicadas en el diario oficial La Gaceta, **a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales**, respetando los diversos grados de autonomía administrativa e independencia funcional. (Ley №8968, 2011, artículo 16).

Es decir, debe velar por el cumplimiento del derecho de seguridad digital, lo cual debe realizar a través de:

- **La emisión de directrices de seguridad de la información dirigidas a las instituciones públicas:** desde el momento de su creación la Prodhab no ha emitido ninguna directriz.
- **Requerir que los responsables de las bases de datos personales que se encuentran obli-**

gados a inscribir sus bases de datos cuenten con protocolos de actuación: hasta el momento hay 135 bases de datos inscritas, dentro de las cuales no se encuentran bases de datos sensibles como la de Hacienda y EDUS.

- **Recibir notificaciones de incidentes de vulneración de la seguridad de las bases de datos:** si debido a esta notificación la Agencia inicia una investigación, podría imponer una multa si encuentra que la ley ha sido violentada de alguna manera. De acuerdo a la agencia, durante el año 2022 se han recibido 6 reportes de vulneración de bases de datos de parte de empresas privadas y de dos Instituciones Públicas.

Como puede verse, la normativa brinda unos requisitos mínimos que debe seguir toda organización que le interesa proteger la información personal y que tiene la obligación de resguardar, por lo que si cuando se inscribe la Prodhab hace una buena labor, puede asegurarse que el responsable de la base de datos haya recorrido pasos básicos hacia una protección de la información de los datos. En caso de un tratamiento no adecuado podrá utilizar todas las herramientas que le confiere la ley, dentro de las cuales están el imponer multas.

7.7.3 Costa Rica en el índice Global de Ciberseguridad 2020

Como lo indica el Castro-Obando (2021) en el capítulo 1 del Informe Hacia la Sociedad de la Información y el Conocimiento 2021, nuestro país se encuentra en la posición número 8 de la región, ganando 10 posiciones con respecto al año 2019. Lo más interesante, es que en donde mejor destaca Costa Rica es en el componente legal:

> Considerando que cada pilar puede alcanzar una calificación máxima de 20 puntos, **resulta evidente que las dimensiones más avanzadas al 2020, fueron las relacionadas con medidas legales y de cooperación,** aunque también se dio un progreso importante en cuestiones organizacionales y en el desarrollo de capacidades destinadas a fortalecer la seguridad cibernética en el país.
>
> A pesar de esto, **la puntuación en el pilar técnico sigue siendo baja** y muestra la necesidad de realizar acciones que contribuyan al fortalecimiento de las capacidades de implementación de las instituciones y organizaciones encargadas de la seguridad cibernética en Costa Rica. (Castro-Obando, 2020, p.47.)

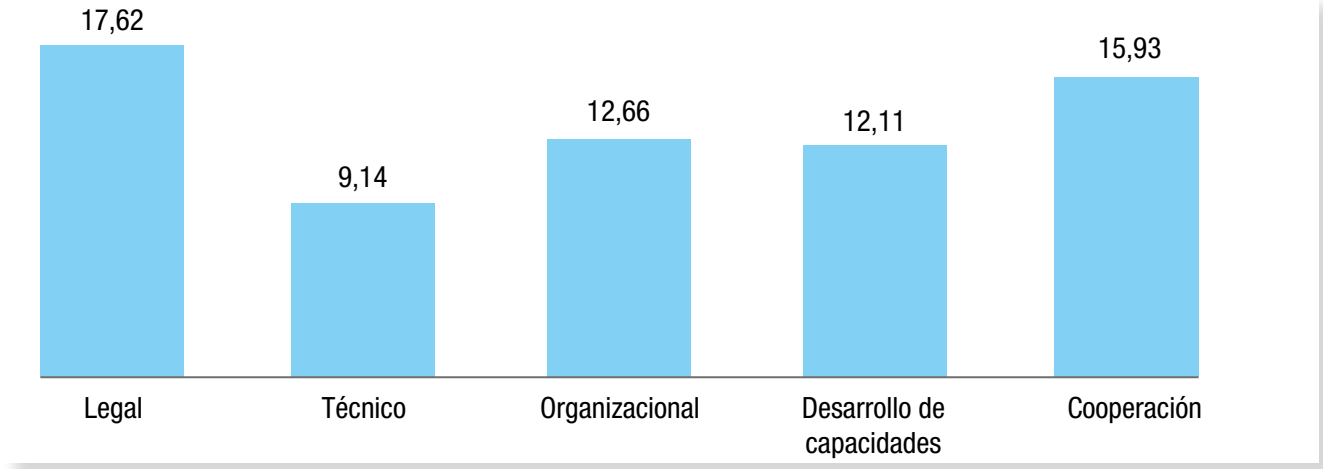


Figura 7.8. Puntuación obtenida por Costa Rica en el Índice Global de Ciberseguridad 2020 -por pilar-

Fuente: Tomado de Castro-Obando, 2021.

Lo anterior refleja una realidad importante, las reformas al Código Penal sobre delitos informáticos, la ley de protección de datos personales[14] (№8968) y la adhesión de nuestro país al Convenio Europeo sobre Ciberdelincuencia han tenido un impacto positivo en la percepción de ciberseguridad que tiene el país, a pesar de que en lo técnico existan falencias y que en la práctica lo legal no se está verdaderamente cumpliendo.

7.7.4. El derecho de libertad de expresión en el ciberespacio

De acuerdo con nuestra Constitución Política, todos pueden comunicar sus pensamientos de palabra o por escrito, y publicarlos sin previa censura; pero serán responsables de los abusos que cometan en el ejercicio de este derecho, en los casos y del modo que la ley establezca. (Constitución Política de Costa Rica, 1949, artículo 29). La libertad de expresión ha sido potenciada en el ciberespacio por plataformas y algoritmos que le permiten a las personas manifestarse de múltiples maneras, sin intermediarios, hasta de manera gratuita, con la posibilidad de lograr un alcance que en el siglo pasado solo era posible para los grandes medios de comunicación. Este cibermundo de oportunidades le permite a todos los sectores de la población manifestarse, sin que exista una adecuada comprensión de los alcances de sus acciones y las consecuencias que esto le puede traer a su vida.

La Constitución Política de Costa Rica, en su numeral 28, busca darle garantía a las personas para que puedan manifestarse libremente, sin que puedan ser perseguidas o inquietadas por:

> La manifestación de sus opiniones ni por acto alguno que no infrinja la ley.
>
> Las acciones privadas que no dañen la moral o el orden públicos, o que no perjudiquen a tercero, están fuera de la acción de la ley.
>
> No se podrá, sin embargo, hacer en forma alguna propaganda política por clérigos o seglares invocando motivos de religión o valiéndose, como medio, de creencias religiosas. (Constitución Política de Costa Rica, 1949, artículo 28).

Sin lugar a duda, este mandado constitucional presenta enormes desafíos para respetarse en el ciberespacio, ya que los entornos digitales presentan características que no era posible imaginar en la Costa Rica de a mediados del siglo pasado. Los desafíos relacionados con el ciberespacio son:

1. Manifestación de los pensamientos en entornos sin ubicación geográfica definida y sin límite con respecto a su alcance.
2. Medios de comunicación alojados en servidores en el extranjero.
3. Espacios de opinión masiva sin control editorial.
4. Dependencia de todos los sectores de la sociedad sobre medios controlados por empresas extranjeras desde otras naciones.
5. Impacto global de las comunicaciones creadas desde Costa Rica.
6. Regulación internacional sobre protección de datos personales.
7. Autorregulación de las plataformas tecnológicas.

De la mano de estos desafíos, los abusos de las bondades de la tecnología pueden provocar problemas como:

1. **Desinformación masiva**: desde información falsa relacionada con temas de salud hasta los relacionados con temas electorales.
2. **Acoso cibernético:** las comunicaciones digitales pueden utilizarse para acosar de manera insistente a las personas. En el año 2018 se presentó el proyecto de ley №21187, el cual

14 Ley de Protección de la personal frente al tratamiento de sus datos personales.

que buscaba sancionar esta conducta y la difusión de información falsa con fines electorales.

3. **Manifestación del odio**: una clase de contenido que ha proliferado en internet son las manifestaciones de odio por razones de etnia, preferencia sexual, creencias religiosas, entre otras. En países como España se sancionan algunos delitos de odio.
4. **Delitos informáticos**: delitos como la violación de correspondencia o comunicaciones, violación de datos personales, pornografía infantil, entre otros son comunes en los entornos tecnológicos.

El delito de violación de correspondencia o comunicaciones y su impacto en la libertad de prensa

En nuestro país, el delito de violación de correspondencia o comunicaciones del Código Penal, en su párrafo segundo, sanciona con penas de 1 a 3 años, la divulgación del contenido de documentos o comunicaciones privadas de manera expresa, pero excluye toda sanción cuando la acción se realiza en interés público:

> La misma sanción indicada en el párrafo anterior se impondrá a quien, con peligro o daño para la intimidad de otro, utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público. (Código Penal de Costa Rica, 1970, artículo 196, párrafo segundo).

De manera interesante, nuestro Código Penal sí sanciona penalmente al delincuente informático que captura ilegalmente la información de interés público para su posterior difusión, por lo que no se debilita la protección penal ante los accesos ilegales, ya que no sería de recibo que algún ciudadano decida vulnerar todos los sistemas informáticos de empresas o instituciones públicas con el fin de encontrar evidencia de algún acto de corrupción para luego alegar que es una actividad de interés público.

La reforma finalmente permitió que tan solo 3 años después con los *Panama Papers (2016)*, los medios de comunicación tuvieran mayor seguridad jurídica al dar cobertura mediática con contenido confidencial en los casos Cochinilla (2021) y Pandora Papers (2021). Esta libertad puede generar un debate con respecto a temas éticos o morales, pero lo que no se puede negar es que fortalece la libertad de expresión en un país. Aunque todavía hay espacio para una regulación que incorpore principios de protección de datos personales, se puede decir que el país salió fortalecido.

En el caso de *Panama Papers*, se filtraron documentos y el contenido de comunicaciones electrónicas confidenciales, los cuales se encontraban bajo el resguardo de una firma legal, la cual fue víctima de una extracción y divulgación de la información de sus clientes para quienes realizaban actos que aunque no necesariamente fuesen delictivos, sí podrían tener roces éticos o de índole moral, principalmente desde la perspectiva tributaria. Infobae lo explica de la siguiente manera:

> Con el nombre de los Panama Papers se conoce a la investigación periodística global liderada por el Consorcio Internacional de Periodistas de Investigación (ICIJ, por sus siglas en inglés), que expuso a la luz los negocios offshore de políticos, empresarios, deportistas y celebrities internacionales.
>
> Se basó en la filtración de 11,5 millones de documentos internos del estudio panameño Mossack Fonseca, la más grande en la historia del periodismo y la que tuvo -y sigue teniendo- mayor impacto a nivel mundial.
>
> Los archivos incluyeron correos electrónicos, listados de sociedades, beneficiarios, actas, escrituras y registros de sociedades offshore intercambiados entre Mossack Fonseca y sus

> clientes, en los últimos 40 años. Fueron filtrados por una fuente anónima al diario alemán Süddeutsche Zeitung, y compartidos por ICIJ con más de 370 periodistas miembros de la organización en 76 países. La información incluyó datos de cuentas bancarias y de 214.488 empresas offshore conectadas con más de 200 países.
>
> Hasta las primeras revelaciones periodísticas conocidas a nivel mundial en simultáneo el 3 de abril de 2016, la gran mayoría de estas firmas creadas en jurisdicciones consideradas paraísos fiscales -por su baja o nula tributación y el anonimato de sus dueños- se mantenían ocultas. (Fitz, 2019, párr. 1-4)

En nuestro país, el medio de comunicación DatabaseAR de Ameliarueda.com y El Semanario Universidad se encargaron de analizar los datos filtrados y hacer distintas publicaciones en donde se expuso a distintas figuras públicas de nuestro país. Esto no estuvo exento de controversia, ya que como lo relata el Observatorio de Política Pública (OPI) de la Universidad de Costa Rica, inclusive distintos medios fueron críticos con respecto al manejo que le dieron estos medios a la información:

> En Costa Rica, ese tipo de operaciones financieras las realizaron desde políticos hasta empresarios y banqueros relacionados con diversas empresas como Pipasa, Borda Azul, HI-C, Improsa, entre otras, y medios de comunicación como Grupo Nación y Crhoy.com. El reportaje completo y la lista de personas y empresas vinculadas en Costa Rica con este tipo de actividades, que se pueden catalogar de especulativas, están en los reportajes que han hecho en profundidad el Semanario Universidad y DataBase. Sin embargo, los esfuerzos hechos por estos dos medios de comunicación nacional han sido criticados de una u otra forma en sus notas y noticias por otros medios de comunicación vinculados con las personas que han realizado estas operaciones financieras con la firma Mossack Fonseca en el país. Es el caso de algunas notas periodísticas del medio Crhoy.com, en donde se critica específicamente al Semanario Universidad, por medio de varios entrevistados, por haber realizado una investigación superficial, y se le acusa de tergiversar la información y difamar a las personas que efectuaron ese tipo de operaciones financieras en el país con la firma Mossack Fonseca (Observatorio de Política Pública [OPI], 2016, párr. 3).

Aunque se pueda discutir sobre la calidad del análisis de la información e inclusive sobre si era necesario incluir a ciertas personas, el interés público de esta filtración es innegable. A raíz de esta filtración, la Asamblea Legislativa abrió una comisión especial investigadora dirigida a identificar mecanismos o prácticas utilizadas para eludir o evadir tributos, así como las deficiencias, vacíos y omisiones que pueda tener la legislación costarricense para la adecuada fiscalización y recaudación tributarias.

Un elemento que merece antención es el cómo una filtración de datos de una empresa privada genera una enorme discusión de interés público a nivel internacional, lo que antes hubiese sido solo posible con la filtración de información de algún gobierno, ahora hace que cualquier persona se encuentre expuesta al escrutinio público.

Descentralización de internet y autorregulación

En un mundo globalizado en el cual nuestros principales medios de comunicación utilizan plataformas digitales de empresas extranjeras que se rigen por una regulación estadounidense, la cual es flexible y propicia la autorregulación, se generan grandes retos sobre la libertad de expresión de los ciudadanos y hasta del Estado costarricense, por la posible censura si no se cumplen las normativas internas de dichas empresas.

La legislación estadounidense le ha brindado amplias potestades a las empresas tecnológicas en cuanto a la moderación de sus usuarios y la exclusión de responsabilidad sobre los contenidos que estos publiquen. En 1996, la sección 230 de la Ley de la Decencia de las comunicaciones fue promulgada para permitir una mayor libertad en un sector que requiere de esta para poder seguir innovando y crecer. En este sentido se ha pronunciado la Fundación Frontera Electrónica (EFF, por sus siglas en inglés):

> La Sección 230 dice que "Ningún proveedor o usuario de un servicio informático interactivo será tratado como el editor o portavoz de cualquier información proporcionada por otro proveedor de contenido de información" (47 U.S.C.§ 230).
>
> En otras palabras, **los intermediarios en línea que alojan o vuelven a publicar discursos están protegidos contra una serie de leyes que, de otro modo, podrían utilizarse para responsabilizarlos legalmente por lo que otros dicen y hacen.** Los intermediarios protegidos incluyen no solo los proveedores de servicios de Internet (ISP) habituales, sino también una serie de "proveedores de servicios informáticos interactivos", que incluyen básicamente cualquier servicio en línea que publique contenido de terceros.
>
> Aunque existen importantes excepciones para ciertas reclamaciones penales y basadas en la propiedad intelectual, CDA 230 crea una amplia protección que ha permitido que prospere la innovación y la libertad de expresión en línea. (EFF, 2015, párr. 3)

Previo a esta ley, los medios de comunicación electrónicos en los Estados Unidos podían ser tratados como editores, lo que conllevaba responsabilidades que hubiese impactado la libertad que tanto caracteriza el internet occidental moderno, por lo que su importancia es de gran relevancia:

> Antes de 1996, la ley sobre responsabilidad legal por la distribución del discurso de otras personas se basaba en un fallo judicial de 1959.
>
> El caso se centró en Eleazer Smith, el propietario de 72 años de una librería en South Main Street en el centro de Los Ángeles. Fue arrestado por un oficial del LAPD por vender una copia de una novela sobre una despiadada agente inmobiliaria lesbiana considerada obscena bajo la ciudad y Ley del Estado.
>
> Smith argumentó que no podía revisar todos los libros en su tienda, y su caso llegó a la Corte Suprema. Allí, el tribunal decidió que Smith tenía razón, y podría ser encontrado en violación de la ley solo si no retiraba el libro después de ser informado de que era ilegal venderlo. En los años posteriores, los tribunales confirmaron esa distinción legal entre distribuidores como las librerías y editoriales de los periódicos.
>
> La Sección 230 hizo explícito en su lenguaje que un sitio web no podía ser tratado como un editor o un portavoz, lo que teóricamente dejó la puerta abierta para que fueran tratados como una librería; de hecho, así es como el juez describió CompuServe en uno de los primeros casos de sitios de Internet. (Deam, 2020, párr. 18-21)

Derecho de rectificación en página de Facebook

La Sala Constitucional costarricense niega el derecho de rectificación a un administrado en una página de Facebook, al considerar que no es un medio de comunicación o difusión:

> **se denota que el mensaje que genera la disconformidad del recurrente no se dio a través de un medio de comunicación o difusión, sino en la página de Facebook del**

Ministerio accionado. **Esta situación conlleva que la figura del derecho de rectificación o respuesta no resulta aplicable al caso en estudio,** toda vez que los numerales 66 y siguientes de la Ley de la Jurisdicción Constitucional establecen expresamente dicho requisito para que pueda ejercerse el derecho antes citado. De esta forma, si el recurrente considera que la publicación hecha en las redes sociales de la autoridad recurrida resulta improcedente, cuenta con la posibilidad de recurrir a la vía de legalidad ordinaria, donde podrá ejercer los remedios previstos por el ordenamiento jurídico para hacer valer sus derechos, en caso de estimarlo procedente…

V.- Ahora bien, sin demérito de lo externado en el considerando anterior, la mayoría de la Sala considera necesario mencionar que actualmente existe un debate, en el ámbito doctrinal y jurisprudencial, que apenas comienza[15], en el sentido de si es posible o no ejercer el derecho de rectificación y respuesta en las redes sociales internet, Facebook, Twitter, etc. Incluso, hay algunos estados que han dado una respuesta afirmativa frente al desarrollo de la tecnología en las comunicaciones, toda vez que el alcance, impacto y la permanencia en el tiempo de la información es mayor que un medio de difusión tradicional.

De ahí que algunos tribunales hayan admitido el ejercicio del derecho de rectificación y respuesta en las redes sociales, no solo para ordenar que se elimine la información inexacta o agraviante, sino para se otorgue el derecho de rectificación y respuesta en las redes sociales. En esta dirección se puede consultar las sentencias n.° STL 11943-2014 emitida por la Sala de Casación Laboral de la Corte Suprema de Justicia de Colombia y n.°s. T-050/16 y T-063A/17 de la Corte Constitucional de ese mismo estado.

Hay que aclarar que en Colombia se promulgó la Ley n.° 1341 de 2009 que regula el uso de las tecnologías de la información y comunicación, la que, en su artículo 70, estatuye que se garantiza el derecho de rectificación y respuesta a toda persona o grupo de personas que se consideren afectados por información inexacta que se transmita a través de los servicios de telecomunicaciones -en el numeral 6 de esa normativa se define qué se entiende por uso de tecnología de la información y comunicación-.

Adoptando como marco de referencia lo anterior, es importante advertir que el ordenamiento jurídico costarricense muestra un desfase con la realidad muy importante -asunto de lege ferenda, por lo que hay una serie de situaciones e interrogantes que no encuentran un cauce procesal rápido y sencillo para proteger al habitante de la República en aquellos casos en los cuales, a causa de una información inexacta o expresión agraviante, se le vulnera su derecho al honor, el buen nombre o reputación.

Más grave aún, es el supuesto del uso de redes sociales de órganos y entes públicos, cuando a causa de una publicación se afecta el derecho al buen nombre de una persona. Así, desde la perspectiva de la mayoría del Tribunal, el estado en que se encuentra el ordenamiento jurídico costarricense impone una reflexión colectiva para conciliar la libertad de información y expresión y el derecho al honor en las redes sociales. (Sala Constitucional, Resolución N° 21306 – 2020).

Es preocupante cómo la Sala Constitucional reconociendo que hay una problemática que afecta dere-

15 La Sala Constitucional indica que el debate apenas comienza, cuando la resolución es del 2020 y como indicamos anteriormente en España desde el 2018 se reconoce de manera expresa el derecho de rectificación en internet.

chos fundamentales, que inclusive ha sido regulada en países como Colombia de manera expresa en la ley, decida no proteger al ciudadano con una interpretación tan absurda como indicar que una página de Facebook no es un medio de difusión.

Bloqueo, ofensas, derecho a comentar y la moderación en medios sociales de instituciones públicas

No se puede bloquear a un usuario sin una debida razón, lo que de cierta manera le permite a la institución pública establecer una política de moderación:

> De la sentencia parcialmente transcrita se colige que las redes sociales como Facebook, no solo proveen información, sino que, además, son un canal para expresarse. Por ello, **es que no puede una autoridad pública válidamente bloquear de Facebook a un usuario, sin que exista una razón que lo justifique de por medio,** que en este caso, debido a la omisión de la accionada de informar sobre este punto en concreto, se desconoce si la hubo. Lo que sí se tiene como cierto es que la cuenta se encuentra bloqueada, con la afectación que ello conlleva a los derechos fundamentales de la amparada, como el de expresión. Por tales motivos, es que el amparo sí debe estimarse en cuanto este punto se refiere. (Sala Constitucional, Resolución No 01988 - 2015)

Si una institución pública decide que va a tener presencia en medios sociales, le debe permitir a los ciudadanos comentar en las mismas. Por esto no puede utilizar las herramientas que permiten desactivar comentarios:

> En el escrito de interposición que originó este recurso de amparo, la parte recurrente alegó que las autoridades del MEP publicaron un video que fue enviado por correo electrónico a todos los funcionarios ese ministerio y a la comunidad estudiantil, titulado: "Mensaje de la Ministra de Educación sobre el mantenimiento de la educación combinada". Ahora bien, se ha tenido por demostrado que el MEP tiene una cuenta en la plataforma YouTube denominada "Ministerio de Educación Pública de Costa Rica". Se constata que el 26 de abril de 2021, el MEP publicó en redes sociales el video llamado "Mantenimiento de la Educación Combinada en Centros Educativos" tanto en el Facebook como en el canal de YouTube del MEP. El canal de YouTube del MEP no tenía habilitada la opción de comentarios, pero el 05 de mayo de 2021 esta opción fue habilitada. El mencionado video del MEP permite la recepción de comentarios en la plataforma de YouTube. De la revisión del video en cuestión, se desprende que el recurrente ya pudo hacer sus comentarios respecto al contenido del mensaje dado por la señora Ministra de Educación Pública. (Sala Constitucional, Resolución No 14043 - 2021)

Incluso ser funcionario que trabaje en la misma institución titular de la cuenta no le impide ejercer este derecho a comentar e inclusive criticar a su patrono:

> El hecho de que a un funcionario público se le abra un procedimiento administrativo por realizar un comentario genérico sobre el desempeño de los jefes en la corporación municipal constituye una medida excesiva de la Administración Pública que limita su libertad de expresión.
>
> Es bien sabido que las limitaciones a la libertad de expresión y de información están sometidas a un test estricto de razonabilidad, lo cual significa, ni más ni menos, que toda acto o medida que la restrinja es sospechoso, por lo que la autoridad pública tiene la carga de la prueba de demostrar que hay un interés público apremiante, plenamente justificado, en la medida o acto, así como el deber de demostrar que la medida o acto adoptado es la menos

gravosa para el derecho fundamental, amén que debe de interpretarse restrictivamente.

Concretamente, debemos verificar que la finalidad perseguida con la apertura del procedimiento administrativo es legítima, importante e imperiosa; que es un medio adecuado, efectivamente conducente y además necesario y que no pueda ser remplazado por un medio alternativo menos lesivo; y adicionalmente, se debe aplicar un juicio de proporcionalidad en sentido estricto mediante el cual se verifique que los beneficios de la apertura del procedimiento administrativo excedan claramente las restricciones impuestas a la libertad de expresión…

En otro orden de ideas, no cabe duda que en la sociedad democrática los funcionarios públicos estamos en el deber de soportar frases mortificantes, todo ello en garantía de una libertad que constituye un presupuesto esencial del Estado social y democrático de Derecho. En este caso, **es mejor tolerar un exceso de naturaleza genérico que restringir indebidamente la libertad de expresión**, especialmente que la afirmación, que tanto molesta al jerarca de la municipalidad de San José, no se dirige a ninguna persona específica. De ahí que resulta procedente acoger el recurso de amparo, como en efecto se hace. (Sala Constitucional, Resolución No 07500 - 2015).

Los funcionarios pueden bloquear usuarios, siempre que no sea en las cuentas institucionales

La Sala sin entrar a analizar si al ciudadano se le estaba violando el derecho de acceso a información pública por el uso que le podría dar una alcaldesa a su cuenta en Facebook, decide no reconocerle derecho alguno, sin hacer un análisis adecuado:

> De los hechos que se tienen por debidamente demostrados en este asunto, se advierte que ninguno de los precedentes anteriores es plenamente aplicable al mismo. Aquí el Recurrente lo que alega es que se lesionó su derecho de libertar de expresión, luego de haber hecho comentarios en la cuenta privada de la Alcaldesa tiene en Facebook, dicha funcionaria bloqueó el acceso del recurrente a esa cuenta. *Se advierte que no se trata de la cuenta institucional de la Municipalidad de Naranjo, razón por la cual este Tribunal considera que no existe la lesión que el recurrente alega, pues no existe un derecho fundamental a tener acceso a las cuentas personales de ningún particular, tampoco cuando este ostente un cargo público*. (Sala Constitucional, Resolución No 01988, 2015).

En otro caso similar, en una cuenta de una diputada, la Sala resuelve de manera similar, pero se extiende al decir que las ofensas no tienen protección constitucional:

> Así por ejemplo, carecen de protección Constitucional, los insultos o los juicios de valor formalmente injuriosos e innecesarios para la expresión de una idea, pensamiento u opinión, de modo que, en el sub-lite, la Sala no encuentra que el bloqueo, aplicado al recurrente, en la red social de "Facebook" lesione su libertad de expresión. (Sala Constitucional, Resolución No 1453,2019).
>
> En otro caso, en donde los comentarios estaban relacionados con una página de Facebook del Banco de Costa Rica, negó protección al ser un amparo contra particulares, en donde el banco realizó su acción en su capacidad de derecho privado (Sala Constucional, Resolución No 03871 - 2018)

En los Estados Unidos, en un caso similar a los anteriores, en donde un político en su página de Facebook bloquea a un particular y otro donde el expresidente Trump bloqueó a un ciudadano en su cuenta de Twitter, los tribunales estadounidenses analizaron

el concepto de foro público, la restricción al acceso a información de interés público debido a la manera oficial en las cuales utilizaban los funcionarios sus cuentas en medios sociales, más allá de que si no existiese una obligación legal de mantener estas mismas activas[16].

Bloqueo de periodista en chat grupal de Ministerio

Un periodista interpone un recurso de amparo aduciendo temas de moderación es removido de un grupo de Whatsapp dirigido a prensa. En apariencia la persona había violado las reglas al compartir un enlace de un medio para aclararle a otro colega sobre un tema, por lo que la Sala considera que fue una medida desproporcionada, aunque reconoce que existe posibilidad de moderación:

> V.- Primeramente, se debe aclarar que **esta Sala no objeta que existan reglas de cordialidad que los participantes del grupo deban respetar.** Por otra parte, tampoco desaprueba que se puedan imponer límites, **incluso la separación temporal del grupo, a quienes irrespeten las reglas preestablecidas, siempre y cuando tales límites sean razonables, las regla, fijadas previamente,** sean suficientemente claras y se refieran a conductas que generen algún perjuicio a otros participantes. Es decir, debe existir una necesaria relación de proporcionalidad entre la conducta censurable y la consecuencia y esa relación debe estar clara desde el momento en que se establecen las reglas. Ahora bien, a juicio de este Tribunal, en este caso concreto, una expulsión indefinida, es decir, no sujeta a ningún plazo, no resulta de ninguna manera razonable. Ciertamente, el Ministerio de Seguridad Pública advirtió, en general, a los participantes sobre la posible exclusión y puso en conocimiento las reglas de cordialidad, pero no consta que se indicaran con claridad las consecuencias por no observarlas y, en todo caso, solamente se menciona la exclusión del grupo y sin ningún tipo de gradualidad. En relación específica con el recurrente, solo consta que hizo una única intervención aclaratoria, que, como tal, no se observa que perjudique a los demás participantes. No se trata de propaganda ni de comentarios ofensivos o irrespetuosos.
>
> En consecuencia, la exclusión definitiva que se le impuso es totalmente desproporcionada. Ciertamente, existen otros medios por los cuales el recurrente continúa recibiendo información, pero no se puede perder de vista que el grupo "Prensa MSP-Medios" es un canal de carácter oficial creado por la Oficina de Prensa de una institución pública, de manera que las limitaciones impuestas a sus miembros deben guardar armonía con los principios constitucionales. En consecuencia, la decisión del Ministerio de Seguridad Pública, desproporcionada como tal, pone además al comunicador en desventaja al privarlo de una forma fluida de recibir la información. En consecuencia, de conformidad con las razones expuestas, se impone estimar el recurso. (Resolución Nº 17051,2018).

7.8. EL DERECHO AL TESTAMENTO DIGITAL

La vida digital de un costarricense está compuesta por sus acciones, obras, posesiones, conexiones e información que no necesariamente se encuentra bajo su control, pero que le afectan en su vida personal y profesional más allá de las fronteras del ciberespacio. Mientras la persona se encuentra con vida, utilizará todas las herramientas y ejercerá los derechos que le permitan tener un control sobre su vida en el ciberespacio. Sin embargo, los datos que comprenden

16 En el Tribunal de Apelaciones de los Estados Unidos para el Segundo Circuito, Knight First Amendment Institute, et al v. Donald J. Trump, et al.

su vida digital suelen estar alojados principalmente en servidores ubicados fuera del territorio nacional, por lo que el gobierno de estos entornos digitales se regirá por regulación extranjera, la normativa de las plataformas y/o las reglas contenidas en contratos inteligentes, lo cual representa un desafío mayor cuando la persona fallece.

El patrimonio de un usuario de internet puede incrementarse con su actividad en línea, debido a la adquisición de bienes digitales, apertura de cuentas, producción de obras, entre otras acciones que pueden tener un valor económico, como las siguientes:

1. **Obras de su propiedad o licencias de disfrute de obras digitales (Música, películas, contenido audiovisual, entre otros).** Una persona puede ir adquiriendo o produciendo contenido, el cual puede tener todavía más valor que un bien inmueble. Un ejemplo de esto sería el caso de un Token No Fungibles (NFT), el cual puede valer en algunos casos millones de dólares.
2. **Criptomonedas** (por ejemplo, Bitcoin, Ethereum, Monero). Una sola unidad de una criptomoneda puede tener más valor que una propiedad, lo que genera la necesidad de buscar una solución para poder heredarlas sin que esto conlleve debilitar la seguridad informática del sistema. Lo anterior no tiene una solución fácil para personas que tienen sus criptomonedas en monederos más seguros, en donde solo ellos tienen el control de la llave privada.
3. **Cuentas en medios sociales** (Páginas de Facebook, canales de Youtube, cuenta de Twitter). Una cuenta en un medio social con una gran audiencia puede tener un gran valor de mercado, por lo que es cada vez más común encontrarse con personas cuyas grandes audiencias les han generado una verdadera fortuna.
4. **Dominios web (.com, .net, org).** El corazón de un comercio en línea o de la presencia digital de una persona, marca u organización puede encontrarse en un dominio el cual de manera orgánica puede atraer millones de visitas y de los cuales depende un proyecto digital para ser exitoso**.**
5. **Aplicación** (Para el móvil, escritorio u otra plataforma). Una aplicación que se encuentre alojada en una tienda de aplicaciones puede representar un negocio por sí mismo, el cual puede generar dinero a través de anuncios publicitarios, compras dentro de la aplicación o por la compra de la licencia para usarla por parte de los usuarios. La autorregulación ha sido la solución para esta problemática, ya que muchas plataformas están permitiendo a los herederos acceder al contenido, sin embargo, depende mucho de la buena voluntad de cada empresa tecnológica, con respecto a dar el paso de reconocer este derecho. Por otro lado, con respecto a los datos personales, la ley №8968 permite que los herederos ejerzan los derechos propios de la autodeterminación informativa del fallecido.

7.9. EL DERECHO DE DESCONEXIÓN DIGITAL EN EL CONTEXTO DEL TELETRABAJO

A las personas teletrabajadores la Ley № 10168 (2022), que reforma la Ley de Teletrabajo, les reconoce el derecho a la desconexión digital, con el grave error que permite que el trabajador pueda ser contactado para emergencias, dejando un gran espacio para la interpretación y en donde el derecho podría resultar inútil. Esto se establece en el artículo 9 de dicha norma, en el que se menciona explícitamente que

> Sin perjuicio de lo dispuesto en el párrafo anterior y con el fin de garantizar el respeto de su tiempo de descanso, vacaciones, permisos y su intimidad personal y familiar, la persona teletrabajadora tendrá derecho a la desconexión

digital fuera de la jornada u horario establecido, salvo que se trate de situaciones imprevistas y urgentes, en las que se debe contar con su anuencia. (Ley 9738, 2019, artículo 9).

7.10. DERECHO DE ACCESO A INTERNET

El acceso a internet en la actualidad se convierte en un habilitador del desarrollo personal, tanto a nivel intelectual, económico como cultural. La Sala Constitucional, de manera valiente y visionaria ha decidido reconocerlo como un derecho fundamental:

> interpuso recurso de amparo y manifestó que reside en Alajuelita, específicamente detrás del Liceo de esa localidad. Indica que **se presentó ante el instituto recurrido a solicitar el servicio de Internet residencial, pero se le denegó el servicio aduciendo que no había cobertura en el lugar donde vive**. Menciona que **el acceso a la Internet fue contemplado recientemente como un derecho fundamental, por lo cual considera que la denegatoria violenta sus derechos fundamentales**, todavía con más razón si se toma en cuenta que lo requiere para sus estudios universitarios…
>
> V.- DERECHOS FUNDAMENTALES CONCULCADOS. En cuanto a este último punto, debe decirse que el avance en los últimos veinte años en materia de tecnologías de la información y comunicación (TIC´s) ha revolucionado el entorno social del ser humano. Sin temor a equívocos, puede afirmarse que estas tecnologías han impactado el modo en que el ser humano se comunica, facilitando la conexión entre personas e instituciones a nivel mundial y eliminando las barreras de espacio y tiempo**. En este momento, el acceso a estas tecnologías se convierte en un instrumento básico para facilitar el ejercicio de derechos fundamentales como la participación democrática (democracia electrónica) y el control ciudadano, la educación, la libertad de expresión y pensamiento, el acceso a la información y los servicios públicos en línea, el derecho a relacionarse con los poderes públicos por medios electrónicos y la transparencia administrativa, entre otros**. Incluso, se ha afirmado el carácter de derecho fundamental que reviste el acceso a estas tecnologías, concretamente, el derecho de acceso a la Internet o red de redes. Resolución Nº 04142 – 2011).
>
> V.- B- Sobre los derechos fundamentales a la información y la comunicación.
>
> En este caso concreto, por el servicio público en cuestión –el servicio de telecomunicaciones- también están involucrados otros dos derechos fundamentales, el derecho a la comunicación y el derecho a la información.
>
> En cuanto a estos derechos, **debe indicarse que, a la luz de la sociedad de la información y del conocimiento actual, el derecho de todas las personas de acceder y participar en la producción de la información, y del conocimiento, se vuelve una exigencia fundamental, por ello tal acceso y tal participación deben estar garantizados a la totalidad de la población.**
>
> Si bien son derechos relacionados con otros, tales como la libertad de expresión, y la libertad de prensa, estos derechos tienen su particularidad propia. Asimismo, aunque se perfilan más claramente en la actualidad, tienen sus raíces en la Declaración Universal de Derechos Humanos, promulgada el 10 de diciembre de 1948, cuando señala en su artículo 19º que "todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión", y en la Convención America-

na sobre Derechos Humanos, promulgada el año 1969 (Pacto de San José), cuando indica que la libertad de pensamiento y expresión comprenden "...la libertad de buscar, recibir y difundir información e ideas. (Sala Constitucional - Res. Nº 10627-10).

En este contexto de la sociedad de la información o del conocimiento, se impone a los poderes públicos, en beneficio de los administrados, promover y garantizar, en forma universal, el acceso a estas nuevas tecnologías.

Partiendo de lo expuesto, concluye este Tribunal Constitucional que el retardo verificado en la apertura del mercado de las telecomunicaciones ha quebrantado no solo el derecho consagrado en el artículo 41 de la Constitución Política sino que, además, ha incidido en el ejercicio y disfrute de otros derechos fundamentales como la libertad de elección de los consumidores consagrada en el artículo 46, párrafo in fine, constitucional, el derecho de acceso a las nuevas tecnologías de la información, el derecho a la igualdad y la erradicación de la brecha digital (infoexclusión) –artículo 33 constitucional-, el derecho de acceder a la internet por la interfase que elija el consumidor o usuario y la libertad empresarial y de comercio. (Sala Constitucional - Res. Nº 10627 – 10).

7.11. LA LABOR DE LA PRODHAB

La Agencia de Protección de Datos de los Habitantes desde su creación ha tenido grandes problemas para cumplir con las atribuciones que se le han asignado por ley e inclusive para consolidarse como la defensora de la autodeterminación informativa en Costa Rica. La Prodhab recibe entre 67 y 133 denuncias por mes, de las cuales el 83% corresponde a infracciones por parte del sector privado. Además, debido a que todavía no se están publicando las resoluciones de la agencia no sabemos el resultado de estas denuncias y el fundamento legal.

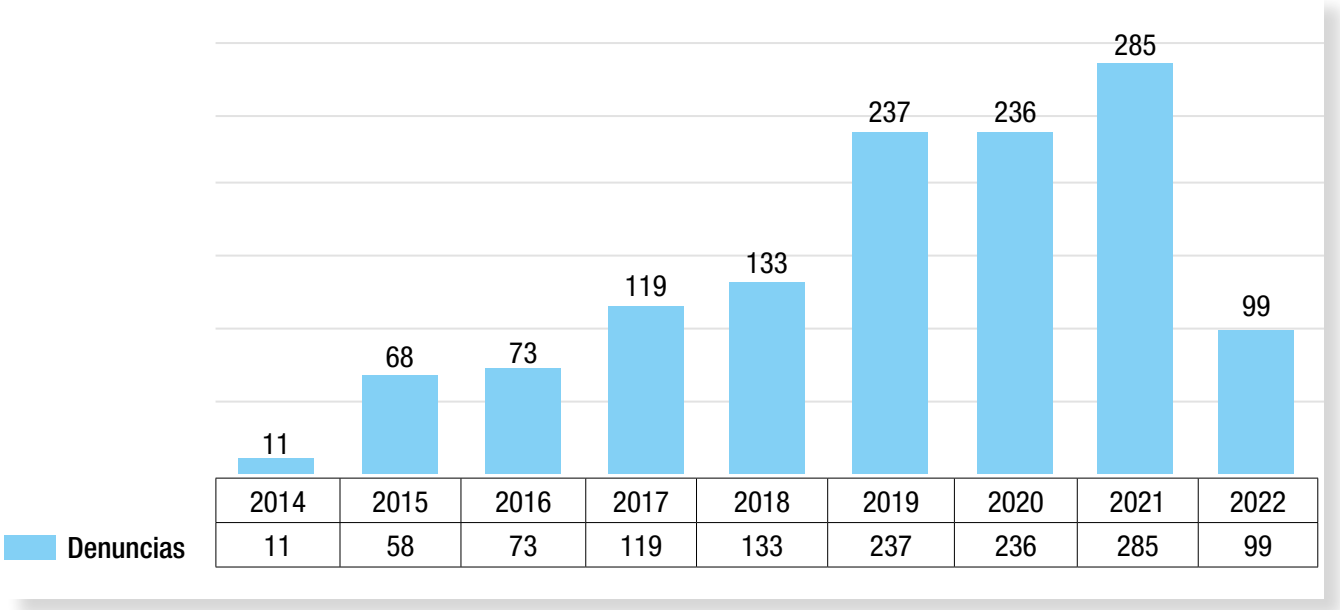


Figura 7.9. Denuncias recibidas por la Prodhab (2014-2022)

Fuente: Prodhab, 2022.

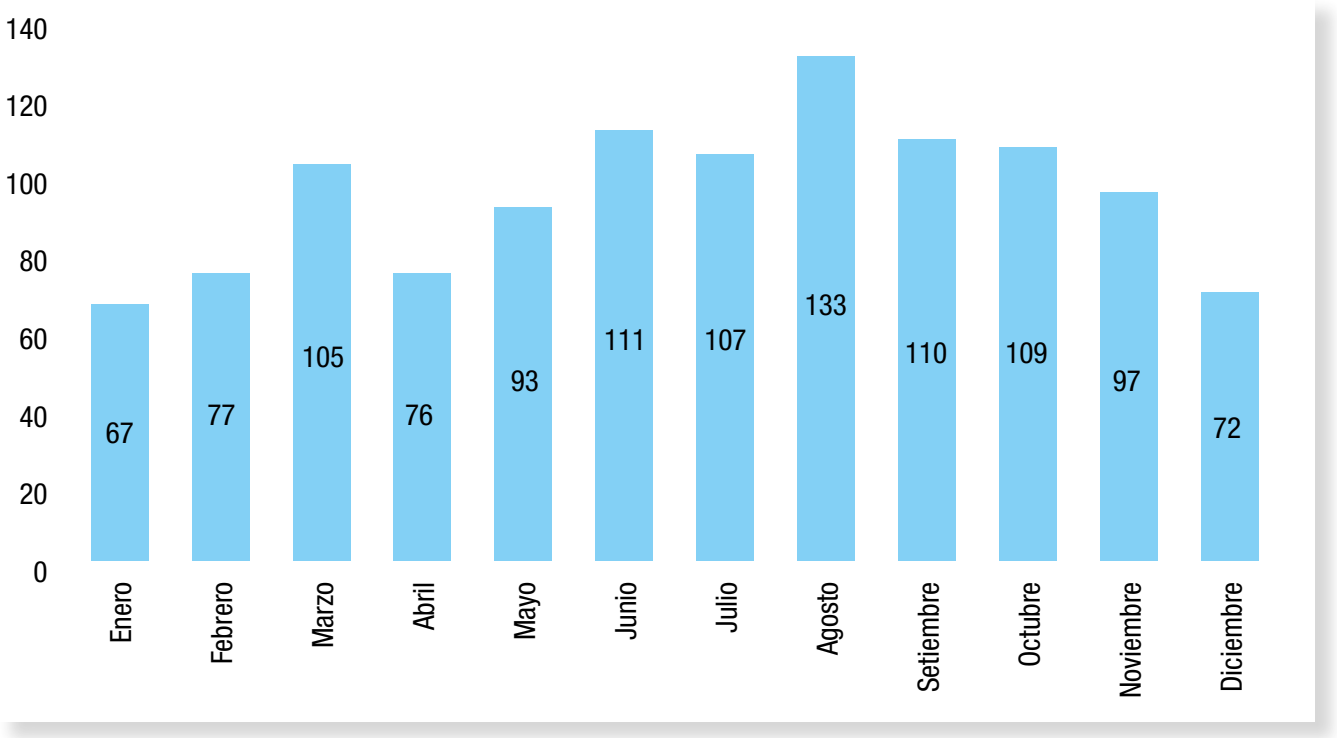


Figura 7.10. Denuncias promedio recibidas por la Prodhab (2014-2021) -promedio mensual-

Fuente: Prodhab, 2022.

La PRODHAB tiene como uno de sus objetivos el velar por el cumplimiento de la normativa vigente de protección de datos personales, sin embargo, en los últimos 2 años ha tenido mucha atención sobre sus acciones, debido a los escándalos relacionados con protección de datos personales en donde no ha cumplido sus deberes. Entre estos pueden mencionarse:

1. **CASO UPAD (2020)**. Siendo el caso de violación de la normativa de datos personales más importante de la historia de Costa Rica, que inclusive generó una investigación penal al ex presidente de la República, Carlos Alvaro. Parece sorprendente que hasta el momento no existe sanción alguna por un incumplimiento flagrante de la ley №8968. Como se ha visto en otros informes de PROSIC, cuando este caso fue denunciado por prensa, la agencia primero salió a indicar públicamente que no había nada irregular en las acciones del gobierno, para luego indicar que lo iba a investigar. Finalmente, la señora Elizabeth Mora, como directora de la Agencia, compareció en la Asamblea Legslativa e indicó que había detenido dicha investigación:

La Prodhab aplicó el principio de "prejudicialidad" sobre el expediente 028-02-2020, en vista de que ambas gestiones podrían derivar en resultados sancionatorios. "El procedimiento que está establecido en la ley 8968 no es un procedimiento disciplinario-administrativo, sino que es un procedimiento sancionatorio, por lo tanto, tuvimos la consideración de que corresponde declarar la prejudicialidad", explicó. (Alfaro, 2020, párr.3).

Cabe señalar que hasta la fecha ninguna institución de gobierno sido sancionada por este caso.

2. **CASO FARO (2021):** Un caso de infracción flagrante por parte del Ministerio de Educación Pública (MEP), por el cual renunció la Ministra de Educación y por el cual la Sala Constitucional indicó que hubo "una lesión grave y grotesca al derecho a la intimidad"[17]. Se conoció que la agencia de forma atípica asesoró al MEP cuando esto no se encuentra dentro de sus atribuciones establecidas por ley[18] y en donde quien tuvo que actuar con celeridad para proteger a la población infantil fue el Tribunal Contencioso administrativo[19], ya que nuevamente la agencia no mostró interés en hacer cumplir la ley con celeridad y de forma proactiva. Hasta la fecha el MEP no sido sancionada por este caso.

3. **CASO BAC-SICERE:** En el año 2015, el país amaneció con la noticia de que un banco privado había hackeado una base de datos y extraído información de más de 500 mil costarricenses[20]. **La Prodhab, bajo la dirección del señor Mauricio Garro también suspendió la investigación por supuesta prejudicialidad[21].** En enero de

17 Como lo cubrió el Semanario Universidad: La resolución de la Sala Constitucional se da luego de declarar con lugar un total de 15 recursos de amparo presentados por padres de familia contra el MEP. De acuerdo con el departamento de prensa de la Sala Constitucional, de forma unánime, en la sesión de este viernes 17 de diciembre, el Tribunal concluyó que hubo "una lesión grave y grotesca al derecho a la intimidad", cobijado en el artículo 24 de la Constitución Política. Además, los magistrados concluyeron que la aplicación de las pruebas para obtener datos personales se dio desde una posición de poder y en contra de una población vulnerable. También señalaron que los datos fueron obtenidos a través de una prueba obligatoria, impuesta a personas en proceso de formación que requieren de especial protección del Estado en virtud de lo dispuesto en el numeral 3.1 de la Convención sobre los Derechos del Niño y el ordinal 51 de la Constitución Política. (Cordero, 2021, párr.2-4).

18 Como lo cubrió Amelia Rueda: La Agencia de Protección de Datos de los Habitantes (Prodhab) se abstuvo de dar detalles sobre las asesorías y recomendaciones que brindó al Ministerio de Educación Pública (MEP) con relación al tratamiento de datos personales sensibles de menores de edad recolectados por medio del cuestionario de "factores asociados" de las Pruebas FARO. Su directora, Elizabeth Mora, estuvo este martes en programa deNuestra Voz e indicó que no podía brindar información específica sobre estas asesorías debido a que el tema se encuentra en proceso de investigación. (Alvarado, 2021, párr.1).

19 Como lo cubrió Delfino.cr: Este miércoles 24 de noviembre, a las 8 de la mañana, el Ministerio de Educación Pública (MEP) inició con la entrega en la sede del Segundo Circuito Judicial de San José, de los formularios de factores asociados de las Pruebas FARO, aplicados el pasado viernes 12 a los estudiantes de quinto año de primaria. Estos son justo los cuestionarios que el Tribunal Contencioso Administrativo ordenó al ministerio entregar, en una resolución emitida ese mismo viernes 12 por parte del juez Alex Rojas Ortega, que ordenó al MEP no destruir ni entregar a los tutores de los menores de edad, si no pasar de una vez a la instancia judicial correspondiente. La orden fue emitida a raíz de una solicitud de medida cautelar provisionalísima planteada por el Sindicato de la Judicatura (Sindijud), que pidió la "incautación inmediata y devolución" de la prueba por contener en los formularios una serie de preguntas que abordan datos sensibles y privados que lesionan la intimidad de sus agremiados "y que atentan contra los derechos elementales de sus hijos e hijas menores de edad". (Mora, 2021, párr. 1-3).

20 Como lo reportó crhoy.com: Entre marzo y mayo, el Sistema Centralizado de Recaudación (Sicere) de la Caja Costarricense de Seguro Social (CCSS) fue vulnerado, por medio de un robot de software que habría sido activado por dos funcionarios de BAC Credomatic, no de la operadora de pensiones, para sustraer el historial laboral de más de 500.000 cotizantes. (Rojas, 2015, párr. 4).

21 Como lo reportó La Nación: La Agencia de Protección de Datos de los Habitantes (Prodhab) resolvió suspender la investigación por presunto hackeo en el Sistema Centralizado de Recaudación (Sicere), en espera de los resultados del proceso que también se

2021, el Ministerio Público solicitó un sobreseimiento para los dos exempleados del BAC que realizaron dicha actividad[22]. Sin embargo, hasta la fecha, el BAC no ha sido sancionado por este caso, ni la ciudadanía cuál fue el resultado de la investigación realizada por la Prodhab.

Como puede verse, en 2 de los 3 casos más importantes que ha tenido que investigar la agencia ha utilizado el instituto de la prejudicialidad como una vía para suspender el proceso. Este instituto se utiliza en un proceso judicial con el fin de suspenderlo hasta que el juez penal resuelva el mismo, para así evitar contradicciones judiciales.

La prejudicialidad como obstáculo de la aplicación de la normativa de protección de datos personales

Con el fin de comprender si dicho instituto se está utilizando de la manera correcta, es importante preguntarse si este aplica para el caso de procesos administrativos sancionatorios como el que realiza Prodhab ante una denuncia por infracción de la ley 8968. Para este fin, se entrevistó al señor Fabián Volio, reconocido abogado constitucionalista, al que se le realizó la siguiente pregunta:

> **¿Se puede aplicar la prejudicialidad en los procesos sancionatorios, haciendo una diferencia con lo aplicable para los sancionatorios disciplinarios, tal como lo indica la Prodhab?**
>
> El abogado respondió de manera contundente:
>
> **No, en primer lugar, creo que esa es una tesis equivocada.** El género, por decirlo así, es el derecho sancionatorio, que según con nuestro Tribunal Constitucional se divide en dos: A) el derecho sancionatorio judicial penal; y B) El derecho sancionatorio administrativo. Son dos cosas totalmente diferentes, pero tienen reglas en común de respeto al derecho a un debido proceso legal.
>
> El proceso sancionatorio administrativo se divide a su vez, en dos: A) el proceso sancionatorio disciplinario, que se aplica a los funcionarios públicos para sancionarlos; y B) El proceso sancionatorio por sí, que se aplica a personas o empresas contratistas del Estado o- reguladas por el Estado y sus instituciones. Entonces, la diferenciación está en la atribución de un órgano para disciplinar a un funcionario público porque ejercer su jerarquía, caso en el cual impondrá sanciones, pero de tipo laboral administrativa.
>
> Ahora bien, cuando se trata del proceso sancionatorio en sí, se imponen multas u otro tipo de sanciones contra entes, empresas contratistas, órganos regulados, como en el caso de la materia del manejo de los datos personales, como la autoridad que ejerce la Agencia de Protección de Datos del Ministerio de Justicia.
>
> En el caso penal, se trata del Poder Judicial y ahí se imponen sanciones o penas de prisión o de otro tipo de sanciones penales judiciales.

sigue en el Ministerio Público. La resolución se tomó este miércoles, informó la oficina de prensa del Ministerio de Justicia y Paz a solicitud de este diario. La Prodhab está adscrita al despacho de la ministra. Esta medida se tomó basada en el principio de prejudicialidad, informó la oficina de prensa. (Ávalos, 2015, párr. 1-3)

22 Como lo cubrió nación.com: La Fiscalía solicitó al Juzgado Penal de San José el sobreseimiento de dos exempleados bancarios investigados por el supuesto hackeo al Sistema Centralizado de Recaudación (Sicere), de la CCSS, donde se guardan los datos de 1,7 millones de cotizantes. La petición de "sobreseimiento por duda" fue enviada desde el 22 de setiembre en relación con la causa tramitada bajo el expediente 15-000648-0612-PE, informó la oficina de prensa del Ministerio Público ante consulta de *La Nación (Ávalos, 2021, párr.1y2)*.

El concepto de prejudicialidad se utiliza siempre en el caso de los jueces respecto a otros jueces, es decir que un proceso judicial no puede continuar porque hay uno previo. Pero en el caso de las sanciones administrativas no existe esa relación, la sanción administrativa puede imponerse independientemente de la sanción penal; con una única advertencia y es que si ya se ha dictado una sanción penal no pueden contradecirse los hechos o resolverse en la vía administrativa ninguna calificación de los hechos diferente a la que ha ocurrido en la vía judicial.

Evidentemente, porque ahí sí se impone el criterio de los jueces sobre los funcionarios públicos, pero con esa única salvedad. Es decir, que un funcionario público no puede contradecir las decisiones y las conclusiones de un tribunal judicial penal. Sin embargo, la vía administrativa debe continuar, sea sancionatoria o disciplinaria. Así es que considero que ese es un error muy grave cometido por la Agencia de Protección de datos, porque sí pudo haber impuesto sanciones administrativas, por actos cometidas por todos los entes y personas reguladas, independientemente de que todavía no se haya resuelto el caso en la vía judicial penal. Así es que creo que es una decisión desafortunada. (Fabián Volio, Comunicación personal, 28 de junio de 2022).

Los tipos de caso que ve la agencia

El 40% de los ciudadanos realizan denuncias vinculadas con una solicitud de eliminación o supresión de los datos personales y tan solo el 3% por el incumplimiento del derecho de acceso a la información personal, lo que puede revelar que los ciudadanos desconocen la importancia de este derecho que es mediante el cual este puede conocer sobre los tratamientos, el tipo de datos y hasta la fuente de obtención de la información personal por parte del responsable de la base de datos.

Por otro lado, resulta revelador que a pesar de que el derecho al olvido es tan conocido por la academia, en la práctica los ciudadanos lo desconocen, ya que solo el 4% de los casos están relacionados con este tipo de casos.

La independencia de la Agencia

La independencia de la agencia y de su director(a) es esencial para que la Prodhab pueda realizar las funciones que le fueron encomendadas por ley, por lo que es importante analizar el tiempo que han durado en el cargo cada uno de los directores como un reflejo de cuánta estabilidad laboral tienen. Debido al Caso UPAD en donde la Prodhab no defendió los intereses de los habitantes, se ha debatido mucho sobre los cambios que deben realizarse en la agencia para que tenga independencia. Siendo que la exdirectora Elizabeth Mora, quien tenía la responsabilidad de realizar dicha investigación, la que más días en el cargo ha estado, parece que no es un tema menor.

Esta directora fue removida de su puesto en el presente año, como decisión del nuevo Ministro del Ministerio de Justicia y Paz, lo que también refleja que los directores dependen de decisiones políticas. Sin embargo, como en otras ocasiones la opinión pública no conoció lo que motiva el cambio de dirección, ya que no se basa en ningún incumplimiento de sus deberes. Y esto es relevante, ya que el gobierno anterior la pudo haber cesado, ya que ha enfrentado distintas controversias relevantes para su puesto:

1. Diputadas del Partido Liberación Nacional y un diputado de Nueva República le pidieron de manera expresa su renuncia por su inacción en el Caso UPAD (2020).[23]

23 Diario Extra le dio cobertura al hecho con el titular "Piden cabeza de directora de Prodhab" , la cual se puede encontrar en https://www.diarioextra.com/Noticia/detalle/423037/piden-cabeza-de-directora-de-prodhab y crhoy.com le dio cobertura con el titular "Diputadas de Liberación Nacion-

2. La Sala Constitucional ordenó testimoniar piezas al Ministerio Público para que investigue el supuesto incumplimiento, por parte de dicha directora, de lo resuelto en la Sentencia N° 2020-007781[24], y que resulta ser la segunda declaratoria de desobediencia.
3. Investigación por exceso de ausencias e irregularidades en el traslado de edificio. Otros funcionarios denunciaron que la directora faltaba mucho al trabajo y que inclusive durante el traslado de edificio la agencia estuvo sin acceso a internet, servicios de limpieza entre otros.[25]

Esto ha motivado la presentación de diversos proyectos de ley por parte de distintos diputados. Entre las iniciativas presentadas se puede hacer mención a las siguientes:

a. **Proyecto de Ley № 21828:** Presentado por el diputado José María Villalta y que propone trasladar la agencia a la Defensoría de los Habitantes, por lo que la persona defensora es quien elige al director(a) nacional.
b. **Proyecto de Ley № 22388:** Propuesto por el diputado Enrique Sánchez con el fin de convertir a la agencia en un órgano adscrito a la Asamblea Legislativa, por lo que su director(a) lo elige el Poder Legislativo.
c. **Proyecto de Ley № 23097:** Presentado por el diputado Eliécer Feinzag para trasladar la agencia al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt), como un órgano adscrito a este. El director será propuesto por Micitt y el Consejo de Gobierno designará a la Dirección y el Adjunto de la Agencia de Protección de Datos. Una vez que el Consejo de Gobierno haya nombrado al director o directora tanto propietario como adjunto, enviará el nombramiento junto con el expediente del concurso a la Asamblea Legislativa, que dispondrá de un plazo de treinta días naturales para objetar el nombramiento por mayoría calificada.

La Política de Privacidad

El Comité de Políticas de Economía Digital de la OCDE le recomendó al país la creación de una Estrategia de Privacidad, la cual refleje un enfoque coordinado entre los organismos gubernamentales[26]. Dicha estrategia fue elaborada en enero del 2020 por el consultor Mauricio París, con el financiamiento de la Embajada Británica y dentro de los elementos que propone es que el país debe establecer en su hoja de ruta están:

al piden renuncia de directora de Prodhab, la cual puede leerse en https://www.crhoy.com/nacionales/diputadas-del-pln-exigen-renuncia-a-directora-de-prodhab/.

24 La Sala Constitucional indica en la resolución No 2021008545: "En vista de que la recurrida omitió rendir el informe dentro del plazo fijado por este Tribunal en la audiencia de desobediencia de este asunto, de conformidad con el artículo 45, de la Ley de la Jurisdicción Constitucional, se tienen por ciertos los hechos en lo que a esa funcionaria atañe y se procede a analizar la constitucionalidad del asunto con base en los demás elementos aportados a los autos. En consecuencia, denota esta Sala que existe un incumplimiento por parte de la autoridad recurrida, en relación con lo ordenado por este Tribunal en la sentencia principal. Así las cosas, y al tratarse de una segunda declaratoria de desobediencia, según se pudo constatar del primer considerando de esta resolución, lo procedente es ordenar el testimonio de piezas por el incumplimiento de la Sentencia N° 2020-007781 de las nueve horas cuarenta y cinco minutos del veinticuatro de abril de dos mil veinte. (R. 2021008545, Sala Constitucional, 2021).

25 Diario Extra le dio cobertura a este hecho con el titular "Investigan exceso de ausencias de directora", la cual puede verse en https://www.diarioextra.com/Noticia/detalle/411975/investigan-exceso-de---ausencias-de-directora.

26 De acuerdo a lo que indica la misma Estrategia de privacidad (p.5) que se obtuvo de la Prodhab, entregada a través del oficio Oficio APD-DRAB-039-08-2022 y en la exposición de motivos del proyecto de ley 23.097 (p.4.)

Director (A)	Duración en el cargo	Inicio	Finalización	Motivo 2020	Motivo 2022
Arlene González Castillo	1 año y 6 meses (559 días)	5 marzo 2012	6 de julio, 2013	Prohab no tiene registro	Decisión del jerarca.
Natalia Artavia Chavarría	9 meses (294 días)	Setiembre de 2013	6 de julio, 2014	Prohab no tiene registro	Decisión del jerarca.
Alejandro Ulate Campos	14 días	7 de julio, 2014	21 de julio, 2014	No se registro en la lista de directores	Decisión del jerarca.
Mauricio Garro Guillen	2 años y 6 meses 30 días (945 días)	21 de julio, 2014	28 de febrero, 2017	Decisión del jerarca	Decisión del jerarca.
Wendy Rivera Román	1 año y 2 meses (432 días)	1 de marzo, 2017	7 de mayo, 2018	Decisión del jerarca	Fin del plazo de nombramiento.
Ana Karen Cortés Víquez	1 año y 14 días (379 días)	15 de junio, 2018	29 de mayo, 2019	Renuncia por motivos personales	Renuncia.
Elizabeth Mora Elizondo	2 años y 10 meses y 23 días (1058 días)	Junio, 2019	13 de junio, 2019	Continuaba en el cargo	Decisión del jerarca.
Wendy Rivera Román	En curso	16 junio, 2022	Vigente	No aplica	Continúa en el cargo.

Figura 7.4. Directores de la Prodhab (2012-2022)

Fuente: Elaboración propia con base a la Prodhab.

1. **Consagrar el Derecho a la Protección de Datos Personales como un derecho autónomo mediante una reforma a la Constitución Política.** Lo anterior, lo justifica no solo por la importancia de este derecho, sino también por la tendencia internacional en la materia.
2. **Adhesión al Convenio 108.** En la estrategia París (2020) indica que la importancia del Convenio 108 radica en que es el único instrumento internacional de alcance global en materia de protección de datos personales e implica adoptar un estándar de protección de datos personales más elevado del que se mantiene hoy. Con lo anterior se indica que el país asumiría un compromiso internacional en protección de datos, por medio de un tratado internacional con rango superior a la ley. Adicionalmente, indica que al adherirse al Convenio 108 y sus Protocolos podría permitir que el país opte por una Decisión de Adecuación por parte del Consejo de Europa.

3. **Armonización entre el derecho a la privacidad, el derecho al tratamiento de los datos personales y el derecho a la transparencia e información pública**. En este apartado se establecen ejemplos de limitaciones sobre el acceso a información pública y excesos que ha permitido la Sala Constitucional sacrificando el derecho de autodeterminación informativa. Al mismo tiempo, se critica el decreto 40200-MP-MEIC-MC, "Transparencia y Acceso a la Información Pública".

El primer decreto contiene deficiencias importantes. En primera instancia, define de manera extensa el derecho al acceso de la información pública. Obliga a las instituciones públicas y a quien maneje fondos públicos a mantener una página web que publicite, entre otros: mecanismos y resultados en evaluaciones de desempeño de funcionarios, las planillas con el salario bruto y un listado de los subsidios, becas, donaciones, exoneraciones o cualquier otra transferencia o beneficio otorgado a personas particulares, sólo efectúa una leve referencia a la Ley 8968 (París, 2020, p.21).

Como puede verse, esta crítica iba en línea contraria a la dirección que llevaba el Poder Ejecutivo con UPAD.

1. **Reforma integral a la Ley 8968. Como indica París (2020**). La estrategia establece que el proceso de actualización normativa debe cumplir con lineamientos de la propia OCDE y encontrarse bajo el paraguas del Convenio 108**.**
2. **Replantamiento de la Prodhab.** Dentro de los elementos que destaca París (2020) en la Estrategia es que la Agencia debe gozar de la estructura, la autonomía y la competencia que le habilite a ser un órgano en grado de desconcentración máxima, con una idoneidad especial y técnica que se relacione con la Administración mediante el Micitt.
3. **Tratamientos de datos personales por parte del Estado.** Se indica que siendo el Estado costarricense el que maneja la mayor cantidad de datos de los costarricenses, se requiere una adecuada estructuración y protección de la privacidad por parte del Estado. Recomienda París (2020) realizar un inventario de las bases de datos, ya que de acuerdo con dicho estudio resultó claro que solo un promedio del 38% de las autoridades indica contar con un inventario de bases de datos personales, pero poco menos del 30% cuenta con políticas sobre el manejo de tales datos. Una vez se realice esta labor, las instituciones deben regularizar este tratamiento en cumplimiento de la ley № 8968. Finalmente, se encuentra que hay instituciones que cuentan con funciones que duplican la de Prodhab, por lo que este es un elemento que se recomienda debe subsanarse.

Esta estrategia no fue aprobada por la comisión conformada para esos efectos, ya que estos determinaron que el documento presentado no resultó satisfactorio para considerarse como una estrategia, lo que fue avalado por la señora Elizabeth, en su condición de directora. Al mismo tiempo, la nueva directora de la agencia indica que durante el segundo semestre del 2022, se retomará el documento elaborado en esta oportunidad con el fin de realizar una propuesta y someterla a algún mecanismo de consulta pública.

7.12. PROYECTO DE REFORMA AL ARTÍCULO 24 DE LA CONSTITUCIÓN POLÍTICA (№ 22.063)

El 14 de julio de 2020, la diputada Silvia Vanessa Hernández Sánchez presentó un proyecto de ley que pretende hacer un cambio constitucional al artículo 24 de la Constitución el cual reza así:

Norma vigente	Propuesta del Proyecto № 22.063
Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.	Se garantiza el derecho a la vida privada, a la protección de los datos personales, a la libertad y al secreto de las comunicaciones. Mediante ley especial podrán adoptarse limitaciones a estos derechos para salvaguardar la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y las libertades de terceros, así como por cuestiones de interés público.
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.	Son inviolables los documentos privados, los datos personales sensibles 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, fijåará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, o datos personales sensibles, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.
Norma vigente	**Propuesta del Proyecto № 22.063**
Igualmente, 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.	Igualmente, 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.

La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos. Una ley especial, aprobada por dos tercios del total de los Diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión.	Una ley especial, aprobada por dos tercios del total de los Diputados, fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los sistemas de contabilidad y sus soportes, o acceder a datos personales para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos, y cuáles otros órganos de la Administración Pública podrán revisar los documentos o acceder a datos personales que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión.
No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación.	No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación.

Como puede verse, la propuesta de reforma constitucional principalmente pretende hacer cambios puntuales:

1. **Incluir el concepto de vida privada, en sustitución del de intimidad**. Al igual que España[27], Costa Rica protege de manera expresa la intimidad en su constitución, por lo que el desarrollo jurisprudencial trata el concepto de intimidad y vida privada de manera indistinta.

El concepto de vida privada en la mayoría de países del continente europeo es mucho más amplio que el de intimidad, ya que inclusive pertenece al primero. A su vez lo recogen distintos tratados internacionales ratificados por Costa Rica, por lo que es un concepto que ya se encuentra incorporado en nuestro ordenamiento jurídico.

Sin embargo, el juez constitucional costarricense, así como el español, no hacen distinción entre intimidad y vida privada, por lo que en la práctica podría parecer una propuesta superficial, pero que a futuro podría permitir un mejor desarrollo de la protección de las distintas manifestaciones de la vida privada que deben regularse.

2. **Se incorpora la inviolabilidad de los datos personales sensibles.** Nuestra Constitución Política no protege de manera expresa al dato personal con respecto a su inviolabilidad, por lo que este proyecto pretende hacer una protección expresa, pero solo con respecto a los datos personales sensibles. Lastimosamente, el concepto de dato sensible que se encuen-

27 El artículo 18 de la Constitución Española reza de la siguiente manera: 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen; 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito; 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial y 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. (artículo 18, 1978, Constitución Política, España).

> tra contenido en la legislación costarricense es indeterminado y genera inseguridad jurídica, por lo que aunque pueda parecer útil limitar la protección constitucional únicamente respecto a los datos relativos al fuero íntimo de la persona, en la práctica podría ser peligroso en el caso de las acciones de las autoridades.

En la actualidad, el Ministerio Público accede a datos relativos a la ubicación de personas investigadas sin orden judicial. Esto lo hace a través de un sistema denominado SOLITEL[28], el cual permite el acceso a estos datos, que son solo datos personales de acceso restringido, de acuerdo a la Ley № 8968,. Estos datos, en algunos casos, pueden revelar datos sensibles de las personas, como cuando permiten concluir que una persona está en un sitio religioso o relacionado con sus preferencias sexuales.

3. **Permite la limitación del derecho a la vida privada, protección de datos personales, la libertad y el secreto a las comunicaciones por ley especial**. Siempre y cuando sea para salvaguardar la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y las libertades de terceros, así como por cuestiones de interés público.

Este es el elemento más controversial, el cual provocó que el abogado constitucionalista Fernando Zamora expresara en el diario La Nación que se trataba de una propuesta imprudente, siendo el extracto más importante de su opinión la siguiente:

Redacción genérica y abierta

> De acuerdo con la redacción, bastaría con esgrimir los derechos de un tercero, cualquier asunto de interés público o para la seguridad nacional, cuestiones de salud o seguridad ordinaria, entre otros, para que se prive al ciudadano de la libertad de comunicarse y del derecho a su vida privada y a la intimidad de sus datos personales, y, consecuentemente, sus comunicaciones sean vigiladas por el Estado.
>
> Como se lee en el texto, la propuesta cita muchas razones por las cuales sería posible imponer limitaciones a estos derechos tan sensibles. (Zamora, 2022, párr. 6-7).

El autor del proyecto, el señor Mauricio París, le contestó al señor Zamora por dicho medio, siendo el extracto más importante de su respuesta la siguiente:

> La posibilidad de que los derechos constitucionales sean limitados mediante ley no tiene ninguna novedad en el ordenamiento jurídico, pues lo establece expresamente el artículo 19 de la Ley General de la Administración Pública desde el año 1978.
>
> Al contrario, uno de los valores agregados que representa esta propuesta de reforma constitucional es un blindaje de reserva de ley a la protección de datos personales, del que hoy carece por no ser un derecho constitucional.
>
> Como antecedente, en el caso de la UPAD, la principal discusión jurídica fue, precisamente, la potestad del Poder Ejecutivo para adoptar una limitación de derechos fundamentales mediante un decreto ejecutivo.
>
> La reforma brindaría una capa adicional de protección a los datos personales sensibles, que son los que representan el fuero más íntimo de una persona y cuyo tratamiento representa mayores riesgos a los derechos y libertades del ciudadano.
>
> El párrafo segundo de la reforma garantiza la inviolabilidad de las comunicaciones y de los datos personales sensibles, por lo que de la lectura de la propuesta queda claro que, lejos de involucionar, la norma propuesta le garantiza máxima protección jurídica tanto a los datos personales sensibles como al secreto de las co-

28 Sistema Informático de Solicitudes de Telecomunicaciones.

municaciones. (París, 2022, párr. 6-9)

4. **Requiere que las leyes que habiliten las transferencias de datos personales interinstitucionales y/o el acceso a los datos de los habitantes sean aprobadas por dos tercios del total de los Diputados.** Esta es la propuesta más acertada desde la perspectiva de elevar el marco de garantía con respecto a los datos personales de los costarricenses. Sin embargo, se debe tomar en cuenta que no se debería avanzar en esta propuesta si el Estado no ejecuta una Estrategia de Privacidad, para garantizar que ninguna función relevante del Estado va dejar de realizarse al cortársele el acceso a algunos datos, ya que es claro que muchas instituciones transfieren datos sin un claro fundamento de derecho.

En general, se puede indicar que esta propuesta es buena para provocar un debate regulatorio alrededor del reconocimiento de algunos derechos digitales y el fortalecimiento de la protección a la vida privada, como un todo. Debido a lo anterior, el concepto de libertad - que se encuentra en la norma vigente y que en la propuesta no se desarrolla - podría ser ampliado con el fin de avanzar hacia el reconocimiento de derechos digitales en entornos digitales.

CONSIDERACIONES FINALES

La tecnología es una plataforma llena de oportunidades de la cual la sociedad no puede prescindir, de la misma manera que no se puede dar el lujo de no observarla y analizarla, con el fin de buscar formas de sacarle mejor provecho y reducir riesgos. Este ejercicio no debe realizarse desde la perspectiva de una sola disciplina, ya que los retos que nos traen las TIC son transversales, por lo que hacer un abordaje desde un solo campo siempre será limitado y podrá afectar negativamente los resultados.

A nivel de ejemplo, hemos visto que en materia de ciberseguridad Costa Rica destaca a nivel latinoamericano principalmente por sus avances en materia legal, pero que es débil en otras áreas técnicas cuyas debilidades han explotado con éxito los ciberdelincuentes que han atacado múltiples instituciones en el último año.

Otra área importante en la que debe avanzarse es en la capacitación de líderes sobre:

1. La importancia del respeto de los derechos digitales como muro de contención de la democracia.
2. La ciberseguridad como un mecanismo defensivo de derechos y libertades.
3. La importancia de la creación de estrategias para robustecer los dos anteriores en el cumplimiento de los objetivos organizacionales.

Lo anterior, es relevante porque durante los ataques que sufrió el país, se tomaron decisiones y se dieron declaraciones por parte de líderes gubernamentales que dejaban claro que se le daba poca relevancia a la privacidad y que lo que más importaba era lo económico. Precisamente esta posición de poco interés por la ciberseguridad y el respeto de derechos digitales es la situación que puso en mayor riesgo al país, ya que cuando no se comprende la importancia de una materia es susceptible de ser descuidada.

Hacia una Estrategia costarricense de protección de los derechos digitales

El Estado costarricense debe tener un norte con respecto a cómo deberá enfrentar el avance tecnológico sin sacrificar la dignidad y libertad del individuo, al mismo tiempo que promueve la innovación y la libertad económica. Para este fin, el Estado costarricense, liderado por cada Poder de la República debe realizar acciones y generar estrategias relacionadas con sus funciones:

1. El Poder Ejecutivo deberá:

a. **Aprovechar el debate generado alrededor de reformas sobre protección de datos personales** y el artículo 24 de la Constitución Política para alimentar sus propias estrategias y liderar el desarrollo normativo de acuerdo a un plan integral.

b. **Publicar una Estrategia de Privacidad**. En esta deberá establecerse cuáles serán los pasos a seguir para proteger la información personal de los ciudadanos, tomando en cuenta desde lo jurídico hasta lo técnico. Es importante señalar que mientras existen leyes que protegen la privacidad del ciudadano, el Estado va en sentido contrario revelando la vida privada del ciudadano sin que exista un debate legislativo sobre sobre el impacto de estas decisiones sobre el habitante.

   En esta investigación se tuvo acceso al documento que se desarrolló, con el apoyo de la Embajada Británica y que se considera que aunque no puede considerarse como una estrategia por sí misma, sí tiene las bases necesarias para iniciar una discusión fuerte sobre esta materia. Pero que a su vez, la principal debilidad de dicho proceso fue el no contar con un mejor instrumento consultivo a los grupos de interés relacionados con esta materia, para elevar la discusión.

a. **Actualizar e implementar la Estrategia de Ciberseguridad**. Los esfuerzos que se realizaron por el gobierno de Luis Guillermo Solís para su desarrollo, en colaboración con la OEA, quedaron en papel muerto debido al poco interés demostrado en la materia por el gobierno de Carlos Alvarado. El actual gobierno se encuentra realizando una revisión, pero la prueba de fuego será garantizar su efectiva implementación.

b. **Creación y publicación de una Carta de Derechos Digitales**: el Micitt deberá lanzar un proceso de consulta pública para co-crear con la sociedad civil, academia, empresas tecnológicas y diversos grupos de interés para acordar una Carta de Derechos Digitales que deberá guiar la creación de toda Política Pública.

c. **Actualizar la Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0, para incluir como principio estratégico el respeto de derechos digitales.** Esto debido a que la Estrategia actual se sustenta en la transparencia y hace omisión absoluta del respeto de la privacidad o de otros derechos digitales.

d. **Creación y publicación de una Estrategia para el aprovechamiento de la Inteligencia Artificial.** Como hemos analizado en este y otros capítulos esta tecnología emergente será esencial para el desarrollo económico de los países, pero que al mismo tiempo representa importantes riesgos para la vida privada. Debido a esto el país debe discutir sobre cuál va a ser la estrategia que va a tomar para proteger los derechos humanos de las personas, haciendo un sano balance con respecto al aprovechamiento que se debe realizar de la misma para que prospere la nación.

II. El Poder Judicial deberá:

a. **Publicar una Estrategia de Lucha contra la Ciberdelincuencia en la cual defina la política criminal relacionada con el cibercrimen.** Esto con el fin de mantener actualizada la normativa sustantiva y procesal, de acuerdo a los objetivos establecidos por la Estrategia y poder ser efectivo en esta lucha.

b. **Publicar una Estrategia de Ciberseguridad.** Con el fin de analizar los riesgos que tiene el Poder Judicial y sus usuarios en la utilización de TIC y crear un marco estratégico sobre cómo enfrentar las amenazas cibernéticas. Esta estrategia debe estar alineada con las emitidas por el Ejecutivo, tanto a nivel de privacidad como en ciberseguridad. Dentro de esta estrategia, debe contemplarse el avance hacia la creación de una Ley que proteja al Usuario Financiero Nacional. A través de esta normativa se le debe permitir a los usuarios decidir sobre el grado de riesgo que desea tener y sobre los estándares mínimos de seguridad digital que se debe poseer en una plataforma bancaria. Quiere decir, que se deben ampliar las opciones que tiene el usuario para proteger sus fondos, de tal manera que sirva como una barrera adicional de seguridad bancaria, en donde si el banco falla en el cumplimiento de estas barreras deba realizar un proceso expedito de devolución del dinero.

El Poder Legislativo deberá contar con una Estrategia de revisión, coordinación y actualización de la normativa vigente relacionada con las TIC, de acuerdo con las necesidades de los otros Poderes de la República. Deben crearse canales abiertos para la priorización de los temas que son necesarios para cumplir con los objetivos establecidos en las distintas estrategias, sin lo cual es difícil ser efectivo debido a la rapidez con la que evoluciona esta materia.

La libertad de la persona en entornos tecnológicos y el uso de la tecnología

Las sociedades modernas dependen de la libertad en el ciberespacio y en el uso de la tecnología, para el desarrollo de los derechos digitales, el fortalecimiento de las democracias y la generación de oportunidades para todos los ciudadanos.

Sin embargo, para garantizar un respeto de los derechos humanos y la adecuada convivencia en entornos digitales las libertades pueden requerir limitaciones, las cuales deberán ser las mínimas posibles para cumplir sus objetivos. Esta intervención mínima del Estado tiene como fundamento el respeto y garantía de la autonomía individual, la libertad económica y la dignidad del individuo que son piedra angular en un sistema democrático que propicie prosperidad, innovación y libertad.

Al erigir un principio de intervención minima en la libertad de la persona en entornos tecnológicos y el uso de la tecnología, que requiera mayoría calificada en el Congreso para limitarla, propicia entornos de autorregulación que deberán alejarse de abusos para evitar regulaciones que les coarten su libertad. Lo anterior, en comprensión de que el ciberespacio ya es gobernado en su mayoría por empresas tecnológicas que se rigen por un ordenamiento jurídico estadounidense que les permite tener el internet libre que disfrutamos a nivel mundial.

Para el autor, debe proponerse una reforma del artículo 24 constitucional, que le brinde contenido al concepto de libertad en ese numeral. Se deberá vincular con la tecnología y libertades individuales, con el fin de propiciar un desarrollo nacional de creación y respeto de los derechos digitales.

Esta reforma fortalecerá el sistema democrático costarricense, ya que obligaría al Estado a alejarse de la vigilancia indiscriminada y a generar consensos en toda limitación que propongan en el uso de la tecnología.

José Adalid Medrano Melara

Abogado especialista en derecho informático, conferencista internacional, consultor y capacitador sobre ciberdelincuencia y protección de datos personales. Coordinador de la Especialización en Derecho Informático de la Escuela Libre de Derecho y coordinador de la Comisión de Innovación Regulatoria del Colegio de Abogados y Abogadas. Co-redactor de reformas al Código Penal costarricense sobre delitos informáticos y del más reciente proyecto de ley de lucha contra la Ciberdelincuencia (Proyecto № 21187).

adalid@ciberjuristas.com

REFERENCIAS

Castro-Obando, V. (2020). Marco Institucional y Políticas Públicas TIC. En: Programa Sociedad de la Información y el Conocimiento (Ed.), *Informe Hacia la Sociedad de la Información y el Conocimiento 2020* (13-98). Prosic-UCR.

Castro-Obando, V. (2021). Institucionalidad y políticas públicas TIC. En: Programa Sociedad de la Información y el Conocimiento (Ed.), *Informe Hacia la Sociedad de la Información y el Conocimiento 2021* (15-89). Prosic-UCR.

Acceso a la Justicia (2022). De Lege Ferenda. Recuperado de https://accesoalajusticia.org/glossary/de-lege-ferenda/

Agencia Española de Protección de Datos (2019). Estudio: Fingerprinting o Huella del dispositivo. Recuperado de https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf

Alfaro, J. (29 de junio de 2020). Prodhab detuvo investigación sobre caso UPAD ante pesquisas judiciales. Recuperado de https://www.ameliarueda.com/nota/prodhab-detuvo-investigacion-sobre-upad-pesquisas-judiciales-presidencia

Alvarado, A. (16 de diciembre, 2021). Prodhab evita dar detalles sobre asesoría dada al MEP para cuestionarios de pruebas FARO. Recuperado de https://www.ameliarueda.com/nota/prodhab-abstiene-detalles-asesoria-mep-cuestionarios-noticias-costa-rica

Amador, A (2021). Acceso y uso de las TIC en los hogares costarricenses. Informe de Prosic, UCR. Recuperado de http://www.prosic.ucr.ac.cr/sites/default/files/recursos/informe_prosic_2021_int._completo.pdf

Ávalos, A. (24 de enero, 2021). Fiscalía descarta llevar a juicio supuesto 'hackeo' a base de cotizantes de CCSS. Recuperado de https://www.nacion.com/el-pais/salud/fiscalia-descarta-llevar-a-juicio-supuesto-hackeo/6EWZHLKL2RFU5LNYG6JO354S5I/story/

Ávalos, A. (8 de octubre, 2015). Agencia de protección de datos suspende investigación por «hackeo» en planillas de CCSS . Recuperado de https://www.nacion.com/el-pais/salud/agencia-de-proteccion-de-datos-suspende-investigacion-por-hackeo-en-planillas-de-ccss/DQNMCWNFFZFN5LIUNJ5FYTN5AE/story/

Barrio, M. (2020) Manual de Derecho Digital. Tirant lo Blanch.

Barrio, M (24 de junio de 2022) Sobre el metaverso y su impacto en el Derecho Recuperado de https://confilegal.com/20220624-sobre-el-metaverso-y-su-impacto-en-el-derecho/

Barrio Andrés, M. (2021). Génesis y desarrollo de los derechos digitales. Revista De Las Cortes Generales, (110), 197-233. Https://doi.org/10.33426/rcg/2021/110/1572

BBC Mundo (22 de diciembre, 2014) "Sextorsión", el chantaje por internet que deja indefensos a cientos de miles de hombres. Recuperado de https://www.bbc.com/mundo/noticias/2014/12/141222_tecnologia_sextorsion_chantaje_internet_sexo_extorsion_ig

Belcic, I.(5 de febrero, 2020). Guía esencial del phishing: cómo funciona y cómo defenderse. Recuperado de https://www.avast.com/es-es/c-phishing

Ciberseguridad en Costa Rica (Octubre, 2010). PROSIC. Recuperado de http://www.prosic.ucr.ac.cr/sites/default/files/documentos/ciberseguridad_2010.pdf

Consejo Irlandés de Libertades Civiles (16 de mayo, 2022). The Biggest Data Breach [La mayor filtración de datos]. Recuperado de https://

www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/

Consejo de Europa (2022). Democracia. Recuperado de https://www.coe.int/es/web/compass/democracy

Consejo de Europa (2014). Guía de los derechos humanos para los usuarios de internet. Recuperado de https://rm.coe.int/16804c177e

Consejo de Europa (18 de agosto de 2018). Informe de Evaluación Inicial -País, Costa Rica-, Capacidades de Justicia Penal en materia de cibercrimen y evidencia electrónica.

Constitución Española (1978). Cortes Generales, España. Recuperada de https://www.boe.es/buscar/act.php?Id=BOE-A-1978-31229

Cordero, M. (17 de diciembre, 2021) Sala IV: MEP lesionó derecho a la intimidad de estudiantes y sus familias con aplicación de pruebas FARO. Recuperado de https://semanariouniversidad.com/pais/sala-iv-mep-lesiono-derecho-a-la-intimidad-de-estudiantes-y-sus-familias-con-aplicacion-de-pruebas-faro/

Córdoba, J. (1 de mayo, 2022). Innovación regulatoria en defensa de los Derechos Humanos. Recuperado de https://www.diarioextra.com/Noticia/detalle/471086/innovaci-n-regulatoria-en-defensa-de-los-derechos-humanos

Cyphers, B. (19 de marzo de 2020) Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It. (Google dice que no "vende" tus datos. Así es como la empresa los comparte, monetiza y explota.) Recuperado de https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and

Deam, S. (3 de junio de 2020). Los datos clave sobre la ley de internet que Trump quiere cambiar. Recuperado de https://www.latimes.com/espanol/politica/articulo/2020-06-03/los-datos-clave-sobre-la-seccion-230-la-ley-de-internet-que-trump-quiere-cambiar

Derechos Digitales, América Latina (11 de febrero de 2022). Carta al presidente y a la Asamblea Legislativa de El Salvador. Las reformas legales en El Salvador: un gran retroceso en los derechos humanos y el Estado democrático. Recuperado de https://www.derechosdigitales.org/17840/las-reformas-legales-en-el-salvador-un-gran-retroceso-en-los-derechos-humanos-y-el-estado-democratico/

EFF (3 de abril de 2015). Section 230 of the Communications Decency Act [Seccón 230 de la Ley de Decencia de las comunicaciones] Recuperado de https://www.eff.org/es/issues/cda230

Europa Press. (2 de Julio, 2022) El 74% de los españoles cree, erróneamente, que es posible borrar totalmente su presencia en la Red. Recuperado de https://www.20minutos.es/tecnologia/ciberseguridad/el-74-de-los-espanoles-cree-erroneamente-que-es-posible-eliminar-totalmente-su-presencia-en-la-red-5024450/

Fitz, M (9 de abril de 2019). ¿Qué son los Panama Papers?. Recuperado de https://www.infobae.com/politica/2019/04/09/que-son-los-panama-papers/

Fernández, Y. (14 de mayo, 2021). Qué es la Dark Web, en qué se diferencia de la Deep Web y cómo puedes navegar por ella. Recuperado de https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedes-navegar-ella

Gobierno de España (14 de julio 2021). Carta de Derechos Digitales. Recuperado de https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_redes.pdf

Google (2022). Acerca de la segmentación por lista de clientes. Recuperado de https://support.google.com/google-ads/answer/6379332?Hl=es

Guzmán, L. (2021). Chile, pionero en la protección de los "neuroderechos". Recuperado de https://es.unesco.org/courier/2022-1/chile-pionero-proteccion-neuroderechos

Herrera, H. (18 de enero, 2022) ¿Qué es el Metaverso por el que Zuckerberg lo está apostando todo? Recuperado de https://www.larazon.es/ciencia/20220118/hlemfz27inffxfeexxmeonm3ti.html

Hernández, J. (2018). Expectativas de Privacidad, Tutela de la intimidad y protección de datos. Sociedad Digital y Derecho. Recuperado de https://www.boe.es/biblioteca_juridica/publicacion.php?Id=PUB-NT-2018-97

Hill, M. (29 de enero, 2021) 66% of Workers Risk Breaching GDPR by Printing Work-Related Docs at Home (El 66% de los trabajadores se arriesga a incumplir el GDPR al imprimir en casa documentos relacionados con el trabajo). Recuperado de https://www.infosecurity-magazine.com/news/workers-printing-docs-home/

Kaspersky (2022) ¿Qué es la Deep Web y la Dark Web?. Recuperado de https://www.kaspersky.es/resource-center/threats/deep-web

Jones, H (2021). Real-Time Bidding: The Ad Industry Has Crossed A Very Dangerous Line (Puja en tiempo real: La industria publicitaria ha cruzado una línea muy peligrosa) Recuperado de https://www.forbes.com/sites/hessiejones/2021/10/18/real-time-bidding-the-ad-industry-has-crossed-a-very-dangerous-line/?Sh=103d3ee748ca

Jiménez, E. (14 de agosto, 2018) Plazas para investigar caso del cemento chino enfrentan a director del OIJ y Consejo Superior. Recuperado de https://www.nacion.com/sucesos/judiciales/plazas-para-investigar-caso-del-cemento-chino/A6JYAWZROZAMPBZOVL4HTTRVUM/story/

Jiménez, E. (9 de mayo, 2022) Delincuentes compran datos sensibles de bancos para escoger a víctimas de estafa. Recuperado de https://www.nacion.com/sucesos/judiciales/delincuentes-compran-datos-sensibles-de-bancos/XDZLR7D7PBCXXGADJETSCGHTX4/story/

Ley de Privacidad del Consumidor de California. 2018. Estados Unidos.

Ley francesa relativa a la informática, ficheros y libertades (1978). Recuperada de https://wipolex.wipo.int/es/text/514593

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

Lopez, M. (15 de noviembre, 2021). MEP acoge medida del Tribunal de no destruir los polémicos cuestionarios de factores asociados, aplicados en pruebas FARO. https://www.larepublica.net/noticia/mep-acoge-medida-cautelar-del-tribunal-de-no-destruir-los-polemicos-cuestionarios-de-factores-asociados-aplicados-en-pruebas-faro

Medrano, J. (23 de julio, 2021). El problema con la regulación del Child Grooming en el proyecto de ley № 21.507. Recuperado de https://adalidmedrano.com/child-grooming-proyeto/2021/

Medrano, J. (17 de mayo, 2021). El delito de violación de datos personales. Revista Tribuna Libre, Edición 8/1. Recuperado de https://tribunalibre.uescuelalibre.cr/edicion-8-1-derecho-informatico/

Miranda, W. (27 de octubre de 2020). Nicaragua aprueba una ley que impone penas de cárcel a quienes el gobierno considere que publi-

quen noticias falsas. Recuperado de https://elpais.com/internacional/2020-10-27/daniel-ortega-aprueba-una-ley-para-imponer-carcel-a-quienes-considere-que-publiquen-noticias-falsas-en-nicaragua.html

Mora, A. (24 de noviembre, 2021). MEP entrega al Contencioso los cuestionados cuestionarios asociados a las pruebas FARO. Recuperado de https://delfino.cr/2021/11/mep-entrega-al-contencioso-los-cuestionados-cuestionarios-asociados-a-las-pruebas-faro

Moreno, M. (27 de agosto, 2020). Más de 2.400 departamentos de policía de todo el mundo utilizan Clearview AI, la controvertida herramienta de reconocimiento facial que robó millones de fotos de Facebook para crear su base de datos. Recuperado de https://www.businessinsider.es/2400-policias-usan-clearview-ai-reconocimento-facial-705589

Murillo, E. (2 de mayo, 2022) Expertos en Derecho e Informática criticaron un proyecto de ley que pretende regular la actividad de criptoactivos en el país. Recuperado de https://www.crhoy.com/tecnologia/fdsespecialistas-cuestionan-proyecto-de-ley-para-regular-criptoactivos/

Muñoz, D. (25 de febrero, 2020). Pretenden revertir los avances en datos abiertos. Recuperado de https://semanariouniversidad.com/bloque1/pretenden-revertir-los-avances-en-datos-abiertos/

NordVPN. (2022) Analyzing 4 million payment card details found on the dark web (Analizando 4 millones de datos de tarjetas de pago encontrados en la web oscura) Recuperado de https://nordvpn.com/es/research-lab/payment-card-details-theft/

OEA, (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.

OPI. (5 de abril de 2016). Los Panamá Papers sacuden Costa Rica. Recuperado de https://opi.ucr.ac.cr/node/632

Orellana, 3 (22 de junio de 2022). ¿Qué es el metaverso, cómo funciona y quiénes están detrás? Recuperado de https://es.digitaltrends.com/realidad-virtual/que-es-metaverso/

París, M. (28 de enero, 2020). Estrategia de Privacidad.

París, M. (9 de agosto, 2022) . La reforma del artículo 24 de la Constitución. Recuperado de https://www.nacion.com/opinion/foros/la-reforma-del-articulo-24-de-la-constitucion/3AS65CJEEZCCZFTHF26QZT7GZA/story/

Pascual, M (29 de octubre, 2021). Metaverso: el mundo virtual donde Zuckerberg quiere que compres, te diviertas y trabajes. Recuperado de https://elpais.com/tecnologia/2021-10-30/metaverso-el-mundo-virtual-donde-zuckerberg-quiere-que-compres-te-diviertas-y-trabajes.html

Pridat (2022) Página principal. Recuperado de https://pridat.org

Prospect (5 de noviembre de 2021) New protections needed to stop employer surveillance of remote workers (Se necesitan nuevas protecciones para frenar la vigilancia de los trabajadores a distancia por parte del empresario). Recuperado de https://prospect.org.uk/news/new-protections-needed-to-stop-employer-surveillance-of-remote-workers

Redacción. (8 de marzo de 2019). Los planes de Rusia para castigar las “fake news” y mandar a la cárcel a quienes hablen mal del gobierno. Recuperado de https://www.bbc.com/mundo/noticias-internacional-47492208

Resolución No 01345 – 1998, Sala Constitucional de Costa Rica.

Rallo Lombarte, A. (2020). Una nueva generación de derechos digitales. Revista de Estudios Políticos, 187, 101-135. Doi: https://doi.org/10.18042/cepc/rep.187.04

Rojas, L. (20 de octubre, 2015) BAC se contradice por supuesto robo de datos a la Caja Recuperado de https://archivo.crhoy.com/bac-se-contradice-por-supuesto-robo-de-datos-a-la-caja/nacionales/

Romero, F. (6 de Julio, 2022). Tecnología de reconocimiento facial: cómo se usa en Ucrania y por qué sigue siendo tan controvertida. Recuperado de https://theconversation.com/tecnologia-de-reconocimiento-facial-como-se-usa-en-ucrania-y-por-que-sigue-siendo-tan-controvertida-185458

Sanger, D. (11 de setiembre, 2020) Russian Criminal Group Finds New Target: Americans Working at Home (El grupo criminal ruso encuentra un nuevo objetivo: Los estadounidenses que trabajan en casa) Recuperado de https://www.nytimes.com/2020/06/25/us/politics/russia-ransomware-coronavirus-work-home.html

SEKOIA.IO (2022) SEKOIA.IO Mid-2022 Ransomware Threat Landscape .(Panorama de la amenaza del ransomware SEKOIA.IO Mid-2022) Recuperado de https://blog.sekoia.io/sekoia-io-mid-2022-ransomware-threat-landscape/

Sophos (2022). The State of the Ransomware 2022 (El Estado del Ransomware 2022). Recuperado de https://www.sophos.com/es-es/white-paper/state-of-ransomware

Solove, D. (2002). Conceptualizando Privacidad [Conceptualising Privacy]. California Law Review. Recuperado de https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?Article=2086&context=faculty_publications

Zamora, F. (5 de agosto, 2022) Una propuesta imprudente. Recuperado de https://www.nacion.com/opinion/columnistas/una-propuesta-imprudente/FOY4OSBTJZAO-7PAPP2XMNJSDV4/story/

Valverde, L. (21 de abril de 2022). Hacienda indagó a más de 200 empresas por presunto fraude o infracciones tributarias. Recuperado de https://www.crhoy.com/economia/hacienda-indago-a-mas-de-200-empresas-por-presunto-fraude-o-infracciones-tributarias/

Velásquez, A. (21 de Agosto de 2012) Expertos creen que Ley de Delitos Informáticos debe ser equilibrada en aspectos jurídicos y técnicos. Recuperado de https://www.ucr.ac.cr/noticias/2012/08/21/expertos-creen-que-ley-de-delitos-informaticos.html

ENTREVISTAS

Fabián Volio Echeverría. Abogado Especialista en Derecho Constitucional. 28 de julio de 2022.

Miguel Ramírez. Fiscal Adjunto de la Fiscalía Adjunta de Fraudes y Ciberdelincuencia. 21 de junio de 2022.