7

Capítulo

Riesgos en el tratamiento de datos personales relativos a la salud en tiempos de pandemia

José Adalid Medrano Melara

Las tecnologías de la información y la comunicación (TIC) han transformado de manera acelerada a la sociedad en la que vivimos, con cambios más pronunciados que los que ha experimentado la humanidad en siglos, lo que deja poco espacio para la comprensión de las implicaciones de estos y el cómo debe abordarse desde la educación y el derecho.

La pandemia ha profundizado la dependencia a la tecnología, generado exclusión para todo aquel que no pueda accederla de la manera adecuada; al mismo tiempo ha sido un motor de transformación social que se dirige a favorecer a los grupos más capacitados para sacarle ventaja. Por lo anterior, debemos avanzar en la reducción de la brecha digital, sin descuidar los programas educativos sobre cómo usar las TIC de manera responsable y cómo sacarle provecho.

Una sociedad que no comprende la importancia de la privacidad, la ciberseguridad y la autodeterminación informativa no está preparada para el uso de las TIC, ya que esa vulnerabilidad en el conocimiento va a ser explotada por diferentes actores delictivos, comerciales y políticos que la utilizarán para sus propios fines. La candidez de las personas usuarias se aprovecha a diario y suele causar graves daños económicos, políticos y morales, sin que realmente exista una opción para dejar de utilizar tecnología sin una consecuencia grave para la vida de las personas.

Debido a la ubicuidad tecnológica el concepto de privacidad, construido con paradigmas de siglos pasados, está siendo desafiado y la pandemia ha resaltado aún más la tendencia a reducir la expectativa que tiene todo ciudadano de esta, lo que conlleva a cambios importantes en el corto, mediano y largo plazo, que deben ser analizados de manera extensa. El uso intensivo de medios sociales, así como el aumento de sensores y cámaras de vigilancia -inclusive con reconocimiento facial- que rastrean el paso por las vías físicas y electrónicas, lleva a las personas a cuestionarse si ya es muy tarde para proteger la privacidad, si ya hemos renunciado a esta, en favor del crecimiento económico y tecnológico, o si todavía hay tiempo de fortalecerla.

La privacidad es un bien jurídico de gran importancia y la base de todo sistema democrático, sin embargo, cuenta con la pecu-

liaridad de estar construida con un material flexible que le permite irse adaptando a la noción que de ella que se va construyendo en toda sociedad. Por ende, dependerá en gran manera del conocimiento que tengan las personas sobre los riesgos inherentes a la reducción de lo que vamos considerando aceptable.

De lo anterior deriva la importancia del fortalecimiento de los programas educativos y las campañas de concientización que le permitan a toda la población la comprensión más completa sobre las consecuencias de las decisiones diarias que se toman sobre esta materia y sobre los alcances de la legislación.

Figura 7.1. Violaciones a la privacidad

Fuente: Elaboración propia.

Una sociedad más educada es menos complaciente con los cambios que buscan reducirle el ámbito de protección de su vida privada, lo que lejos de ser un obstáculo para la innovación y el crecimiento económico es una oportunidad para la participación sobre el cómo deben regularse ciertas materias. Como dato histórico, es interesante señalar que durante los primeros proyectos que se discutieron en el país sobre una ley sanitaria hubo poco apoyo por parte de gobernantes del país debido al temor de lastimar algunas libertades individuales, principalmente la correspondiente a la inviolabilidad del domicilio. Lo anterior, refleja que su discusión no fue totalmente pacífica[1] y que mucho le debe su aprobación al hecho que se discutiera ya con los conocimientos adquiridos en la lucha contra contra la pandemia de gripe de 1918, con un resultado donde se cedieron libertades individuales en favor de la salud pública[2].

Por otro lado, durante la pandemia Covid-19, se ha evidenciado en la población cierta despreocupación, relajamiento o desconocimiento con respecto a ciertas prácticas que afectan la privacidad. En ese sentido, las y los ciudadanos han visto como algo aceptable la toma de la temperatura antes de ingresar a distintos establecimientos, aunque esta captura del dato sensible lo realicen personas cuyos oficios no guardan ninguna relación con el de salud y/o con el secreto funcional, como lo exige la ley. A pesar de que la ley no se cumple, faltan pronunciamientos sobre la legalidad de la práctica o la elaboración de protocolos de actuación por parte de la Agencia de Protección de Datos de los Habitantes (Prodhab) dirigidas a mitigar el impacto sobre la privacidad ciudadana.

1 La Ley sobre Protección de la Salud Pública se aprobó en 1923, y como lo reseña Zúñiga (2007) el ilustre galeno Solón Muñoz en un artículo publicado en La Nación en 1963 indica que fue tan previsora "satisfizo las necesidades crecientes del país durante 20 años", a pesar de que los primeros intentos de codificación sanitaria tuvieron poco apoyo por parte de los gobernantes de la época.

2 Como lo indica el Semanario "La "gripe española", como se le llamó al nuevo tipo de influenza propagado al son de los tambores de la I Guerra Mundial, llegó a finales de febrero de 1920 y la tomó con las defensas por el suelo, cuando la esperanza de vida al nacer no llegaba ni a los 30 años" (Murillo, 2020).

En el sentido opuesto, a la luz de la pandemia, se puede analizar cómo la privacidad debe tener límites, ya que se han visto casos en los que algunas personas han tomado decisiones vinculadas con su derecho de autodeterminación informativa al no informar, antes de ingresar en un hospital, que pertenecen a una burbuja familiar donde existe una persona que padece Covid-19, lo que ha expuesto al personal médico.

Los ejemplos anteriores generan un interesante debate sobre las excepciones que deben imperar en tiempos de pandemia y la regulación especial que debe surgir del mismo, ya que cada país enfrenta el Covid-19 con las capacidades biológicas de sus ciudadanos, la fortaleza de sus instituciones y de los plexos normativos vinculados con la batalla contra esta amenaza viral, que en el caso de la protección de la privacidad, a nuestro país lo encuentra debilitado, no solo por la falta de cultura de privacidad imperante, sino también por sus instituciones endebles y escándalos nacionales que generan desconfianza en la población sobre la protección de un derecho fundamental como la autodeterminación informativa.

En este capítulo relataremos las oportunidades inherentes al uso de las TIC en el campo de la salud, el derecho de autodeterminación informativa, las violaciones a la privacidad en nuestro país y los cambios regulatorios durante la pandemia, así como el avance acelerado del cibercrimen.

7.1 LA PROTECCIÓN DE LOS DATOS PERSONALES

¿Qué es un dato personal?

La normativa costarricense de protección de datos personales le define como "cualquier dato relativo a una persona física identificada o identificable" (Ley N°8968, 2011, artículo 3, inciso b). Ejemplos de datos personales son los siguientes:

1. Nombre de una persona.
2. Cédula de identidad.
3. Dirección de correo electrónico (ej. sunombrecr@gmail.com)
4. Expediente médico de una persona.
5. Dictamen médico.

El Convenio 108 del Consejo de Europa *"Para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal"* (1981), al que Costa Rica ha mostrado interés en adherirse[3], en el artículo 2 (inciso a), define dato personal como: "cualquier información relativa a una persona física identificada o identificable". El Reglamento General de Protección de Datos (RGPD), al que se le considera como un estándar en materia de protección de datos y que fue emitido en el 2016 lo define de una manera más amplia:

> toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (Reglamento General de Protección de Datos, 2016, artículo 4).

La Sala Constitucional, en el año 2002, define al dato personal e indica que en el caso de los datos sensibles, como los relativos a la salud, estos no pueden ser accedidos sin el consentimiento expreso del titular:

> III.- El objeto de protección del hábeas data y los principios básicos para la protección de datos. Objeto de protección del hábeas data son los "datos de carácter personal", es decir, **cualquier información relativa a una persona** física o jurídica **identificada o identificable.** El grado de protección de los datos dependerá de la naturaleza de los mismos, así, debe el Estado procurar que los datos íntimos (también llamados "sensibles") de las personas no sean siquiera accedidos sin su expreso consentimiento. (Sala Constitucional, Resolución Nº 08996 – 2002)

3 El Encuentro Anual de autoridad de Protección de Datos Personales del año 2018 fue clausurado por el presidente Carlos Alvarado y "manifestó el firme compromiso que tiene el país con el tema y anunció la próxima adhesión de Costa Rica al Convenio 108 del Consejo de Europa". (Boletín Informativo, 2018).

El derecho de autodeterminación informativa

Este derecho digital es esencial para el desarrollo de las personas en la era de la sociedad de la información en donde el tratamiento de los datos personales -por parte de empresas, organizaciones o el Estado- es necesario para que puedan darnos los servicios que requerimos sin tener que renunciar a nuestra dignidad, honor, vida privada y libertades individuales inherentes a nuestra persona.

Nació con el fin de evitar que se propicien acciones discriminatorias, como un derecho de control que tiene el individuo sobre el flujo de informaciones que conciernen a su persona, el cual está conformado por principios, garantías y excepciones contenidos en el ordenamiento jurídico.

En la normativa costarricense de protección de datos personales[4] y en diversas resoluciones de la Sala Constitucional se ha definido a la autodeterminación informativa como un derecho fundamental derivado del derecho a la privacidad, que tiene toda persona sobre el flujo de informaciones que conciernen a su persona, de acuerdo a las garantías y excepciones que contiene el ordenamiento jurídico, con el fin de evitar que se propicien acciones discriminatorias.

Trece años antes que contáramos con una ley de protección de datos, en febrero de 1998, la Sala Constitucional costarricense reconoce los retos de la sociedad informatizada y el concepto clásico del derecho a la intimidad:

> El derecho a la intimidad. Lo que hoy conocemos como "sociedad informatizada" plantea nuevos retos al concepto clásico del derecho a la intimidad. En la décadas 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 que fin le eran solicitados sus datos personales, quienes tienen acceso a ellos y con cual objeto. Consecuentemente, el derecho a la protección de la persona frente al procesamiento de sus datos personales es una cuestión que se deja sólo a la academia. Es pronto también para cuestionarse si la manipulación de los datos personales puede vaciar el contenido esencial de algunos de los derechos fundamentales. Menos aún se concibe que el desarrollo informativo pueda implicar alguna forma de violencia. En la actualidad, la doctrina nacional y extranjera, admite que la manipulación de la información posibilita el control sobre el ciudadano como una alternativa real y efectiva. De tal manera que los derechos individuales de los ciudadanos puedan quedar prácticamente sin contenido efectivo. (Resolución Nº 01345 - 1998)

En relación con la tecnología, la Sala Constitucional deja claro que la esfera privada ya no se reduce al domicilio o a las comunicaciones[5]:

> 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 las y 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 a las personas una tutela a la intimidad que implique la posibilidad de controlar la información que lo pueda afectar. Lo expuesto, significa que el tratamiento electrónico de datos, como un presupuesto del desarrollo de nuestra actual sociedad democrática debe llevarse a cabo afianzando los derechos y

4 El artículo 4 de la ley Autodeterminación informativa N°8968, define al derecho de autodeterminación informativa de la siguiente manera: "Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.
Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias" (Ley Nº 8968, 2011, artículo 4).

5 En línea similar, en 1991 (ley Nº 7242) y 1996 (Ley Nº 7607) se reformó el artículo 24 de la Constitución Política, y es importante destacar que en la primera se amplió la protección de los documentos y comunicaciones, incluyendo ya no solo las escritas u orales, sino las de cualquier tipo, lo que se extiende a las contenidas en soportes electrónicos.

> garantías democráticas del ciudadano (arts. 24, 1, 28, 30, 33 y 41 de la Constitución). (Sala Constitucional, Resolución Nº 01345 - 1998)

Finalmente, la Sala Constitucional sin reconocerla como autodeterminación informativa, reconoce el derecho de control de las personas sobre sus datos personales:

> El Derecho a la Intimidad implica reconocer y aceptar el derecho fundamental de toda persona física o jurídica a conocer lo que conste sobre ella, sus bienes o derechos en cualquier registro o archivo, de toda naturaleza, incluso mecánica, electrónica o informatizada, sea público o privado; así como la finalidad a que esa información se destine y, en su caso, a que se rectifique, actualice, complemente o suprima, cuando el sujeto considera que la misma es incorrecta, inexacta o que implique discriminación. Lo mismo que a no ser utilizada o divulgada indebidamente y se respete su legítima confidencialidad. El fin de este derecho consiste en que cualquier persona tenga la posibilidad de defenderse contra calificaciones sospechosas incluidas en registros que sin darle derecho a rectificarlas o contradecirlas podrían llegar a causarle un grave perjuicio. Este derecho _como todos los fundamentales_ es personal, a favor de su titular (Resolución Nº 01345 - 1998)

Un año después, la Sala Constitucional reconoce la autodeterminación informativa, sus principios y la protección de los datos sensibles:

> Es la llamada protección a la autodeterminación informativa de las personas, la cual rebasa su simple ámbito de intimidad. Se concede al ciudadano el derecho a estar informado del procesamiento de los datos y de los fines que con él se pretende alcanzar, junto con el derecho de acceso, corrección o eliminación en caso el que se le cause un perjuicio ilegítimo.
>
> El derecho de autodeterminación informativa tiene como base los siguientes principios: el de transparencia sobre el tipo, dimensión o fines del procesamiento de los datos guardados; el de correspondencia entre los fines y el uso del almacenamiento y empleo de la información; el de exactitud, veracidad, actualidad y plena identificación de los datos guardados; de prohibición del procesamiento de datos relativos a la esfera íntima del ciudadano (raza, creencias religiosas, afinidad política, preferencias sexuales, entre otras) por parte de entidades no expresamente autorizadas para ello; y de todos modos, el uso que la información se haga debe ser acorde con lo que con ella se persigue; la destrucción de datos personales una vez que haya sido cumplidos el fin para el que fueron recopilados; entre otros. (Sala Constitucional, Resolución N°04847-99)

En 1998, al momento de la primera resolución de la Sala relacionada con la protección de los datos personales, en la Asamblea Legislativa se discutía el proyecto de ley 12.827 sobre el Recurso de Habeas Data, el cual reformaba la Ley de Jurisdicción Constitucional y establecía a la Sala Constitucional como autoridad nacional en esa materia. De esta manera, lo indica la opinión jurídica de la Procuraduría General de la República, por parte del procurador constitucional Odilón Méndez, sobre el numeral 19 de dicho proyecto:

> CAPITULO IV.- Autoridad Nacional de Protección de datos.
> SECCION I. Naturaleza, atribuciones y competencias.
>
> Art. 19.- Naturaleza.
>
> Para el proyecto elaborado en Costa Rica, en trámite de aprobación ante la Asamblea Legislativa, se tiene que el órgano encargado para conocer del trámite informatizado de datos, con atribuciones y competencia absolutas, es la SALA CONSTITUCIONAL de la Corte Suprema de Justicia, que por lo demás conoce de las acciones de Inconstitucionalidad, los Recursos de Amparo y Hábeas Corpus. El Proyecto 12827 propone la adición a un nuevo Capítulo IV, denominado "del Recurso de Hábeas Data", al Título III de la Ley de la Jurisdicción Constitucional, Ley No. 7135, de 1989. Este es un órgano cuyas resoluciones son irrecurribles y funciona en forma independiente y absoluta al amparo de esta ley. La Sala Constitucional tendrá jurisdicción completa sobre estos casos y su naturaleza, atribuciones y poderes. Competencias, entre otros, ya están previstos en la ley mencionada. (OJ- 040-98, PGR, 1998).

Trece años antes, con la aprobación de la ley № 8968 (2011), el país decidió crear una autoridad nacional de datos adscrita al Ministerio de Justicia y Paz, como un órgano de desconcentración máxima, con independencia de criterio, a la cual llamó Agencia de Protección de Datos de los Habitantes (Prodhab). Esta decisión parecía acertada, aunque en la práctica se ha demostrado que la independencia de la agencia no parece sólida, lo que ha quedado evidenciado con el caso UPAD, por lo que ahora no luce tan irracional lo que proponía el proyecto de ley № 12827, en cuanto a que sea la Sala Constitucional de forma exclusiva quien resuelva los casos de Habeas Data, al menos en los casos donde el infractor sea el Estado.

En esa línea, y como una manera de ver cómo se desarrollaba la discusión en aquel momento, donde las y los costarricenses daban sus primeros pasos en el acceso a internet, es de gran valor leer un extracto de la opinión jurídica citada supra en cuanto a lo que llama como el Poder Informático:

> Ante la proliferación de centros de información que recogen datos de las personas, ha surgido lo que se ha dado a conocer como Poder informático, que bien puede ser controlado por entes públicos o privados. Ello es así porque constantemente las personas están brindando información propia que es conocida y divulgada mediante bancos de datos. Estos podrían ser objeto de calificaciones que se presten para discriminaciones, intromisiones de su intimidad, persecuciones en el campo económico y laboral, y las más sutiles violaciones a los derechos de la personalidad, la imagen y el honor, como pertenecientes al derecho a la autodeterminación informativa, toda vez que no exista una legislación adecuada y eficiente a la protección de dichos derechos y de la libertad informática y al principio de igualdad.
>
> Con los avances de la tecnología se hace más difícil llevar a cabo este control. En materia de datos personales, al ponerse en peligro distintos derechos de la personalidad, se dificulta la determinación de cual información está siendo recolectada, para qué fines, en qué forma y quiénes pueden acceder a ella.
>
> Es por ello que los legisladores ordinarios y constituyentes de nuestro tiempo deben buscar fórmulas jurídicas que permitan limitar o controlar el uso del poder informático. En Costa Rica, no queriendo permanecer al margen de esta problemática tan actual y haciéndose eco de las Recomendaciones emitidas en las anteriores Conferencias de Ministros de Justicia de los Países Iberoamericanos, en sentido de adoptar medidas legislativas encaminadas a proteger eficazmente los derechos de las personas afectadas por el uso de ordenadores tanto a nivel gubernamental como privado, recientemente ha impulsado en el seno de la Asamblea Legislativa un proyecto de ley (el número 12827) tendiente a garantizar el derecho a la autodeterminación informativa mediante el instrumento procesal conocido como HABEAS DATA, el cual ha sido reconocido por la doctrina, la jurisprudencia y las legislaciones avanzadas como garante de aquél derecho fundamental. Aunque en Costa Rica existe todo un aparato institucional y jurídico que ha permitido avanzar en materia constitucional en modo sorprendente y así regular los abusos de terceros a los derechos de los ciudadanos, no existe un control claro y específico respecto a la vida privada y a la informática. Hoy, la empresa privada así como órganos y entes públicos han instalado una estructura informática capaz de procesar y tener acceso a información confidencial de vital importancia para la intimidad personal y familiar de los ciudadanos, sin que exista un mecanismo claro que proteja al ciudadano contra una posible manipulación de los datos personales que lesionen sus derechos. (OJ-040-98, PGR, 1998).

A pesar de que el proyecto de ley fue aprobado en primer debate[6], el país tuvo que esperar 13 años más, para tener una ley de protección de datos, la cual vino a plasmar en

6 En 1998, la aprobación en primer debate del proyecto de ley sobre protección de datos personales fue cubierta por La Nación como "Ley limita divulgar datos" e iniciaba de la siguiente manera: "La Asamblea Legislativa aprobó ayer en primer debate un proyecto de ley que limita a personas y a la prensa a obtener y conocer información preservada en archivos computadorizados o manuales del Gobierno o el sector privado. (La Nación, 1998).

la norma que el derecho de autodeterminación informativa es un derecho fundamental, aunque en la práctica es discutible sobre si se generó una mejor protección.

7.2. PRINCIPIOS DE LA AUTODETERMINACIÓN INFORMATIVA

Este derecho que protege a los ciudadanos de tratamientos que pueden afectarle en su vida personal, lo conforman principios y garantías que se encuentran regulados en nuestra normativa, entre los que pueden mencionarse:

Principio de consentimiento informado (artículo 5, Ley № 8968)

Cuando se soliciten datos de carácter personal, es necesario que el responsable de la base de datos obtenga un consentimiento libre[7], en documento escrito - físico o electrónico- en el cual debe informar de previo a los titulares o a sus representantes, de modo expreso, preciso e inequívoco:

a. De la existencia de una base de datos de carácter personal.
b. De los fines que se persiguen con la recolección de estos datos.
c. De los destinatarios de la información, así como de quiénes podrán consultarla.
d. Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos.
e. Del tratamiento que se dará a los datos solicitados.
f. De las consecuencias de la negativa a suministrar los datos.
g. De la posibilidad de ejercer los derechos que le asisten.
h. De la identidad y dirección del responsable de la base de datos.

El consentimiento informado no será necesario en las siguientes circunstancias:

a) Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo.

b) Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general.

c) Los datos deban ser entregados por disposición constitucional o legal.

Principio de calidad de la información (artículo 6, Ley № 8968)

Los datos personales únicamente pueden ser recolectados, almacenados o empleados para su tratamiento cuando los mismos sean actuales, veraces, exactos y adecuados al fin para el cual fueron recolectados.

El legislador estableció el derecho al olvido al establecer que en ningún caso se puedan conservar datos personales que puedan afectar al titular, de cualquier modo, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados[8]. Al mismo tiempo, indica la ley que en caso de que sea necesaria la conservación de esos datos, en un plazo superior al establecido se deberán desasociar de su titular. De acuerdo con este principio, el responsable de la base de datos deberá:

1. Velar por que los datos sean tratados de manera leal y lícita.

7 De acuerdo al reglamento, el consentimiento debe ser libre, lo que significa que "no debe mediar error, mala fe, violencia física o psicológica o dolo, que puedan afectar la manifestación de voluntad del titular" ((Artículo 4, Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales N° 37554-JP, 2016).

8 De manera contradictoria con lo que establece la ley, el reglamento en su artículo 11 establece:
"La conservación de los datos personales que puedan afectar a su titular, no deberá exceder el plazo de diez años, **desde la fecha de terminación del objeto de tratamiento del dato,** salvo disposición normativa especial que establezca otro plazo, que por el acuerdo de partes se haya establecido un plazo distinto, que exista una relación continuada entre las partes o que medie interés público para conservar el dato" (Artículo 11, Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales N° 37554-JP, 2016).

2. Modificar o suprimir los datos que falten a la verdad.
3. Eliminar los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados.
4. Recopilar los datos con fines determinados, explícitos y legítimos: no serán tratados posteriormente de manera incompatible con dichos fines.
5. Tomar las medidas necesarias para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.

Derecho de acceso a la información (artículo 7, inciso 1, Ley № 8968)

La información personal deberá ser almacenada de tal forma que permita que la persona interesada tenga garantía plena del ejercicio de su derecho de acceso, con las siguientes facultades:

a. **Obtener en intervalos razonables**, **sin demora y a título gratuito**, **la confirmación o no de la existencia de datos suyos en archivos o bases de datos.** En caso de que sí existan datos suyos, estos deberán ser comunicados a la persona interesada en forma precisa y entendible.

b. **Recibir la información relativa a su persona, así como la finalidad con que fueron recopilados y el uso que se le ha dado a sus datos personales.** El informe que contenga esta información deberá ser completo, claro y exento de codificaciones. De la misma manera, si existen términos técnicos, deberá acompañarse de una explicación de los términos técnicos que se utilicen en el mismo.

c. **Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al titular.**

d. **Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales.**

El responsable de la base de datos deberá evacuar la consulta de información dentro del plazo de cinco días hábiles a partir de la recepción de la solicitud. De acuerdo al reglamento, salvo que la persona interesada demuestre de manera fundamentada que existe una vulneración de sus derechos, podrá ejercer este derecho con un intervalo mínimo de seis meses.

Derecho de rectificación (artículo 7, inciso 2, Ley № 8968)

El titular o la persona interesada podrá solicitar que sus datos sean:

a. **Actualizados:** cuando hayan dejado de ser actuales.

b. **Rectificados**: cuando resulten ser inexactos, incompletos o confusos.

c. **Eliminados:** cuando se hayan tratado con infracción a la ley, en particular a causa del carácter incompleto o inexacto de los datos, o hayan sido recopilados sin autorización del titular.

Garantía de confidencialidad, (artículos 7, incisos 2-y 11, Ley № 8968)[9]

Es la obligación de toda persona que tenga participación en el tratamiento o almacenamiento de datos personales, de cumplir con el deber de confidencialidad. Ya sean empleados o funcionarios que trabajen directamente con o como el responsable de la base de datos, intermediario tecnológico o proveedor de servicios **están obligados al secreto profesional o funcional**, el cual no fenece una vez de finalizada su relación con la base de datos. Sin embargo, esta obligación podría ser relevada por orden judicial en lo estrictamente necesario y dentro de la causa que conoce.

7.3. DATOS PERSONALES RELATIVOS A LA SALUD

La condición de salud de una persona es un motivo protagónico por el cual se han discriminado a las personas en la historia, por lo que no es de extrañar que la información

9 En la ley esta garantía se encuentra contenida en el derecho de rectificación, aunque por ser de naturaleza distinta, se desarrolla de manera autónoma.

personal relativa a la salud a nivel legal goce con una mayor protección, porque es claro que el abuso de estos datos puede generar un grave impacto en la vida de las personas.

En el derecho comparado, vemos como el derecho de control sobre el conocimiento que pueden tener terceros de nuestra vida privada se ha venido desarrollando como un ámbito subjetivo de libertad garantizado por el sistema jurídico estadounidense, en donde las resoluciones constitucionales han tenido gran relevancia. En esa línea, el caso Griswold vs. Connecticut generó un precedente judicial histórico, que como lo indican Valenzuela y Villacencio (2015), en Estados Unidos se da la instauración del derecho a la privacidad como fundamento para evitar la intervención del Estado en temas relacionados con los derechos sexuales y reproductivos de las mujeres, más precisamente, con el derecho a la anticoncepción. En este caso, la Corte Suprema de Justicia de los Estados Unidos declaró inconstitucional la Ley de Connecticut ya que violaba la privacidad de las personas, en un caso en donde fueron arrestados y procesados penalmente un ginecólogo y la directora de una clínica que se encargaban de informar parejas casadas sobre cómo prevenir la concepción y para tal efecto también distribuían los medios de prevención. Esto es sumamente relevante, porque como lo indica Saldaña (2007), la dificultad para definir con precisión el ámbito de la privacidad, ha motivado que la doctrina y jurisprudencia norteamericanas hayan adoptado una orientación pragmática, identificando progresivamente el conjunto de intereses relevantes que integran esta noción desde la perspectiva constitucional (Saldaña, 2007, pp. 87-86.). Esta resolución reconoce la privacidad como un principio inherente a la persona humana, que se encuentra protegido implícitamente en la constitución de los Estados Unidos. Como lo reseña Sánchez (2015)

> Por ello, en 1965 se derogó la ley de Connecticut, con una votación de 7 - 2. Fue el juez William Douglas quien escribió por decisión mayoritaria un nuevo derecho constitucional. La resolución del juez Douglas se basó en que existe un derecho constitucional implícito en la Constitución Norteamericana; él justificó, argumentó y confrontó los diferentes tipos de derechos por medio de la analogía y la hermenéutica, en diversos casos.
>
> En los casos mencionados se establece una relación lógica y coherente; en todos hubo una violación al "due process" -el debido proceso legal- contenido en la Decimocuarta Enmienda. Dicho proceso establece que, las autoridades públicas deben respetar todos los derechos que tiene la persona. Es decir, que el Estado o Gobierno no puede privar o entrometerse en los derechos del individuo, sin que haya habido un debido proceso. El juez William Douglas argumentó, con base en estos casos, que a pesar de que la Constitución y la Carta de Derechos (Bill of Rights) no establezcan la libre asociación, la libertad de los padres y tutores de dirigir la educación de los niños y la libre elección de la forma de educación; son considerados derechos periféricos de la Primera Enmienda (que establece que no se hará ley restringiendo la libertad, lo que equivale a decir que se tiene derecho a privacidad o a proteger la vida privada que de cualquier intromisión). Además, la Cuarta y la Quinta Enmiendas también fueron descritas como protectoras contra invasiones gubernamentales "de la santidad del hogar de un hombre y de las privacidades de la vida". También se considera a la Tercera y Cuarta Enmiendas como "derecho a la privacidad" reservado al pueblo.
>
> Estableció que el derecho a la privacidad es un derecho de la PERSONA fundamental, para poder existir en una sociedad libre. Puesto que vivir en una sociedad libre implica, que se reconozca el derecho de cada individuo, éste puede hacer uso de sus dominios privados, para alcanzar sus propios propósitos. Igualmente, reconoció el derecho de la propiedad privada y la privacidad familiar -en los cuales ni el Estado ni nadie podrá entrometerse-.
>
> Para concluir con el razonamiento del juez William Douglas, es preciso mencionar que, el derecho de la privacidad, se decretó que era un derecho más antiguo que la Declaración de los Derechos, más antiguo que los partidos políticos y que los sistemas escolares. Por ende, es un derecho fundamental y básico del individuo, como el de sus relaciones interpersonales -léase la relación matrimonial-. Por ello se declaró aquí ilegal el estatuto de Connecticut, por invadir el derecho a la privacidad de una relación matrimonial. (Sánchez, 2015)

En momentos en donde los sistemas informáticos de salud recopilan datos que pueden generar actos discriminatorios, como cuando están relacionados con la orientación sexual, enfermedades, entre otros estrictamente relacionados con nuestra vida privada y vinculados con nuestra salud, cobra especialmente relevancia esta histórica resolución en la cual se relaciona la libertad sobre un tema de salud reproductiva en la que para que el Estado pueda tener injerencia, debe hacerse el conocimiento de las decisiones de los ciudadanos. En los Estados Unidos desde 1996, a nivel federal, los datos personales relativos a la salud están protegidos por la Ley HIPAA (Ley de Portabilidad y Responsabilidad de Seguros Médicos), la cual regula de forma especial esta materia de forma expresa, protegiendo la información médica tanto del Estado como de sujetos privados, lo cual es especialmente relevante en el país norteamericano.

En nuestro país, distintas resoluciones de la Sala Constitucional y en nuestra ley de protección de datos personales, los datos relativos a la salud se encuentran comprendidos dentro de la categoría especial de datos personales sensibles. Los datos sensibles son definidos de la siguiente manera:

Información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, **información biomédica o genética, vida** y orientación sexual, entre otros. (Ley № 8968, 2011, artículo 3, inciso e.)

De acuerdo al RGPD, de la Unión Europea, los datos relativos a la salud se definen como aquellos datos personales referentes a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. (Reglamento General de Protección de Datos, 2016, artículo 4, inciso 15).

La ley № 8968 en su numeral 9 contiene dos importantes regulaciones sobre esta categoría especial:

1. **Establece que el suministro de datos personales sensibles no podrá ser obligatorio**. Lo anterior en la línea del consentimiento que debe ser libre y expreso.
2. **Prohíbe el tratamiento de datos que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas, así como los relativos a la salud, la vida y la orientación sexual,** entre otros. Esta norma genera una enorme inseguridad jurídica ya que la lista no solo no es taxativa, sino que permite toda clase de interpretaciones que pueden ser peligrosas para la innovación.

Las excepciones que contiene la ley para esta son las siguientes:

a. **El tratamiento de los datos sea necesario para salvaguardar el interés vital del interesado** o de otra persona, en el supuesto de que la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento.

b. **El tratamiento de los datos sea efectuado en el curso de sus actividades legítimas** y con las debidas garantías **por una fundación, una asociación o cualquier otro organismo, cuya finalidad sea política, filosófica, religiosa o sindical,** siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo, por razón de su finalidad y **con tal de que los datos no se comuniquen a terceros sin el consentimiento de las personas interesadas.**

c. **El tratamiento se refiera a datos que la persona interesada haya hecho públicos voluntariamente** o sean necesarios para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial.

d. **El tratamiento de los datos resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios,** siempre que dicho tratamiento de datos sea realizado por un funcionario o funcionaria del área de la salud, sujeto al secreto profesional o propio de su función, o por otra persona sujeta, asimismo, a una obligación equivalente de secreto.

La prohibición de este tratamiento debe interpretarse en concordancia con el principio de consentimiento libre y

expreso que debe darse en este tipo de tratamientos. En ese sentido, como un antecedente, en el año 2002, la Sala Constitucional estableció las reglas para el tratamiento de datos personales, prohibió el almacenamiento de estos datos en bases de datos privadas y en registros públicos y determinó que debían ser de acceso restringido:

> **Prohibición relativa a categorías particulares de datos**. Los datos de carácter personal de las personas físicas que revelen su origen racial, sus opiniones políticas, sus convicciones religiosas y espirituales, así como los datos personales relativos a la salud, vida sexual y antecedentes delictivos, no podrán ser almacenados de manera automática ni manual en registros o ficheros privados, y en los registros públicos serán de acceso restringido. (Sala Constitucional, Resolución Nº 8996- 2002).

Por otro lado, en España, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en la actualidad derogada), de la cual se inspiraron nuestros magistrados y legisladores para regular esta materia, rezaba en su artículo 7 sobre datos especialmente protegidos lo siguiente:

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, **nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.**

   Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, **se advertirá al interesado acerca de su derecho a no prestarlo.**

2. **Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias.** Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. **Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.**

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

   No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

   También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. (Ley Orgánica 15/1999, España, 1999)

La inspiración en la legislación española resulta evidente y como puede verse más que la prohibición absoluta del tratamiento de datos personales especialmente protegidos lo que se busca es que la recopilación o tratamiento de los datos no se dé sin el consentimiento del usuario, entre otras excepciones contenidas. En esa misma línea, el artículo 9, del Reglamento General de Protección de Datos (RGPD), en su apartado 2, inciso a), en cuanto a las excepciones de la prohibición al tratamiento establece el consentimiento explícito como la primera de ellas. Dicho artículo reza:

Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. (Reglamento General de Protección de Datos, artículo 9 apartado 1).

Salvo las siguientes excepciones:

a. **El interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados**, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b. El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c. El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d. El tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e. El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f. El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial; (Reglamento General de Protección de Datos, artículo 9 apartado 2).

7.4. INVESTIGACIÓN CIENTÍFICA EN TEMAS DE SALUD

En Costa Rica, desde el año 2014 se cuenta con la Ley Reguladora de Investigación Biomédica, la cual desarrolla el consentimiento informado y el principio de la calidad de la información. De acuerdo a esta, se debe asegurar la confidencialidad de la información, se le debe informar a las personas sobre sus derechos, el cual debe entenderse que incluirá el derecho de autodeterminación informativa y la información suficiente para que el consentimiento se brinde de forma libre, voluntaria y consciente:

> Previo a que se inicie cualquier actividad relacionada con la investigación y antes de que se proceda a firmar el consentimiento informado, el individuo participante deberá ser informado en su propio idioma, en un lenguaje apropiado y comprensible, sobre la naturaleza de la investigación, los procedimientos, los riesgos y beneficios, otras opciones terapéuticas o diagnósticas, **la confidencialidad de la información recabada** y **sobre sus derechos**, de manera que comprenda y tome la decisión de participar o no, de forma libre, voluntaria y consciente, sin coerción, coacción, amenaza, fraude, engaño, manipulación o cualquier otro tipo de presión.
>
> La información del consentimiento informado debe ser veraz, clara, precisa y escrita, de manera que no induzca a error, engaño o coacción y que pueda ser entendida por los participantes. Para

> este efecto, se deberá garantizar que el procedimiento para la firma del consentimiento informado cuente con el tiempo y las condiciones apropiados para que las personas puedan comprender correctamente la información. (Ley Reguladora de Investigación Biomédica, artículo 13, Calidad de la Información).

De acuerdo con los artículos 14 y 25 de ley № 9234 y en respeto del principio de calidad de la información contenido en el artículo 6 de la ley № 8968, los datos recopilados no podrán ser utilizados para un fin distinto para el que fueron recolectados:

> Se prohíbe la utilización de la información y de los datos relativos a la salud de las personas, con fines no contemplados o permitidos en el consentimiento informado o en la ley.
>
> El encargado de la investigación o ensayos clínicos y los responsables de esta solo podrán utilizar la información y los datos relativos a la salud de las personas participantes de conformidad con fines expresamente contemplados o permitidos en el consentimiento informado o en la ley. (Ley Reguladora de Investigación Biomédica, artículo 14, Información del consentimiento informado)

Sobre los fines que deben ser expresamente consentidos por el participante, se debe destacar un análisis de derecho comparado en materia de protección de datos personales, con respecto al considerando 33 del Reglamento General de Protección de Datos, el cual acepta las limitantes que se presentan en esta materia para conocer los fines específicos en una investigación científica:

> **Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida.** Por consiguiente, **debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica**. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida. (Reglamento General de Protección de Datos, 2016, considerando 33.)[10]

En esa misma línea, en España, la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales establece que:

> Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. (Ley Orgánica 3/2018, 2018, Disposición adicional decimoséptima, Tratamientos de datos de salud).

7.4.1 DERECHO DE CONFIDENCIALIDAD

En nuestro país, la Ley Reguladora de Investigación Biomédica, también incorpora el derecho de confidencialidad, en su numeral 25, en el que reitera la prohibición a la utilización de datos relativos a la salud para fines distintos a los que se prestó el consentimiento e indica que las personas participantes en una investigación tendrán, salvo excepciones que contemple la ley, derecho a que se guarde confidencialidad sobre:

1. Identidad
2. Información personal
3. Salud
4. Los tratamientos o los resultados de los análisis
5. Procedimientos a los que fueran sometidos.

Al mismo tiempo, obliga a toda persona o entidad que tenga acceso a los datos confidenciales a que deba:

10 En el continente Europeo, en el contexto de la pandemia, el 21 de abril del 2020, el Comité Europeo de Protección de Datos (CEPD), adoptaron las "Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19", con el fin de dar luz sobre las principales dudas que se estaban presentando, al respecto de esta materia, en especial la base jurídica, la aplicación de garantías con respecto al tratamiento de los datos sanitarios y el ejercicio de los derechos de los interesados.

Adoptar las medidas necesarias para asegurar que no se afectará la privacidad, la confidencialidad, integridad y dignidad de los participantes: aunque la ley no lo indica de forma expresa, nos encontramos ante medidas de seguridad de la información, aunque cuando se refiere al término integridad no lo hace refiriéndose a la información, sino a la persona, lo que resulta confuso y pareciera un claro error de la ley. Sobre la seguridad de los datos, la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales indica que

> 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.[11] (Ley № 8968, 2011, artículo 10, párrafo primero).

7.4.2 Deber de confidencialidad

El numeral 25 supra-citado, también impone este deber a cualquier persona que, en el ejercicio de sus funciones, en una investigación donde participen seres humanos, tenga acceso a datos personales o documentos confidenciales relacionados con la investigación, quedará sometida al deber de confidencialidad. De igual manera, como se mencionó anteriormente, la ley № 8968, en su numeral 11, establece que esta obligación no fenece una vez finalizada su relación con la base de datos.

De acuerdo a esta norma, la obligación de confidencialidad no aplica cuando se consignen en el consentimiento informado y sean aceptadas por el participante, siempre y cuando sean las condiciones establecidas por la ley:

a. Cuando lo requiera el comité ético científico que aprobó la investigación.
b. Cuando lo requiera el Consejo Nacional de Investigaciones en Salud, con el fin de cumplir los requerimientos de una inspección y vigilancia de una investigación.
c. Cuando el monitor o el auditor de la investigación requieran verificar datos contenidos en los expedientes clínicos de los participantes de una investigación, para efectos de una auditoría o seguimiento por parte del patrocinador o autoridad reguladora competente.
d. Cuando lo solicite una autoridad judicial competente.
e. Cuando ocurriera una urgencia médica al participante.
f. Cuando el médico responsable de la atención clínica requiera conocer dicha información para efectos de tratamiento de su paciente. (Ley Reguladora de Investigación Biomédica, artículo 25).

7.4.3 Datos seudonimizados

Con la entrada en vigor del Reglamento General de Protección de Datos (RGPD), España promulgó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la cual de manera interesante, declara lícito el uso de datos personales seudonimizados con fines de investigación en salud y biomédica.

> De acuerdo al RGPD, la seudonimización se refiere a el tratamiento de datos personales de manera tal que **ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física**

11 El artículo 10 sobre seguridad de los datos manifiesta: "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 reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos. (Ley Nº 8968, 2011, artículo 10).

identificada o identificable (Reglamento General de Protección de Datos, artículo 4 inciso 5, 2016).

De acuerdo, a la normativa de protección de datos españolas, el uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requiere:

1. Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.
2. Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

- Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
- Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados. (Ley Orgánica 3/2018, 2018, artículo 4, inciso d).

El artículo también indica que cuando se encuentre la existencia de un peligro, real y concreto para la seguridad o salud de una persona -o grupo de personas-, una amenaza grave para sus derechos o para garantizar una adecuada asistencia sanitaria se podría generar una reidentificación de los datos en su origen. En nuestro país, aunque no existe una regulación expresa sobre cómo proceder en estos casos, podríamos concluir que siempre que sea posible la reidentificación[12], el participante de la investigación puede ser individualizado, esto a pesar de que el numeral 27 de la Ley Reguladora de la Investigación Biomédica, con respecto al derecho de información, incluye una limitación en el inciso a), sobre el acceso a los resultados de los análisis de su caso, cuando estos hayan sido sometidos a procesos de disociación o anonimización.

Lo anterior, debido que al mismo tiempo, en el inciso b) le brinda un derecho "a ser informados acerca de los avances, de los eventos adversos inesperados que se presenten y de los resultados generales de la investigación", y en el inciso f) le da el derecho a "a acceder y obtener copia de su expediente personal, en el cual deberá constar toda la información referente a la investigación o ensayo clínico", por lo que no debería darse una interpretación en perjuicio del participante.

7.4.4 La cesión de datos personales

De la misma manera que se regula en el artículo 14 de la ley 8968, para que estos datos puedan ser cedidos o transferidos, se requiere el consentimiento del titular de los datos. En la Ley Reguladora de Investigación Biomédica, en el artículo 26 se establece de la siguiente manera:

La cesión de datos de carácter personal a terceros ajenos a una investigación donde participen seres humanos requerirá el consentimiento expreso y escrito del participante.

Si los datos obtenidos del participante pudieran revelar información de carácter personal de sus familiares, la cesión a terceros requerirá el consentimiento expreso y escrito de todos los interesados. (Ley Reguladora de Investigación Biomédica, artículo 26).

De manera interesante, en la práctica, los datos de índole genético podrían tener dificultad para ser objeto de cesión ya que tienen la posibilidad de revelar información de los familiares y de acuerdo a esta norma se requiere el consentimiento de todos los interesados. Un caso emblemático que ilustra lo anterior, es el de un asesino en serie en Estados Unidos, en donde utilizaron los datos genéticos de un familiar para dar con este:

El 25 de abril de 2018, la policía arrestó al sospechoso Joseph James DeAngelo, de 72 años y expolicía, por seis cargos de asesinato en primer grado –mató en total a 12 personas– ocurridos entre 1979 y 1986 en California. Antes, este asesino en serie, conocido como el Golden State Killer, había violado a 45 mujeres entre 1976 y 1979, en la mayoría de los casos en sus propias casas en presencia de sus maridos, que habían sido maniatados previamente por el criminal.

Después de varias décadas de búsqueda, las autoridades pudieron detenerle gracias al trabajo de los laboratorios de criminalística y a la evidencia genética a través de las

12 Los procesos de anonimización y disociación reducen de forma significativa el riesgo de identificación pero no lo eliminan.

bases de datos de ADN contrastadas con las muestras obtenidas en las escenas de los crímenes. Hasta ahora, se ha utilizado esta técnica forense para resolver 18 casos en EEUU. "Los familiares lejanos pueden ser utilizados para identificar a la persona. No hay ningún criminal que pueda sentirse seguro. Si tienen tu ADN, en algún momento te atraparán", advierte a Sinc el investigador Yaniv Erlich, director científico en la empresa MyHeritage. (Marcos, 2018)

7.5 EL EXPEDIENTE DIGITAL ÚNICO DE SALUD

El Expediente digital Único (EDUS) es el repositorio de los datos [13] del paciente en formato digital, que se almacenan e intercambian de manera segura y puede ser accedido por múltiples usuarios autorizados[14]. Contiene información retrospectiva, concurrente y prospectiva, y su principal propósito es soportar de manera continua, eficiente, con calidad e integralidad la atención de cuidados de salud (Ley No 9162, 2013, artículo 1).

EDUS ha sido de enorme utilidad para el país, no solo porque moderniza los servicios que puede brindar la Caja Costarricense del Seguro Social, sino porque se convierte en una herramienta que permite brindarle a los tomadores de decisión datos estadísticos que pueden ser de gran ayuda para la toma de decisiones y un desarrollo de políticas de salud pública eficaces. La ley Nº 9162 que regula el Expediente Digital Único de Salud (EDUS) se aprobó el 29 de setiembre del 2013, con 11 artículos y un transitorio, lo que representa un marco regulatorio modesto para un proyecto tan ambicioso e importante para el país, que combina tres diferentes campos, como el de salud, la informática y el derecho. Con respecto a la información privada y la protección de la misma, se regula en el numeral 11, que consta de tres párrafos[15], sobre lo siguiente:

1. **Protección de datos personales:** que toda información contenida en el expediente digital único de salud se considera información privada que contiene datos sensibles. Por lo anterior, la misma debe ser tratada como una categoría especial de datos personales, lo cual conlleva una regulación especial de acuerdo con lo contenido en la ley No 8968, que ya han sido abordadas en el presente capítulo.

La norma indica de forma expresa que se prohíbe el tratamiento de dichos datos, lo cual debe interpretarse en concordancia con la ley de protección de la persona frente al tratamiento de sus datos personales y en el sentido de que quiera tratarse más allá de los fines que se han regulado en esta ley que regula EDUS.

En el reglamento de la ley Nº 9162 , al usuario se le reconocen los derechos sobre sus datos de: **acceso, actualización, rectificación y eliminación (artículos 25 y 28).** De la misma manera, en el numeral 48 del reglamento se establece que la base de datos de EDUS deberá ser inscrita ante la Agencia de Protección de datos de los Habitan-

13 En el reglamento, se define por repositorio de datos de la siguiente manera: "Comúnmente llamado almacén de datos describe un destino único utilizado para almacenar datos de forma lógica que facilita la interoperabilidad" (Reglamento del expediente digital único en salud -Nº 8954-, artículo 1, 2018).

14 El reglamento los define de la siguiente manera: Usuario del EDUS: Persona física legitimada en razón de su función, nombramiento y/o relación con la CAJA, se incluye todos aquellos profesionales en salud en calidad de docentes, que esté expresamente autorizada conforme con este Reglamento y regulaciones específicas, para acceder a los datos contenidos en el EDUS e incluir nuevos datos o registros, actualizar, modificar o consultar; según corresponda su función y nivel de acceso asignado al usuario autorizado. Todo usuario del EDUS se encuentra sujeto al deber de confidencialidad. (Reglamento del expediente digital único en salud -Nº 8954-, artículo 1, 2018).

15 El artículo 11, sobre Información privada y su protección, reza de la siguiente manera: Toda información contenida en el expediente digital único de salud se considera información privada que contiene datos sensibles. Se prohíbe el tratamiento de dichos datos y 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.
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. (Ley N° 9162, 2013, artículo 11).

tes (Prodhab), lo cual de acuerdo con los datos públicos del sitio web de la agencia no se está cumpliendo[16].

2. **Sobre la seguridad de la información**: 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[17].
3. **Deber de confidencialidad.** El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional o funcional, aun después de finalizada su relación con la base de datos[18]. El reglamento define al expediente clínico como confidencial, en las siguientes normas:

Artículo 1: Definiciones

"Confidencialidad: Condición inherente a los datos contenidos en el EDUS correspondientes a una persona física identificada o identificable, cuya divulgación no autorizada constituye un delito penado con multa, prisión y/o inhabilitación para el ejercicio de cargos públicos, de conformidad con el artículo 203 y 196 bis del Código Penal." (Reglamento del expediente digital único en salud -№ 8954-, artículo 1, 2018)
Artículo 19: Confidencialidad y secreto profesional

> **La información, datos y en general registros contenidos en los aplicativos del EDUS son confidenciales.** La obligación de observar esta disposición general incluye a los usuarios de EDUS que por motivo de su labor tengan acceso a dicha información, por lo que su violación acarreará las consecuencias disciplinarias y administrativas que correspondan, sin menoscabo de las consecuencias civiles y penales que el ordenamiento jurídico impone. En protección de la confidencialidad, los usuarios autorizados para acceder al contenido de las bases de datos del EDUS se acreditarán **conforme al nivel de acceso asignado que corresponda, según el uso estrictamente** necesario para el adecuado cumplimiento de su función, en concordancia con lo dispuesto en el presente reglamento. El deber de confidencialidad se mantiene aún después de finalizada la relación con el EDUS. El secreto profesional se rige por lo establecido en el artículo 203 del Código Penal. (Reglamento del expediente digital único en salud -№ 8954-, artículo 19, 2018).

La Sala Constitucional ha dejado claro que **no existe duda en cuanto a la confidencialidad del expediente clínico, debido a los datos sensibles y privados que contienen:**

> Congruente con estas consideraciones, en la jurisprudencia constitucional se ha considerado válido impedir el acceso al expediente clínico de la pareja sentimental sin su consentimiento (sentencias número 2001-07783 de las 10:28 horas del 10 de agosto del 2001 y 2005- 04274 de las 18:06 horas del 20 de abril del 2005), y se vedó también a un funcionario de la Caja Costarricense de Seguro Social consultar los datos de pacientes en el marco de una causa disciplinaria (fallo número 2002-10689 de las 18:16 horas del 7 de noviembre del 2002) (Sala Constitucional, 12-007118-0007-CO, 2012).

De la misma manera, la Sala deja claro que el carácter confidencial del documento **no alcanza para impedir al propio paciente interesado su consulta**[19], **ni para ne-**

16 Bajo consulta hecha el día 11 de junio del 2021, en el sitio de Prodhab sobre bases inscritas hasta abril del presente año http://www.prodhab.go.cr/basededatosinscritas/, la CCSS tiene únicamente inscrita la base de datos correspondiente al sistema de recaudación.

17 De acuerdo al reglamento, la seguridad informática le corresponde a la Dirección de Tecnologías de Información y Comunicaciones de la CCSS.

18 Esto en armonía con el deber de confidencialidad contenido en la ley Nº8968 en el numeral 11: La persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podr. ser relevado del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce (Ley Nº8968, 2011, artículo 11)

19 Todo paciente tiene un derecho de acceso a sus datos personales, lo cual está contenido en el marco normativo de EDUS y la Ley de protección de la persona frente al tratamiento de sus datos personales.

gar el expediente médico de pacientes fallecidos a sus familiares[20].

7.5.1 El reglamento del EDUS y sus posibles ilegalidades

A nivel reglamentario la CCSS trató de cubrir todas las lagunas que se encuentran en la ley, por lo que es claro que en algunas normas podrían presentar cuestionamientos en cuanto a su legalidad, como las que se van a desarrollar a continuación.

Transferencia de datos a otras instituciones públicas

El Reglamento del expediente digital único en salud, emitido por la Caja Costarricense del Seguro Social (CCSS), en su numeral 60 habilita la transferencia de datos personales entre instituciones públicas, lo que contraviene la ley Nº 8968 en su numeral 14, que indica que toda transferencia de datos requiere el consentimiento del titular. Por otro lado, como se indicó anteriormente, la información contenida en EDUS es confidencial y corresponde a datos personales sensibles, los cuales son una categoría especial para el tratamiento de datos personales.

El numeral 60 del reglamento reza lo siguiente:

> **Los datos contenidos en el EDUS podrán ser compartidos con instituciones públicas en razón de la naturaleza de la función y mediante la existencia previa de un convenio entre las partes,** con objetivos claros en pro de la salud pública, en salvaguarda de la integridad y confidencialidad de los titulares de la información.
>
> En todos los casos el AES[21], la Dirección Jurídica y el administrador del Sistema de Información del EDUS emitirán criterio a fin de valorar el fundamento técnico y legal que permita la transferencia de datos, definiendo además el formato y la periodicidad con que debe realizarse la misma. En caso de que los criterios, legal y técnico, resulten positivos le corresponde a los responsables de TIC definir los requerimientos informáticos necesarios para hacer efectiva la transferencia de datos, considerando además los aspectos de seguridad informática que resguarde la confidencialidad de los datos individuales y colectivos. (Reglamento del expediente digital único en salud -No 8954-, artículo 61, 2018)

Esta norma sería violatoria del principio de legalidad (Artículo 11 de la Ley General de Administración Pública) y del principio de reserva de ley (artículo 19, LGAPD) con respecto a la transferencia de datos personales sensibles, **sin el consentimiento del paciente**, la cual es una acción que no está expresamente permitida en la ley del Expediente Digital Único en Salud (Nº 9162) y/o la ley de Protección de la persona frente al tratamiento de sus datos personales (Nº 8968) y su ejecución es una limitación a los derechos de los ciudadanos.

Con respecto a la Ley de SINIRUBE[22] (N° 9137), en su artículo 4, sobre las funciones de esta institución indica que podrán

> "conformar una base de datos actualizada y de cobertura nacional de todas las personas que requieran servicios, asistencias, subsidios o auxilios económicos por encontrarse en situaciones de pobreza o necesidad, así como de aquellos beneficiarios que reciban recursos de programas sociales, independientemente de la institución ejecutora que haya asignado el beneficio. En el artículo 3, inciso a), en cuanto a los fines del Sistema Nacional de Información y Registro Único de Beneficiarios de Estado, indica que **mantener una base de datos actualizada y de cobertura nacional con la información de todas las personas que requieran servicios, asistencias, subsidios o auxilios económicos, por encontrarse en situaciones de pobreza o necesidad**.

En respeto del principio de legalidad y el principio de reserva de ley, SINIRUBE no podría extender la cobertura de datos que recopila para abarcar datos relativos

20 Con respecto al acceso de datos personales, el artículo 7 de la ley Nº 8968 indica que el ejercicio de este derecho, en el caso de datos de personas fallecidas, le corresponderá a sus sucesores o herederos.

21 Área Estadística en Salud de la CCSS.

22 Ley Crea Sistema Nacional de Información y Registro Único de Beneficiarios del Estado (SINIRUBE), del mes de abril del año dos mil trece.

a la salud, los cuales son confidenciales y una categoría especial en el tratamiento de los datos, cuyo tratamiento está prohibido, salvo las excepciones contenidas en el numeral 9 de la ley N°8968, mencionadas anteriormente en este capítulo, en las cuales no contemplan los fines de la base de datos de SINIRUBE. Adicionalmente, en el numeral 15 de la ley N° 9137, indica que las instituciones que integran esta institución, como la CCSS, podrán alimentar dicha base de datos "quedando a resguardo aquella información que sea de carácter confidencial", por lo que a todas luces ninguna información del expediente clínico podría transferirse a dicha base de datos.

A pesar de lo anterior, 43 días antes de que la prensa nacional denunciara el Caso UPAD, Casa Presidencial anunció la integración del EDUS y SINIRUBE **como una manera de fortalecer la atención en salud.** De acuerdo a lo que indicaba Casa Presidencial (2020), el intercambio de datos se dará tras un acuerdo firmado este miércoles que se enmarca en la Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0[23], con respecto a lo siguiente:

1. **Esta alianza permitirá cruzar los datos de ambas plataformas y mejorar el enfoque integral en la atención en salud que tome en cuenta aspectos biológicos, psicológicos y sociales de los usuarios:** con respecto a este apartado anunciado por el gobierno, nos encontramos ante datos personales sensibles y confidenciales, los cuales no pueden transferirse a la base de datos de EDUS, ya que, como se indicó supra, esta cumple con fines distintos a los de SINIRUBE y lo mismo aplica a la inversa, por lo que dicha transferencia de datos sería ilegal.
2. **El SINIRUBE tiene los datos de casi 4 millones de personas que son actuales y potenciales personas beneficiarias de los programas sociales del Estado:** de acuerdo con estos datos, el 75% de la población costarricense requieren -o potencialmente podrían necesita- servicios, asistencias, subsidios o auxilios económicos, por encontrarse en situaciones de pobreza o necesidad.

Debido a las dudas que pueden surgir con respecto a este anuncio y sobre qué información relativa a la salud se comparte entre EDUS y SINIRUBE, vale la pena analizar parte de la entrevista que concedió a La Nación el 27 de febrero de 2019, Juan Luis Bermúdez, como presidente ejecutivo del Instituto Mixto de Ayuda Social (IMAS) y ministro de Desarrollo Humano e Inclusión Social, la cual fue titulada "Presidente ejecutivo del IMAS: 'Hoy no podemos decir que no sabemos dónde están los pobres' y realizada por la periodista Irene Vizcaíno. En esta entrevista, el señor Bermúdez nos informa que para ese momento SINIRUBE cuenta con la información de 4,2 millones de personas[24], lo que les permite realizar una política social de precisión. A continuación, se incorporan las transcripciones de las manifestaciones verbales del señor Bermúdez, junto con un sumario análisis de las mismas.

- **Se cruzan datos de planillas y la información de toda la población trabajadora costarricense, a pesar de que no requieran ayudas sociales:**

"Lo cierto es que también recibe información del SICERE, es decir, de todos los reportes de planillas que todos los patronos a lo largo del país brindan mes a mes a la Caja, se recibe información del EDUS, del Expediente Digital Único en Salud que tiene una ficha homologada a la del IMAS, ¿entonces qué nos permite?, La ficha que levanta el asistente técnico de atención primaria cuando va casa por casa, tiene los mismos elementos de la valoración socioeconómica que tiene la ficha del IMAS, entonces al poder cruzar la información de EDUS con la de ingresos nos permite tener la misma información para calificar a población en su condición, ya sea de pobreza extrema, pobreza, o sea de vulnerabilidad o no pobre, eso nos permite , entonces, tener ya una base de datos de ya 4.2 millones de costarricenses, a los cuales podemos calificar hoy, saber, entrar al sistema y ver con su número de cédula, su nombre, qué condición socioeconómica tiene".

23 La cual se ha señalado en este y el capítulo 6 del año anterior, en cuanto no incorpora a la privacidad como un pilar estratégico.

24 Esto representaría un incremento aproximado de doscientas mil personas cuyos datos se contienen en Sinirube, con respecto al anuncio que hizo Casa Presidencial un año después.

- **Con los datos de la administración pública se genera un censo vivo de los costarricenses[25]:**

"Y eso realmente es un gran avance como país, porque nos permite usar registros administrativos casi para crear un censo vivo, que nos permita rápidamente identificar, a diferencia del censo, o de las encuestas de hogares que tenemos año a año esta sí nos permiten identificar dónde está la población en condición de pobreza, quiénes son, cuál es su nombre, cuál es su apellido, cuál es su número de teléfono y poderles llegar, lo cual nos impone a nosotros un gran mandato ético. Hoy no podemos decir que no sabemos dónde están los pobres".

- **Con los resultados de la prueba de embarazo el IMAS puede hacer un estudio socioeconómico para prever si la persona puede necesitar ayuda:**

"Vea qué interesante, hoy podemos con la información del EDUS, poder determinar cuáles van a ser los 70 mil nacimientos que vamos a tener este año, digamos a lo largo del año irlos captando. ¿Cómo se capta? se captan cuando el ATAP[26] llega a una vivienda e identifica a una mujer en condición de embarazo o cuando esa mujer va a consulta externa y se determina con la prueba de sangre que ella está en condición de embarazo. Desde ese momento podemos tener las condiciones socioeconómicas de su hogar, de su vivienda y podemos desde antes que nazca ese niño ir proactivamente y garantizar que si necesita mejoras en la vivienda poderle dar mejoras a la vivienda, que si va a necesitar una opción de cuido, ofrecerle las alternativas que están cerca de su vivienda, de su lugar de residencia, para que tenga una opción de cuido, si hay una atención de violencia atenderla oportunamente y garantizarle a esos 70 mil niños, un poquito menos, que nacen cada año, sesenta y ocho mil, pero garantizarles que van tener un entorno seguro desde que son detectados en el sistema de salud".

Por otro lado, es importante destacar que un año y dos días después de estas declaraciones a La Nación, en el contexto del escándalo UPAD el IMAS aclaró que

> SINIRUBE no contiene datos sobre la condición de salud o enfermedades de las personas, y que la institución no utiliza información de salud o de enfermedades para determinar la condición socioeconómica de las familias, ni para otorgar beneficios de la oferta institucional (Madrigal, 2020).

7.5.2. Transferencia de datos a organizaciones privadas

El Reglamento del Expediente Digital Único en Salud, habilita la transferencia de datos a organizaciones privadas, a pesar de que esto no se encuentra en la ley del "Expediente digital único de salud" (Nº 9162), ya que esta lo que sí permite es que las organizaciones privadas contribuyan con recursos[27].

En el reglamento se indica que solo se podrán transferir datos irrestrictos de acceso general, por lo que es importante subrayar, que la ley en su artículo 11, indica que todo dato contenido en el EDUS, es un dato sensible, por lo que ninguno podría ser de acceso irrestricto. El numeral 61 del reglamento reza de la siguiente manera:

> **La CAJA podrá transferir los datos irrestrictos de acceso general, a organizaciones privadas según lo dispongan leyes especiales, de conformidad con la finalidad para la cual los datos fueron recabados.**
>
> **El acceso a los datos clasificados como sensibles deberá presentase [sic] autorización explícita por parte del usuario titular de la CAJA.**

25 En Alemania, la conocida ley de Censo de la Población de 1983 fue la que generó la resolución histórica sobre la autodeterminación informativa, como puede leerse en el Capítulo 6 de Prosic del año 2020.

26 Asistentes Técnicos de Atención Primaria (ATAP).

27 Así lo indica el artículo, sobre "Responsabilidad social empresarial" el cual reza de la siguiente manera: Las organizaciones del sector privado no gubernamentales y los organismos internacionales, dentro del marco legal respectivo, podrán contribuir con recursos materiales, económicos y humanos en el desarrollo, la implementación y el uso del expediente digital único de salud, bajo un enfoque de responsabilidad social empresarial, orientando sus esfuerzos a la optimización de la calidad de los servicios a los usuarios de salud. La administración de dichos recursos será competencia de la Caja Costarricense de Seguro Social, conforme a lo dispuesto en la presente ley y los controles propios e impropios que al efecto rijan. (Ley del expediente digital único en salud -Nº 9162-, 2013, artículo 9).

> En todos los casos el AES, la Dirección Jurídica y el administrador del Sistema de Información del EDUS emitirán criterio a fin de valorar el fundamento técnico y legal que permita la transferencia de datos, definiendo además el formato y la periodicidad con que debe realizarse la misma. En caso de que los criterios, legal y técnico, resulten positivos le corresponde a los responsables de TIC definir los requerimientos informáticos requeridos para hacer efectiva la transferencia de datos, considerando además los aspectos de seguridad informática que resguarde la confidencialidad de los datos individuales y colectivos. (Reglamento del expediente digital único en salud -No 8954-, 2018, artículo 61).

Sobre este tema es importante destacar que los datos que podrían compartirse son aquellos de carácter estadístico, siempre que no exista posibilidad de identificar al titular de los datos personales. Lo anterior, a pesar de que no es expresamente lo que busca habilitar esta norma reglamentaria, pero que de acuerdo con el artículo 8, inciso d) sobre las excepciones del derecho de autodeterminación informativa podría realizarse.

Por otro lado, según el artículo 9, inciso 3, los datos de acceso irrestricto son solo aquellos que se establezcan por leyes especiales, por lo que en la práctica es poco lo que se puede compartir en respeto de la normativa de protección de datos.

7.6. RIESGOS EN EL TRATAMIENTO AUTOMATIZADO DE INFORMACIÓN PERSONAL DE SALUD

En la actualidad, los datos personales relativos a la salud pueden ser recopilados inclusive sin la autorización del titular, debido al avance tecnológico, lo que potencialmente puede tener un gran valor para sus titulares y/o un enorme riesgo. La obtención, el análisis y/o revelación de estos datos puede ser aprovechado de múltiples maneras y en distintos campos, desde el científico hasta el delictivo. El tratamiento ilegal y/o abusivo de estos datos puede generar una profunda afectación a la intimidad de las personas, con el agravante que con las TIC su impacto puede ser aún mayor[28].

7.6.1 Los riesgos vinculados con la inteligencia artificial

La utilización de algoritmos avanzados y/o sistemas de inteligencia artificial ha aumentado las posibilidades de diagnóstico automatizado de enfermedades y detección de condiciones de salud de las personas, con poca o ninguna acción requerida por parte del usuario lo que conlleva un potencial riesgo y un necesario debate regulatorio al respecto.

¿Qué es la inteligencia artificial (IA)?

La inteligencia artificial es una disciplina que involucra la utilización de algoritmos que tienen la capacidad de adaptar su comportamiento de manera autónoma a través del aprendizaje de experiencias y/o datos. Como lo indica Martínez et lat. (2019), el término de IA se le atribuye al informático norteamericano John McCarthy, quien, en el año de 1956, acuñó el término, haciendo referencia a la conjetura de que algún día se podría proporcionar información tan precisa a mecanismos o dispositivos electrónicos que existiría la posibilidad de emular el pensamiento y libre albedrío humano. De acuerdo con sus capacidades podemos definirla como

> la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear. La IA permite que los sistemas tecnológicos perciban su entorno, se relacionen con él, resuelvan problemas y actúen con un fin específico (Parlamento Europeo, 2020).

Según Chacón et al. (2015), hay dos enfoques de la IA:

Enfoque científico: utiliza el computador como medio de simulación en la búsqueda para entender y modelar las capacidades de procesamiento de información de la mente humana, comprender los principios generales

28 Su almacenamiento en la nube ha generado que por descuidos de los responsables de las bases de datos y/o por la acción de delincuentes organizados los datos se encuentren sin ninguna protección en internet, generando un grave daño al titular de los datos.

para explicar y modelar sistemas inteligentes, sean humanos, animales o artificiales.

Enfoque de ingeniería: que busca dotar al computador de capacidades que se atribuyen a la inteligencia humana, como por ejemplo la percepción, el razonamiento y la toma de decisiones, así como diseñar máquinas novedosas capaces de realizar cosas que previamente eran hechas solo por humanos o animales, o que inclusive realicen tareas que van más allá de la inteligencia humana.

Como lo indica Microsoft (2018), la investigación en inteligencia artificial no es reciente ya que inició en la década de los 50, continuando el trabajo llevado a cabo por el matemático británico Alan Turing durante la Segunda Guerra Mundial. Sin embargo, no ha sido hasta la última década cuando se han producido los avances más rápidos, como consecuencia de la combinación de tres factores cruciales: computación en la nube, la gran cantidad de datos y los grandes avances en aprendizaje automático. De la misma manera, en los últimos años se han presentado grandes avances de esta disciplina en el campo de salud, lo que requiere un análisis en cuanto a sus oportunidades y sus riesgos.

7.6.2 IA en el campo de la salud

La inteligencia de las máquinas puede transformar nuestra sociedad con grandes avances en el combate de las enfermedades, el aumento en la calidad de vida y la longevidad. Como lo indican Martínez et la (2019) la IA utilizada en el sector salud, con respecto a su aplicación es la que tiene una mayor proporción en cuanto al uso y expectativas que se tienen sobre la misma, entre las que detallan:

> **Asistente robótico para cirugías:** este asistente da la posibilidad al profesional médico de realizar operaciones sin la necesidad de que doctor y paciente se encuentren en el mismo espacio geográfico.
>
> **Las enfermeras virtuales:** son aplicaciones de IA que asisten al paciente en cualquier momento que este desee, mediante una aplicación que puede descargarse de internet hacia un dispositivo móvil.
>
> **La enfermera virtual:** puede hacer seguimiento diario de los valores y mediciones que el paciente mismo puede realizarse desde su casa.

A su vez, en el campo de diagnóstico, la IA se dirige a superar la capacidad humana, con una gran habilidad para detectar patrones en formas que resultan imposibles para un cerebro biológico. Lo anterior, debido al poder computacional, su capacidad de aprendizaje, la posibilidad de recopilación de una ingente cantidad de información personal y un almacenamiento casi ilimitado.

Sin duda los sistemas informáticos inteligentes pueden servir un noble fin de alto interés público, pero como todo tipo de tecnología puede ser abusada con fines distintos para el que fueron creados, por lo que es necesario un marco normativo robusto que permita su adecuado desarrollo. Por esto y con el fin de comprender los alcances que pueden tener estas tecnologías vamos a revisar diferentes desarrollos que se están dando a nivel mundial.

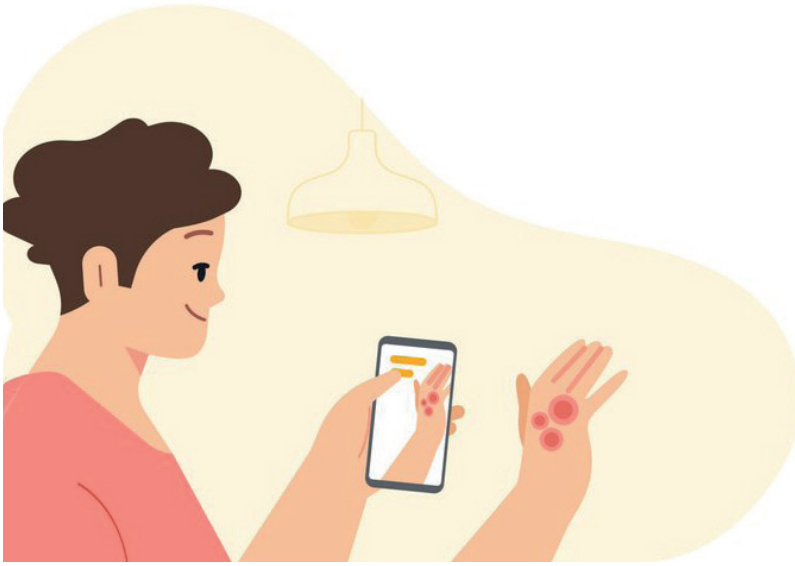

Figura 7.2. Uso de la inteligencia artificial para encontrar respuestas a afecciones cutáneas comunes

Fuente: Tomado de https://blog.google/technology/health/ai-dermatology-preview-io-2021

El primer ejemplo positivo es la nueva tecnología de Google, la cual permite detectar enfermedades cutáneas a través de una aplicación en un dispositivo móvil:

> El equipo de Google presentó una nueva herramienta impulsada por IA que permitirá que los usuarios realicen consultas sobre posibles afecciones de la piel. Solo bastará que el usuario suba unas fotografías tomadas con su móvil y responda

> un cuestionario para que la IA le muestre una serie de resultados. (Schuager, 2021).

Una vez que este tipo de sistemas se perfeccionen, pueden aumentar la esperanza de vida al adelantar los tiempos de detección de enfermedades cutáneas, que más que servir como reemplazo del médico, propicia que las personas se pongan en contacto con un profesional en salud lo más pronto posible.

De manera similar, un científico de la Universidad de Hong Kong desarrolló un método que escanea las retinas de niños de seis años y que utiliza el aprendizaje automático y la inteligencia artificial para detectar autismo o el riesgo del mismo:

> Utiliza una cámara de alta resolución con un nuevo software informático que analiza una combinación de factores, incluidas las capas de fibras y los vasos sanguíneos del ojo… Saber cómo detectar el autismo lo antes posible para iniciar un tratamiento adecuado es clave para conseguir los mejores resultados en el desarrollo de un niño (Castillo, 2021).

En los dos casos anteriores, resulta evidente el beneficio para la población, aunque puede generar preocupación los fines que se persigan en la recopilación, por lo que este avance tecnológico requiere una importante conciencia de la población en cuanto a la privacidad para propiciar cambios regulatorios importantes a nivel global. En esa misma línea, se mencionó en el Capítulo 6 sobre "*Retos regulatorios en la protección de datos personales en Costa Rica*", del Informe Hacia la Sociedad de la Información y el Conocimiento 2020, sobre la Estrategia Nacional de Transformación digital de nuestro país, que busca propiciar cambios en las normativas de privacidad para aprovechar las tecnologías digitales disruptivas al mismo tiempo que no incorpora a la privacidad como un pilar estratégico:

> Sobre esta base, el diseño y accionar 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. (Medrano, 2020).

Conforme los científicos comiencen a aprender a utilizar la IA en el combate de pandemias, debemos estar preparados al momento en donde se proponga ceder libertades en favor del uso de estas tecnologías ya que para evitar abusos es importante ser conscientes sobre los riesgos y los beneficios de la tecnología, así como las consecuencias de ir reduciendo el marco de protección de la privacidad. En un futuro no tan lejano, las máquinas podrán saber si una persona tiene una enfermedad tan solo con escucharla hablar, por lo que se debe pensar bien el marco regulatorio para estas tecnologías. Este año, los científicos ya han logrado resultados en la detección de Covid-19 a partir del análisis de la voz humana:

> Sobre su efectividad en los resultados durante el pasado mes de febrero se ha llevado un estudio de investigación en Mumbai, India, con 2.000 personas, a las que se les instaron instalar su herramienta VocalisCheck en sus respectivos móviles, concluyendo que su algoritmo **tenía una precisión de un 81,2% en la detección de la Covid-19,** donde muchos de los pacientes eran asintomáticos, y por tanto, indetectables por otros métodos. (Hidalgo, 2021, párr. 7).

El aporte que traerá la IA en el combate de enfermedades complejas todavía se escapa de nuestra comprensión, por lo que también es cierto que se debe tener cuidado con buscar regulación que pueda detener la innovación. Las buenas noticias es que los médicos han empezado a ser superados por las máquinas en la detención del cáncer de mama:

> El uso de inteligencia artificial puede ser más preciso que los médicos para diagnosticar el cáncer de mamas a partir del estudio de imágenes de rayos X, según indica una investigación publicada en la revista Nature. Un equipo internacional, que incluye investigadores de Google Health y del Imperial College de Londres, diseñó un sistema informático de inteligencia artificial (AI, por sus siglas en inglés) con el uso de mamografías realizadas a casi 29.000 personas.
>
> El algoritmo fue capaz de ofrecer mejores resultados en la lectura de las imágenes que médicos

> radiólogos, al encontrar casos de cáncer que los expertos no habían detectado y, al mismo tiempo, ignorar "falsos positivos", en los cuales los médicos habían dado erradamente la alerta por la presencia de posibles tumores. (BBC, 2020).

Una tecnología similar se ha utilizado para detectar el cáncer de próstata, en donde este sistema de inteligencia artificial busca irregularidades que son características de esta enfermedad:

> La herramienta mejoró con cada escaneo, refinando sus habilidades y adaptándose para analizar escaneos de diferentes máquinas, eventualmente detectando las características más pequeñas de la enfermedad. Con el tiempo, pudo superar a los radiólogos y detectar crecimientos cancerosos en segundos, incluso antes de que los pacientes presentaran algún síntoma.
>
> El objetivo es entrenar al sistema para que vea lo que el ojo humano no puede, con el objetivo de detectar el cáncer de próstata mediante la detección incidental. Una vez identificado el problema, los profesionales pueden comprobarlo y actuar.
>
> Aprovechando la capacidad de escanear rápidamente imágenes médicas y detectar signos de enfermedades de manera mucho más eficiente que los humanos, un grupo de científicos en Australia ahora han adaptado esta tecnología para la detección temprana del cáncer de próstata, siendo capaces de detectar crecimientos cancerosos en segundos. (Polo, 2021)

Asimismo, la detección temprana del Parkinson se está buscando acelerar por medio de la utilización de IA:

> Un simple examen ocular, combinado con una poderosa tecnología de aprendizaje automático de inteligencia artificial (IA), podría proporcionar una detección temprana de la enfermedad de Parkinson, según una investigación presentada en la reunión anual de la Sociedad Radiológica de América del Norte (RSNA). Usando imágenes de la parte posterior del ojo de pacientes con enfermedad de Parkinson y participantes de control, entrenaron a la SVM para detectar signos sugestivos de enfermedad en la imagen ocular.
>
> Los resultados indicaron que las redes de aprendizaje automático pueden clasificar la enfermedad de Parkinson según la vascularización de la retina, y las características clave son los vasos sanguíneos más pequeños. Los métodos propuestos apoyan aún más la idea de que los cambios en la fisiología del cerebro se pueden observar en el ojo. (Fernández, 2020).

La IA también podría usarse en favor de la salud mental, como lo es el caso de un sistema inteligente solo requiere analizar la voz de la persona para determinar si tiene depresión:

> Inventan una aplicación que, según la forma de hablar, podría detectar cuando un paciente tenga una depresión severa.
>
> Explican que un sistema de inversión del habla es capaz de mapear las señales acústicas con las variables de la pista vocal, mostrando la sincronización y el movimiento espacial de los gestos del habla. Afirman que la coordinación en el habla cambia cuando una persona está deprimida. Si la aplicación detecta que la gravedad de la depresión está aumentando, se informará mediante una notificación urgente al médico. (Hernandez, 2021)

El consentimiento libre en el tratamiento de nuestros datos con fines de diagnóstico es esencial, salvo excepciones que pueden establecerse por ley, ya que de lo contrario se podría utilizar para fines de vigilancia y usos no éticos de toda índole.

Otro de los grandes retos a los que nos enfrentamos con la IA es el que tiene que ver con los sesgos inherentes a estas tecnologías, que pueden presentarse cuando las máquinas son entrenadas con datos de ciertos grupos de población y/o los atributos que se eligen para tomar decisiones son los que lo generan. En este sentido en MIT Technology Review lo explican muy bien que los sesgos se pueden presentar en:

> **Recogida de los datos.** Los datos producen sesgos principalmente por dos vías: o los datos recopilados no son representativos de la realidad o reflejan prejuicios ya existentes. El primer caso podría ocurrir, por ejemplo, si un algoritmo de aprendizaje profundo recibe más fotos de las caras de piel clara que las de piel oscura. El sistema de recono-

cimiento facial, como consecuencia de eso, sería inevitablemente peor en el reconocimiento de las caras de piel más oscura.

Preparación de los datos. Finalmente, es posible introducir sesgos durante la etapa de preparación de datos a la hora de seleccionar los atributos que deseamos que el algoritmo tenga en cuenta. (No debe confundirse con la etapa de la definición del problema. Es posible usar los mismos atributos para entrenar un modelo para objetivos muy diferentes o usar atributos muy distintos para entrenar un modelo para el mismo objetivo) (Hao, 2019, párr. 5 y 6).

Como puede verse, los beneficios de la IA pueden superar los riesgos, siempre y cuando y de manera informada podamos generar política pública y regulación que permita enfrentar este reto de una manera adecuada.

7.7. RIESGOS Y AMENAZAS A LA PRIVACIDAD EN TIEMPOS DE PANDEMIA COVID-19

La pandemia generó un enfoque global por temas de salud en donde ha sido necesario limitad ciertas libertades individuales con el fin de salvar vidas y poder combatir de manera eficiente el Covid-19. Como lo reseñaba la BBC al inicio de la pandemia, que la misma podría utilizarse para fortalecer los autoritarismos y debilitar las democracias, desde la utilización de militares en países con ejercito, la concentración del poder en el Ejecutivo, el uso de tecnología en detrimento de la privacidad, entre otros que destacan:

> El coronavirus parece hecho a medida para los gobiernos y políticos autoritarios que han proliferado en los últimos años. Mientras varios de ellos no creyeron inicialmente en su gravedad, ahora les podría servir para recortar libertades democráticas, dar renovados papeles a los militares, cerrar las fronteras a la migración y exaltar el nacionalismo frente a la cooperación entre países.
>
> Una forma posible de recortar libertades que alarma a expertos y organizaciones de derechos humanos es a través de la tecnología. China, Corea del Sur e Israel están tratando de controlar la crisis actual obteniendo información de los teléfonos móviles de los ciudadanos. Cuando el propietario de un móvil da positivo por covid-19, el Estado accede a un registro de sus movimientos más recientes. Se identifica a los usuarios de otros teléfonos que hayan estado cerca de la persona infectada y se les avisa que están en riesgo. (Aguirre, 2020).

Nuestro país no fue ajeno a este tipo de discusión y se estuvo analizando la posibilidad de utilizar el Expediente Digital Único de Salud de la CCSS para realizar la función de rastreo de contactos, lo que resultaría en un sistema centralizado que podía captar más datos de los ciudadanos, lo que hubiese sido contraproducente[29].

El tratamiento de la información personal relativa a la salud también empezó a realizarse en irrespeto de la legislación vigente, con la publicación de información que pueden que hacen identificable a personas se contagiaron de Covid-19, tanto en medios sociales, medios de comunicación formales y hasta en bases de datos gubernamentales. Los protocolos de salud y las iniciativas del comercio resultaron en una reducción de la privacidad, volviéndose común el tener que tolerar que tomarse la temperatura antes de ingresar a ciertos lugares.

7.7.1 Publicación de datos "anonimizados" de pacientes Covid-19 con fines de análisis

El 9 de setiembre del 2020, el Ministerio de Salud anunció que publicaría una base de datos anonimizadas de todas las personas que han resultado positivas por COVID-19 desde el 6 de marzo al 5 de julio[30]. De acuerdo a la información oficial, la base contiene información de cada paciente (Ministerio de Salud, 2020):

29 En ese sentido, en un reportaje en La Nación que se llamó "Costa Rica desaprovecha rastreo con celulares para combatir covid-19" se analizaba la posibilidad de utilizar EDUS para esa función.Se indicaba que por temas legales no se había empezado a utilizar dicha tecnología. El reportaje puede encontrarse en https://www.nacion.com/el-pais/salud/costa-rica-desaprovecha-rastreo-con-celulares-para/5L27V3PYZJGQRFRC347ZJPEQVU/story/

30 De acuerdo con el sitio oficial esta base de datos se actualizará cada dos meses en el link http://geovision.uned.ac.cr/oges/evolucioncovid.html .

- Edad
- Sexo
- Nacional o extranjero
- Condición migratoria
- Fechas de confirmación del virus
- Distrito, cantón y provincia donde se ubica
- Factores de riesgo que presenta
- Si requirió hospitalización
- Fecha de recuperación
- Tipo de contagio
- Caso autóctono o importado
- Nexos por grupo de contagio

Adicionalmente, verificando el documento que contiene la base de datos, también se incorporan los siguientes datos:

- El número de caso
- Fecha de publicación
- Semana epidemiológica
- Región del Ministerio de Salud
- País visitado
- Calificación final (autóctono, importado)
- Estado (Hospitalizado, fallecido, recuperado, fecha de recuperación)
- Código de asociación.
- Tipo de nexo

A pesar de que el Ministerio de Salud exprese que la información se encuentra anonimizada y por ende no se puede identificar a una persona, lo cierto es que se ha publicado, con acceso global, la suficiente información por cada persona que aumentaría los riesgos de reidentificación. Estos pueden eliminarse o reducirse con un proceso de anonimización de los datos personales y de esta manera evitar que las personas sufran actos discriminatorios, contra su honor y/o dignidad como seres humanos.

El anonimizar los datos no significa que los datos dejarán de ser veraces o útiles, ya que lo que comprende es aplicarle un proceso que permite su utilización, al mismo tiempo que protege la privacidad del usuario.

El Ministerio de Salud debió hacer un análisis del riesgo de la identificabilidad de las personas, basado en la razonabilidad en la disponibilidad de los medios para lograr este fin y la proporcionalidad de los esfuerzos para poder identificar directa o indirectamente a la persona, ya sea por parte del responsable o cualquier otra persona. En ese sentido y como lo indica la Agencia Española de Protección de Datos, el proceso de anonimización debe cumplir los siguientes principios:

1. **Principio proactivo.** La protección de la privacidad es el primer objetivo de la anonimización y su gestión debe realizarse de forma proactiva y no reactiva.
2. **Principio de privacidad por defecto**. El primer requisito conceptual en el diseño de un sistema de información será garantizar la confidencialidad de los interesados. Por lo tanto, conviene que desde el inicio se salvaguarde la privacidad teniendo en cuenta la granularidad o grado de detalle final que deben tener los datos anonimizados.
3. **Principio de privacidad objetiva**. Como resultado de la Evaluación de impacto de Protección de datos (EIPD) existirá un umbral de riesgo o índice de riesgo residual de reidentificación. Este índice de riesgo será asumido por el responsable del tratamiento como riesgo aceptable y será tenido en consideración para el diseño del proceso de anonimización.
4. **Principio de plena funcionalidad.** Desde el inicio del diseño del sistema de información se tendrá en cuenta la utilidad final de los datos anonimizados, garantizando en la medida de lo posible la inexistencia de distorsión con relación a los datos no anonimizados. (Agencia Española de Datos, 2016, pp. 3 y 4)
5. **Principio de privacidad en el ciclo de vida de la información**. Las medidas que garantizan la privacidad de los interesados son aplicables durante el ciclo completo de la vida de la información partiendo de la información sin anonimizar.
6. **Principio de información y formación.** Una de las claves para garantizar la privacidad de los

> interesados es la formación e información que se facilite al personal involucrado en el proceso de anonimización y en la explotación de la información anonimizada. obligaciones.

El no haber realizado este proceso, eleva el riesgo, ya que la información por su estructura informática y el ser de carácter público, le permite a cualquier persona utilizarla con fines distintos para los que fueron publicados. Por ejemplo, en un futuro una aseguradora u otra empresa podrían usarla para crear algoritmos que, en conjunto con otra información adicional, le permitan determinar la posibilidad de que una persona haya tenido Covid-19 con las posibles secuelas que esto conlleva, de acuerdo a la gravedad de la enfermedad, que es un dato que también se encuentra en dicha base de datos. Lo anterior es preocupante debido a que se ha reportado que el Covid-19 deja secuelas en las personas[31], las cuales pueden ser más graves en los casos donde las personas han sido hospitalizadas, que como se indicó es información que está disponible para cualquiera.

Al mismo tiempo, cualquier información que permita la identificación de las personas requiere que se cumpla los requisitos de ley para que sean de acceso irrestricto, lo que en este caso sería a través de una ley de la República[32].

Por otro lado, la Sala Constitucional, en julio de 2021, obliga al Instituto Tecnológico Costarricense a entregar una base de datos personales anonimizada de sus estudiantes, para fines de minería de datos, con excepción de los datos personales sensibles:

> Se declara con lugar el recurso. Se ordena a G.R.R[33], en su condición de director del Departamento de Admisión y Registro del Instituto Tecnológico de Costa Rica, o a quien ocupe tal cargo, que coordine lo necesario, gire las órdenes pertinentes y lleve a cabo todas las actuaciones que estén dentro del ámbito de sus competencias para que, dentro del plazo de UN MES, contado a partir de la notificación de esta sentencia, **ponga a disposición del amparado la información solicitada** mediante las gestiones planteadas el 13 de mayo de 2021 y así se lo comunique al medio señalado para tales efectos. **Lo anterior salvaguardando los datos sensibles o confidenciales,** en caso de haberlos, de conformidad con la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (ley n.° 8968). (Sala Constitucional, Resolución Nº 16570 – 2021)

Es importante subrayar que la Sala Constitucional no define qué se puede entender datos anonimizados y tampoco define qué es un dato personal sensible, por lo que solo se refiere a que de existir esos datos, debe resguardarlos. En el caso en estudio, nos encontramos ante datos personales sensibles, al ser relativos a la salud y en el caso del TEC, el solicitante pide información sensible, como lo es la condición de si el estudiante optó por una beca y si la aceptó[34].

7.7.2 Aplicaciones de notificación de Exposición al Covid-19

Un país que quiera utilizar una aplicación de rastreo de contactos o notificación de exposición de Covid-19 puede elegir entre dos sistemas:

1. **Centralizado**: es aquel donde las autoridades tienen el control de la información personal y les permite saber, de alguna forma, quiénes han tenido interacciones de riesgo para así comunicarles qué acciones tomar. Como lo indica EFF (2020) el servidor central normalmente puede saber qué dispositivos han estado en contacto con los dispositivos de las personas infectadas, y puede ser capaz de vincular esos dispositivos a identidades del mundo real.

31 En este sentido, se indica en "un estudio liderado por la Universidad Rey Juan Carlos y que ha contado con la participación de la Universidad Complutense (ambas en Madrid), ha analizado los síntomas persistentes y secuelas en pacientes hospitalizados por coronavirus durante la primera ola de la pandemia. Al año de haber recibido el alta el 61,2% continuaba padeciendo fatiga. Además de esta, se ha registrado la presencia de otros síntomas respiratorios persistentes: el 2,5% continúa padeciendo tos, el 6,5% presenta dolores torácicos y el 23,3%, disnea. (Consalud.es, 2021).

32 Ver el artículo 3, inciso c) de la Ley Nº8968, on respecto a la definición de datos personales de acceso irrestricto.

33 Por no resultar relevante para el análisis académico la inclusión del nombre solo se utilizaron las iniciales del funcionario.

34 Los datos personales de carácter socioeconómico son datos personales sensibles de acuerdo al artículo 3 inciso e) de la Ley Nº8968.

2. **Descentralizado**: Lleva un rastreo de contactos de forma anónima y le da el control al ciudadano sobre las comunicaciones que podría tener con las autoridades. Este sistema ofrece mayores garantías de privacidad a los ciudadanos porque no suben los datos personales de sus contactos con un servidor central para que las autoridades puedan comunicarse con estos, sino que todo el intercambio se realiza de manera anónima.

A nivel mundial se han implementado programas de rastreo de contacto tecnológico que han resultado violatorios de la privacidad de las personas, lo cual en el largo plazo puede inclusive erosionar la democracia de un país. En ese sentido, un polémico programa israelí fue detenido por la Corte, debido a que recurrió al espionaje:

> La tecnología secreta de rastreo de móviles que utiliza el espionaje israelí va a ser utilizada para supervisar los movimientos de las personas infectadas por el coronavirus. El Gobierno del primer ministro en funciones Benjamín Netanyahu ha aprobado en la madrugada de este martes un decreto por la vía de urgencia que autoriza al Shin Bet, la agencia de espionaje interior, a hacer un seguimiento sin autorización judicial de los pacientes con Covid-19.
>
> Israel informó que utilizaba tecnología de espionaje telefónico de Shin Bet para identificar a personas expuestas al coronavirus al rastrear los movimientos de pacientes infectados. Posteriormente se les ordenaba a todos aquellos que entraron en contacto con los enfermos a confinarse en cuarentena dentro de sus hogares. (Sanz, 2020).

Según ha reportado Amnistía Internacional (2020) los países Bahréin, Kuwait y Noruega han implementado algunas de las aplicaciones de rastreo de contactos contra la COVID-19 más invasivas del mundo, porque las tres realizan rastreos directos o casi directos de ubicaciones de usuarios, subiendo las coordinadas GPS a un servidor central a intervalos frecuentes, rastreando los movimientos de los usuarios en tiempo real. Adicionalmente, "las autoridades de todos estos países pueden vincular fácilmente esta información personal sensible con una persona, pues Qatar, Bahréin y Kuwait exigen a los usuarios registrase con un número de documento nacional de identidad, mientras que Noruega impone el registro con un número de teléfono válido".(Amnistía Internacional, 2020)

En ese sentido, debido a una advertencia del organismo nacional de protección de datos, el gobierno Noruego se vio obligado a suspender la aplicación centralizada en junio del 2020, debido a una advertencia de la autoridad nacional de protección de datos:

> El lunes 15 de junio de 2020 la suspensión de su aplicación de rastreo de la covid-19 tras una advertencia del organismo nacional de protección de datos, el Datatilsyn, que considera que la herramienta invade demasiado la privacidad. En una carta del viernes, el Datatilsyn emitió un preaviso de "prohibición temporal", dejando al instituto sin la posibilidad de tratar los datos personales recogidos gracias a Smittestopp. El organismo indicó que ante la limitada propagación de la epidemia en Noruega, así como la limitada efectividad de la aplicación debido al bajo número de personas que realmente la usan, la invasión de la privacidad que resulta de su uso era desproporcionada. (Agencia AFP, 2020).

Sin embargo, como lo reportó Reuters (2020), en setiembre el país escandinavo anunció que utilizaría el sistema descentralizado de Apple y Google, el cual es más respetuoso de la privacidad, lo que no dejó de destacar el ministro de salud haciendo énfasis en que "Esta aplicación es puramente para rastrear infecciones, no almacena datos de forma centralizada".

7.7.2. La aplicación de notificación de exposición en Costa Rica

En Costa Rica, la aplicación de rastreo de personas infectadas por Covid-19 se bautizó como **Mascarilla Digital**. Este se basa en un sistema descentralizado, que utiliza la tecnología de Apple y Google, y que además cuenta con privacidad por diseño. Esta app funciona utilizando la tecnología de bluetooth, lo que permite que dos personas que tienen la app instalada intercambien códigos generados aleatoriamente que sirven como prueba de interacción. El sistema se basa en el consentimiento del usuario y aunque venga pre-instalado el usuario debe habilitarlo para que inicie su funcionamiento.

El sistema funciona con base en el consentimiento y la privacidad:

1. **El sistema trata con datos anónimos que intercambia entre personas que han habilitado el sistema:** esto permite que solo las personas que han decidido participar intercambien códigos anónimos.
2. **El Ministerio de Salud no puede saber quiénes han recibido una notificación de riesgo, por lo que el aviso únicamente le sirve al individuo para medir el riesgo al que se ha enfrentado.**

En el caso de la persona que ha resultado infectada, de acuerdo a la información oficial, recibirá un mensaje de texto con un código que deberá ingresar en la aplicación para que active la función de compartir las claves anónimas generadas por el dispositivo, para que otros puedan cotejar si las han recibido, lo cual es una alarma que se ha tenido un contacto de alto riesgo.

7.7.3 Controversia por supuesta instalación sin el consentimiento del usuario

Muchos usuarios de teléfonos Android denunciaron que se les instaló una aplicación del Ministerio de Salud sin su consentimiento, la cual estaba vinculada con un sistema de notificación de exposición, en apariencia gubernamental. Con tantos precedentes de violación a la privacidad, es entendible que muchas personas se alarmaran con la instalación de una aplicación la cual no contaba con su autorización.

El problema se presentó solo en algunos dispositivos Android, a quienes les aparecía el ícono de la aplicación, aunque el sistema no iniciara hasta que el usuario se diera de alta. Este error fue reportado días después en Massachusetts en donde también varios usuarios de Android presentaron el mismo error[35], lo que evidencia que nos encontramos ante un fallo informático de índole global, el cual solo afectó a ciertos dispositivos.

Sobre el respeto de la privacidad y ciberseguridad, es importante aclarar que para que el sistema de Mascarilla Digital pudiese usar el API de Apple y Google debió cumplir criterios básicos sobre privacidad, seguridad y control de los datos, porque es un sistema creado para proteger a los ciudadanos de sus gobiernos, por lo que no se permite que estos tengan acceso a más datos de los necesarios[36]. En este sentido esta aplicación no puede obtener la ubicación del usuario u otra información personal, a diferencia de otras aplicaciones que usamos todos los días, las cuales en caso de vulnerabilidades conllevan riesgos mayores

7.7.4 Toma de temperatura en lugares públicos

En nuestro país, la toma de la temperatura, antes de ingresar a ciertos comercios, se ha convertido en una práctica común, a pesar de que no ha sido incluida dentro de los lineamientos generales. Aún así, se ha implementado sin mayor fricción e inclusive la Agencia de Protección de los Datos de los Habitantes (Prodhab) no se ha pronunciado en cuanto esta práctica.

En el continente europeo, la Agencia Española de Protección de Datos (2020), ha mostrado su preocupación por esta práctica, la cual recomienda se realice en concordancia con los lineamientos de las autoridades sanitarias y dentro de su pronunciamiento destacamos lo siguiente:

1. **Nos encontramos ante un tratamiento de datos personales sensibles:** Este tratamiento de toma de temperatura supone una injerencia particularmente intensa en los derechos de las personas afectadas. Por una parte, porque afecta a datos relativos a la salud de las personas, no sólo porque el valor de la temperatura corporal es un dato de salud en sí mismo sino también porque, a partir de él, se asume que una persona padece o no una concreta enfermedad, como es en estos casos la infección por coronavirus.

35 The Verge reportó esta situación en Massachusetts' "COVID-19 exposure notification app auto-installed on Android phones" https://www.theverge.com/2021/6/21/22543486/massnotify-covid-exposure-android-google-apple

36 Al respecto puede verse el principio de minimización de datos regulado en el continente europeo. En la RGPD en su numeral 5, indica que los dantos deben ser: "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".

Por otro lado, los controles de temperatura se van a llevar a cabo con frecuencia en espacios públicos**, de forma que una eventual denegación de acceso a un centro educativo, laboral o comercial estaría desvelando a terceros que no tienen ninguna justificación para conocerlo que la persona afectada tiene una temperatura por encima de lo que se considere no relevante** y, sobre todo[37], que puede haber sido contagiada por el virus.

2. **Sobre los criterios de implementación**. La aplicación de estas medidas y el correspondiente tratamiento de datos requeriría la determinación previa que haga la autoridad sanitaria competente. Continúa la agencia indicando que debe tenerse en cuenta, que según las informaciones proporcionadas por las autoridades sanitarias, hay un porcentaje de personas contagiadas asintomáticas que no presenta fiebre, que la fiebre no siempre es uno de los síntomas presentes en pacientes sintomáticos, en particular en los primeros estadios del desarrollo de la enfermedad, y que, por otro lado, puede haber personas que presenten elevadas temperaturas por causas ajenas al coronavirus. (Agencia Española de Protección de Datos, 2020)

En el caso de Argentina, la autoridad nacional indica que esta toma puede tener un impacto en la privacidad, por lo que ha publicado una guía en la cual indica que es una actividad permitida. Se indica que independientemente de si la empresa u organización registra el dato o pide identificación es un tratamiento de datos personales, por lo que debe cumplir la normativa de protección de datos personales [38] .

En nuestro país, el tratamiento de datos personales relativos a la salud, de acuerdo a la ley № 8968 es necesario que quien realiza la captura de este dato sea una persona cuyo oficio se relacione con el área de la salud y/o cuente con el secreto profesional o funcional[39].

El Ministerio de Salud no ha incluido esta práctica de forma general en sus lineamientos[40], pero sí dentro de algunos de actividades específicas, como es el caso de eventos futbolísticos internacionales[41] en el marco de la alerta por COVID-19, en donde se indica lo siguiente:

> En cada puerta de acceso al estadio se garantizará un puesto de control en donde se le tome la temperatura corporal a todas las personas que ingresan al recinto. Se recomienda que sea en la frente entre las cejas. La temperatura debe tomarse con un termómetro infrarrojo. Toda persona con medición de temperatura igual o mayor a 37.5°c, deberá de ser verificado mediante 2 tomas más, esperando un tiempo de 5min entre cada (Ministerio de Salud, 2021, p.6).

Tomando en cuenta que para los principales servicios que los costarricenses utilizan, no hay un lineamiento por parte del Ministerio de Salud para que se tome la temperatura, nos encontramos ante una situación en donde la práctica parece dirigida a transmitir confianza sobre las medidas para la lucha contra el Covid-19. En este sentido, Agencia Española de Protección de Datos, indica lo siguiente:

> La cámara térmica y la recogida del dato solo puede entenderse como parte de un tratamiento mayor, **y no se puede tomar un dato de salud de una per-**

37 El subrayado no pertenece al original.

38 Puede verificarse en https://www.argentina.gob.ar/noticias/datos-personales-y-registro-de-temperatura .

39 Sobre las excepciones a la prohibición de tratamiento de datos personales ver la ley Nº 8968 en su artículo 9.1 d) que reza de la siguiente manera: "El tratamiento de los datos resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, **siempre que dicho tratamiento de datos sea realizado por un funcionario o funcionaria del área de la salud, sujeto al secreto profesional o propio de su función, o por otra persona sujeta, asimismo, a una obligación equivalente de secreto.**

40 Sobre esto puede verse "Lineamientos generales para oficinas con atención al público (Bancos, correos, instituciones del Estado, Poder Judicial, empresas privadas de servicios) debido a la alerta sanitaria por Coronavirus (COVID-19)".

41 Así puede verse en la segunda versión del "Lineamiento general para la realización de eventos futbolísticos internacionales en el marco de la alerta por COVID-19" (LS-VS-009).

sona y tratarlo espontáneamente por cualquier gestor de un lugar público simplemente porque crea que es lo mejor para sus clientes o usuarios.

La agencia española en análisis sobre el uso de las tecnologías en la lucha contra la pandemia también mostró su preocupación ya que en estas situaciones "tendremos un riesgo de discriminación, estigmatización y tal vez difusión pública de datos de salud" (Agencia Española de Protección de Datos, 2020).

Con respecto a la cámara térmica, el Ministerio de Salud, en el caso de los protocolos para la operación paulatina del Aeropuerto Internacional Daniel Oduber Quirós sobre las cámaras térmicas ha indicado lo siguiente:

> En los procesos de salida y llegada internacional de pasajeros y dado el alto flujo de personas, la concesionaria Coriport realizará mediciones de temperatura corporal con cámara térmica sin contacto a la totalidad de los pasajeros. En caso de que se detecte temperaturas corporales iguales o por encima de 38°C, se procederá con una valoración secundaria de salud por parte de un personal en salud. En el caso del proceso de salidas internacionales, a partir del resultado de la valoración secundaria el personal en salud determinará si el pasajero puede continuar con el viaje o no, y se informará a la Línea Aérea. El personal en salud completará el registro de todo pasajero que pase a esta valoración secundaria (Ministerio de Salud, 2020 pp 10- 11) [42].

Con respecto a las cámaras térmicas que utilizan inteligencia artificial para identificar un rostro humano, al mismo tiempo que le mide su temperatura, con ningún tipo de acción requerida por parte de este. De acuerdo con nuestra legislación, este tipo de cámaras sí presentaría un problema legal, ya que para la captura de un dato personal de salud sin el consentimiento del titular se requiere que la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento[43].

7.7.5. Pasaporte Covid-19

En la Unión Europea, el 1 de julio de 2021 entró en vigor el certificado digital COVID, el cual acredita a la persona cumple con alguna de las siguientes condiciones:

1. Ha sido vacunada contra la COVID-19.
2. Se ha realizado una prueba cuyo resultado ha sido negativo.
3. Se ha recuperado de COVID-19.

De acuerdo a la Comisión Europea (2021), este certificado es gratuito, cuenta con un código QR, que es válido en todos los países de la UE y se destaca las siguientes características:

1. **Formato digital o en papel**: Las autoridades nacionales son las encargadas de su expedición y no es exclusivo de un soporte específico. El mismo se encuentra en la lengua nacional y en el idioma inglés.
2. **Es seguro y fiable:** El Certificado COVID Digital de la UE contiene un código QR con una firma digital para protegerlo contra la falsificación. Cada centro emisor tiene su propia clave de firma digital (esta información se almacena en una base de datos segura en cada país). Cuando se comprueba el certificado, se escanea el código QR y se verifica la firma. La Comisión Europea (CE) ha creado un portal a través del cual puedan verificarse las firmas de los certificados en toda la UE.

42 El Ministerio de salud también en esos casos indicó lo siguiente: La tecnología para la toma de temperatura de pasajeros internacionales (salida o llegada) por su alto flujo, debe cumplir con los siguientes criterios técnicos mínimos:

• Ser portátil para su desplazamiento oportuno a los sitios requeridos.

• Medición de temperatura que evite el contacto directo con el viajero.

• Resultados instantáneos que permitan mantener adecuado flujo de viajeros para evitar aglomeraciones.

• Permitir mediciones de temperatura de manera simultánea.

• Mediciones con bajo margen de error no superior a +/- 0,3 grados Celsius (Ministerio de Salud, 2020 p. 11).

43 En ese sentido ver el artículo 9.1 inciso a) de la ley Nº 8968.

3. **Los datos personales del titular del certificado no tendrán que transmitirse a través del portal, ya que no es necesario para verificar la firma digital.**

El Certificado COVID Digital de la UE contiene únicamente la información clave necesaria, como el nombre, la fecha de nacimiento, la fecha de expedición, la información pertinente sobre la condición que busca certificarse (la vacuna, la prueba o la recuperación) así como un identificador único. Estos datos permanecen en el certificado y no se almacenan ni conservan cuando se verifica un certificado en otro Estado miembro.

¿En qué casos puede requerirse el Certificado COVID Digital de la UE? El certificado traerá beneficios a las personas totalmente vacunadas ya que pueden quedar exentas de las pruebas relacionadas con los viajes o de la cuarentena (14 días después de la última dosis). En la práctica funciona como un documento fiable a través del cual la persona puede probar que cumple con alguna de las condiciones que se certifican en dicho documento.

En el continente europeo, cada país tiene sus propias medidas sanitarias y este certificado lo empiezan a requerir principalmente para ingresar a lugares cerrados. En el caso francés, a través de una ley que ha dividido al país, el parlamento aprobó restricciones sanitarias, que afectarían sobre todo a quienes no cuentan con un Certificado COVID. Como lo reporta France24 (2021), desde el 21 de julio del 2021 lo empezaron a utilizar para ir a cines, museos o lugares deportivos, como consecuencia de un aumento del 140% de contagios en una semana.

En Costa Rica, para que se pueda implementar el Certificado Covid-19 para ingresar a comercios o instituciones públicas, es necesario hacerlo por medio de una ley, debido a lo siguiente:

1. **Entrega y posible almacenamiento de datos personales relativos a la salud:** Nuestra normativa de protección de datos personales, indica que ninguna persona estará obligada a suministrar datos personales sensibles, como los relativos a la salud. En el caso, del Certificado Covid-19, la condición de vacunado o no es un dato relativo a la salud, por lo que en caso de que se requiera para el ingreso a determinados lugares, no solo se estaría obligando a las personas a suministrarlos, sino que en los casos de reservaciones en línea podría conllevar la necesidad de almacenamiento de estos datos, con su respectivos riesgos.

2. **Derecho de admisión en comercios abiertos al público**: La Sala Constitucional ha sostenido que este derecho no es antijurídico cuando se ejerce racionalmente, sin discriminaciones contrarias a la dignidad humana pero que "cuando sirvan de pretexto para realizar, mediante subterfugios diferenciaciones antijurídicas, la discriminación deviene en antijurídica, por estar motivadas en criterios de raza, color, linaje u origen nacional o étnico u otras razones contrarias a la dignidad humana"(Sala Constitucional, Res. Nº 06686 - 2001). Si bien es cierto se podría considerar racional requerir esta información por temas de salud pública, la orden sanitaria no puede ir contra la ley, en cuanto a lo expresado en el apartado anterior y a su vez conlleva una limitación a derechos fundamentales con respecto a la libertad de tránsito, autodeterminación informativa, no discriminación, entre otros que por el principio de reserva de ley podría establecerse únicamente por medio de ley.

7.7.6 PASE DE SALUD DE COSTA RICA

En nuestro país se está implementando un Pase de Salud como requisito de ingreso a territorio nacional y en el cual las personas llenan un formulario en línea a través del cual se le genera un Código QR, cuyo color se generará con base al análisis informático de la información presentada.

Para generarlo, a la persona se le preguntan los siguientes datos:

Tabla 7.1. Información solicitada para la elaboración del Pase de Salud

Datos para la identificación del pasajero	Sobre el viaje
Nacionalidad	Vía de transporte (Aire, mar o tierra)
Cédula, Dimex o Pasaporte	Número de vuelo de llegada a Costa Rica
Nombre y apellidos.	Aeropuerto (SJO, LIR, SYQ)
Sexo (Masculino, Femenino, Prefiero no revelar)	Número de asiento.
Fecha de nacimiento	País de procedencia
Correo electrónico	Fecha de salida del país de procedencia
Teléfono.	Fecha de llegada a Costa Rica
Profesión u oficio.	Países visitados en los últimos 14 días.
Dirección exacta (Provincia, Cantón, Distrito, Otras señas)	Nombre de los acompañantes que viajan con usted

Fuente: Elaboración propia con base a https://salud.go.cr/

Adicionalmente se le hacen las siguientes preguntas de salud:

Tabla 7.2. Preguntas sobre la condición de salud realizadas por el Pase de Salud

Indique si presenta alguno de los siguientes síntomas	Indique si ha estado en alguna de las siguientes situaciones	Se ha aplicado alguna vacuna contra covid-19. (Sí, no)
Fiebre, tos, dificultad para respirar, dolor de garganta, pérdida de olfato, pérdida del gusto, diarrea, ninguno de los anteriores	Contacto cercano con algún paciente diagnosticado con Covid-19, permanecido como paciente en algún centro sanitario en los últimos catorce días en los que se hayan notificado personas enfermas de Covid-19, ninguna de las anteriores	País de aplicación de la vacuna Tipo de vacuna (Pfizer & BioNTech, Moderna, AstraZeneca, Covaxin, Johnson & Johnson/ Janssen Pharmaceuticals, Sinopharm / BIBP1, Sinovac, Sputnik V, Otro) Número de dosis aplicadas. Fecha que se aplicó la vacuna. Subir comprobante de vacunación.

Fuente: Elaboración propia con base a https://salud.go.cr/

Como lo indicaron las autoridades a crhoy.com, el proceso es el siguiente.

> Una vez que la persona llena el formulario en línea debe adjuntar los requisitos sanitarios de ingreso, los cuales, serán validados por el Ministerio de Salud y el Instituto Costarricense de Turismo (ICT) según sus competencias.
>
> Dichos códigos serán de un color particular, que le indicarán al oficial de Migración su condición:
>
> Si es verde significa que no tiene problemas de ingreso y puede continuar con sus trámites.
>
> Si es verde con una línea amarilla quiere decir que puede ingresar al paíspero debe hacer cuarentena.
>
> Si su código QR es morado, el sistema detectó alguna anomalía con su seguro médico).
>
> Si es naranja, tiene problemas de restricción según su país de procedencia
>
> Finalmente, si es rojo, el sistema detecto que tiene problemas con la prueba PCR o presenta riesgo de contagio de COVID-19. (Crhoy.com, 2021).

7.7.7. Legalidad del Pase de Salud

El formato digital estaría validado por el principio de equivalencia funcional contenido en la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, la cual establece en su numeral 3:

> Artículo 3º-Reconocimiento de la equivalencia funcional. Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.
>
> En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. No obstante, el empleo del soporte electrónico para un documento determinado no dispensa, en ningún caso, el cumplimiento de los requisitos y las formalidades que la ley exija para cada acto o negocio jurídico en particular. (Ley Nº 8454, 2005, artículo 3).

La Ley General de Salud, obliga a toda persona a mostrar los certificados de vacunación a la autoridad sanitaria:

> Artículo 152.- Toda persona está obligada a mostrar los certificados de vacunación y de salud de conformidad con los reglamentos respectivos y, en todo caso, **cuando la autoridad sanitaria así lo requiera.**
>
> Ninguna autoridad podrá retener los certificados válidos de vacunación de una persona. (Ley General de Salud, 1973, artículo 152).

Adicionalmente, de acuerdo al artículo 173, de la Ley General de Salud, al ingresar al país, toda persona está obligada a demostrar que cuenta con las vacunas obligatorias, lo que faculta a las autoridades migratorias para requerir esta información personal relativa a la salud.

Según el sitio web del Pase de Salud, el responsable de esta base de datos es el Ministerio de Salud y la finalidad para la que son recolectados los datos es prevenir el contagio de COVID-19 y la asistencia humanitaria. Por ello, este Ministerio es el encargado de cumplir todas las obligaciones contenidas en la normativa nacional de protección de datos personales, en especial lo que tiene que ver con la seguridad de la información contenida en este.

7.7.8. Reforma a la Ley General de Salud en la pandemia

El artículo 160 de la Ley General de Salud fue reformada a través de la ley № 9845, el 30 de abril del 2020, en la pandemia lo que supone algunas obligaciones a los costarricenses vinculadas con el campo tecnológico y de protección de los datos personales:

> **Deber de informar a la autoridad de salud sobre las personas que haya estado en contacto directo o indirecto:** todo paciente de enfermedad transmisible de denuncia obligatoria tiene la obligación de informar a las autoridades los datos de identificación de una persona con la que haya

tenido contacto de forma directa o indirecta, así como una forma de contacto, como el teléfono y correo electrónico.

La persona cuyo caso sea sospechoso o confirmado de un caso de enfermedad transmisible de denuncia obligatoria deberá señalar al médico tratante una dirección de correo electrónico para recibir notificaciones. La notificación que se realice a dicho medio tendrá el efecto de notificación personal.

Una vez constatada la información de contacto brindada por la persona sobre terceras personas con quienes haya entrado en contacto, y tras obtener el consentimiento informado de dichas terceras personas, el Ministerio de Salud podrá utilizarlos como medio de notificación. (Artículo 160, párrafo tercero y quinto, Ley General de Salud).

Transferencia de datos personales entre médico tratante y autoridad de salud: Ante una situación de sospecha o confirmación de un caso de enfermedad transmisible de denuncia obligatoria, el médico tratante deberá ordenar las medidas necesarias para evitar la propagación de la enfermedad, de acuerdo con las normas fijadas por las autoridades sanitarias.

Al mismo tiempo, el médico o la institución para la que este trabaje, que funge como el responsable de la base de datos personales, está obligado a transferirle al Ministerio de Salud la información personal de carácter sensible que ha sido recabada en un plazo de 24 horas y le traslada a este el deber de confidencialidad de la información personal objeto del tratamiento. (Ver el artículo 160, párrafo cuarto de la Ley General de Salud).

La ley №968 obliga a todo responsable de la base de datos personales a requerir el consentimiento del titular del derecho para realizar una transferencia de datos personales o contar con un mandato legal que así lo permita, como en el presente caso.

7.7.9. Riesgos informáticos y Cibercrimen en tiempos de pandemia

El campo de la ciberseguridad está estrictamente ligado con el de la ciberdelincuencia, en el sentido que los delincuentes informáticos se alimentan de los errores de las personas y empresas en la primera en su favor. Los ciberdelincuentes son resilientes porque su campo de batalla cambia día a día, ya que constantemente se reparan errores informáticos y se capacita a las personas con respecto a distintas amenazas.

De acuerdo al Consejo de Europa (2020) al inicio de la pandemia ya había evidencia que los delincuentes se habían adaptado y estaban aprovechando el contexto para las siguientes acciones:

- Campañas de phishing y distribución de malware a través de sitios web o documentos aparentemente genuinos que brindan información o consejos sobre COVID-19, están siendo utilizados para infectar computadoras y extraer credenciales de usuario.
- Se usa ransomware que deja fuera de servicio instalaciones médicas, científicas u otras instalaciones relacionadas con la salud con el fin de obtener un rescate.
- Ataques contra infraestructuras críticas u organismos internacionales, como la Organización Mundial de la Salud.
- Ransomware dirigido a teléfonos móviles de personas que utilizan aplicaciones que engañan al usuario afirmando proporcionar información genuina sobre COVID-19 para conseguir pagos.
- Delincuentes atacan a empleados en teletrabajo.
- Esquemas de fraude vinculados con productos de la salud.
- La desinformación distribuida por cuentas sociales falsas y medios de comunicación fraudulentos que difunden información errónea o noticias falsas para crear pánico, inestabilidad social y desconfianza en los gobiernos o en las medidas adoptadas por sus autoridades sanitarias.

El reporte del Consejo de Europa que se daba a finales de marzo del 2020 nos debe dejar clara la rapidez con la que se adaptan los delincuentes a las nuevas situaciones y oportunidades que se les presentan. De acuerdo a Coalition (2020) el ransomware ha sido de los ataques más utilizados con la pandemia ya que solo en los primeros seis meses del 2020, los ataques de ransomware aumen-

taron en un 260% y el monto del rescate aumentó en un 47%[44].

La pandemia ha traído un incremento en la violación de los datos personales, en particular, ha aumentado el impacto sobre los datos relativos a la salud. Una investigación reciente, publicada en julio de 2020 por *Digital Shadows*, estima que hay más de 15 mil millones de registros robados de más de 100.000 filtraciones de datos actualmente disponibles para la venta en la darkweb, de toda clase de datos. (Segu-info, 2020). Asimismo, según un informe de IBM Security, el secuestro de los datos se duplicó en la pandemia:

> Los resultados muestran que en 2020, los agentes de amenazas cibernéticas se centraron en organizaciones vitales para los esfuerzos globales de respuesta a Covid-19, como hospitales, fabricantes de insumos médicos y farmacéuticos, así como compañías de energía que alimentan la cadena de suministro de Covid-19.
>
> Según el nuevo informe, los ataques cibernéticos a organizaciones de atención médica, fabricación y energía se duplicaron con respecto al año anterior, ya que los agentes de amenazas cibernéticas hicieron blanco en organizaciones que no podían permitirse el tiempo de inactividad debido a los riesgos de interrumpir los esfuerzos médicos o cadenas de suministro críticas. (La Tercera, 2021).

Los datos médicos también se encuentran a la venta en internet, lo que representa una fuente de ingresos para los ciberdelincuentes quienes se van a ver cada vez más interesados en datos que les pueden generar ganancias:

> han surgido nuevos tipos de datos. Este el caso de los historiales médicos personales y los selfis con documentos de identificación personal, que pueden encontrarse con un precio de hasta 40 dólares.
>
> Los datos vendidos en el mercado negro pueden ser utilizados para la extorsión, la ejecución de estafas y esquemas de 'phishing' y el robo directo de dinero. (20 minutos, 2020).

Los datos relativos a la salud, en muchos casos, se encuentran alojados en sistemas informáticos que no se encuentran debidamente actualizados o no cuentan con las medidas de seguridad pertinentes, lo que genera una gran vulnerabilidad para los datos. A nivel nacional, La Nación reportó que el Hospital de Niños perdió una cantidad importante de datos de carácter médico, sin que existiera indicación si fue un ataque informático o la causa, ya que lo que se reportó es que se tenía información en servidores a los cuales no se les daba mantenimiento y ni siquiera pueden cuantificar a cuántos datos ascienden las pérdidas:

> La Dirección Médica del Hospital alegó el 6 de julio anterior que el problema respondía a una falla en un disco duro. Incluso, aseguró que recuperaría los datos en tres semanas. Sin embargo, el 15 de julio cambió el discurso y reconoció que no dispone de respaldos de las imágenes y que es probable que no se rescaten nunca.
>
> En los últimos seis años, la Auditoría Interna de la Caja Costarricense de Seguro Social (CCSS) advirtió, en al menos dos ocasiones, del riesgo de extraviar datos de los menores debido a deficiencias en la administración de tecnologías de información y comunicación. (Bosque, 2021).

El caso nacional no es aislado, ya que a nivel global se dan casos similares. En esa línea, una empresa de seguridad reportó que datos médicos se encontraban disponibles en internet:

> Ha sido la empresa de ciberseguridad CybelAngel la que ha levantado el problema, **exponiendo como los datos médicos expuestos se filtraron desde hospitales y centros médicos de todo el mundo.** Tal y como se encontró la información, personas externas podían acceder fácilmente a datos médicos confidenciales.
>
> El problema en este tema es que los dispositivos médicos suelen ser vulnerables a los ciberataques o a la exposición de datos, porque la tecnología a menudo está desactualizada y los presupuestos de seguridad y TI de la atención médica están sobrecargados. (Polo, 2020)

La conciencia sobre la importancia de la Ciberseguridad debe realizarse tanto en el sector público como en el privado, ya que los delincuentes explotan los errores que cometen los usuarios y los que se encuentran en las tecnologías.

44 Así lo reporta ZDNET, que recoge un reporte de la empresa Coalition https://www.zdnet.com/article/ransomware-accounts-to-41-of-all-cyber-insurance-claims/

CONSIDERACIONES FINALES

La pandemia Covid-19 ha aumentado el tratamiento de datos personales relativos de la salud de los costarricenses, debido a acciones relacionadas con la atención de la enfermedad, actualización de los datos de usuarios de EDUS y la vacunación masiva para combatir la enfermedad. Los datos personales relativos a la salud pertenecen a una categoría especial de dato personal, el cual cuenta con una regulación mucho más estricta en cuanto a su tratamiento, debido a que una acción sobre este puede generar una afectación de una intensidad superior sobre la dignidad del ser humano, al poder propiciar tratos discriminatorios.

En la presente investigación nos hemos encontrado violaciones a la privacidad de los habitantes de la República, las cuales, aunque en apariencia se realicen en buena fe y con las mejores intenciones, siguen siendo ilegales y lesivas de derechos fundamentales, por lo que el país debe avanzar hacia un debate regulatorio sobre esta materia. Una adecuada política pública sobre la informática y la protección de los datos personales se encuentra estrictamente relacionada con el éxito que podamos tener en el desarrollo como país, ya que ninguna actividad económica puede ser ajena a la tecnología en estos días y/o al tratamiento de datos personales.

Para el avance en temas de ciencia y la tecnología se requiere de un marco normativo robusto que promueva un uso ético e impida abusos, al mismo tiempo que habilite la creatividad, la innovación y el desarrollo económico en la ruta de una nación más próspera. Lo anterior, es especialmente relevante en temas como:

1. **El análisis de grandes volúmenes de datos (Big Data):** para una mejor toma de decisiones de política pública y de índole empresarial.
2. **Inteligencia artificial:** la cual inclusive puede llegar a detectar información sensible, como enfermedades, sin mayor interacción por parte del usuario, lo que conlleva oportunidades y riesgos.
3. **Investigación biomédica:** un campo en el que se requiere que exista armonía con las leyes de protección de datos personales y regulación especial que permita el desarrollo científico.
4. **Expediente médico:** tanto a nivel privado, como público se debe contar una regulación especial que regule de forma específica y clara esta materia.

En línea de lo anterior, la creación de toda política pública relacionada con esta materia, se debe establecer la privacidad y otros derechos digitales como un pilar estratégico que debe priorizarse, con el fin de tomar las mejores decisiones para la colectividad, sin que esto represente la erosión de la democracia y libertades individuales que son el fundamento de esta. En esta línea, España en el año 2018 promulgó una Ley Orgánica de Protección de datos personales con el fin de adaptar la normativa española al Reglamento General de Protección de Datos (RGPD) de la Unión Europea, al mismo tiempo que incluía diversos derechos digitales de alta relevancia para la sociedad española. Al mismo tiempo, como parte de la Agenda España Digital 2025, que busca la transformación digital de dicho país, se publicó en julio de 2021 la Carta de Derechos Digitales, cuyo respeto se debe garantizar como parte de los ejes estratégicos.

Nuestro país debe seguir el ejemplo español, con el fin de que el desarrollo científico y tecnológico no representen retrocesos en derechos humanos y el de promover la confianza en la tecnología y la ciencia, que sin lugar a duda deben tener una posición privilegiada en la vida de las personas. Para poder dirigirnos a este camino, es importante que la educación superior se dirija al fomento de más carreras STEM y derecho informático, con el fin de crear profesionales con competencias para prosperar en la cuarta revolución industrial y que puedan participar de los debates regulatorios tan necesarios para crear de manera multidisciplinaria la normativa más robusta y adaptada a las necesidades del país.

La educación del país sobre ciberseguridad y privacidad desde edades tempranas y para todos los sectores de la población es necesaria para reducir los riesgos informáticos relacionados con las acciones que se encuentran en el poder de los ciudadanos y para generar apoyo hacia una Costa Rica que busque el respeto de los derechos en entornos digitales.

Reformas legales necesarias

El país debe iniciar la discusión de distintas reformas que busquen fortalecer el marco normativo relacionado con TIC, con especial atención a los relacionados con temas

relativos a la salud. De acuerdo con lo que hemos analizado en la presente investigación se propone el avance en las siguientes reformas:

1. **Compartición de datos para estudios epidemiológicos en respeto de la privacidad del ciudadano:** el futuro de la lucha de las enfermedades implica en gran medida, la utilización de la tecnología para analizar ingentes cantidades de datos, los cuales a su vez representan un profundo riesgo en la privacidad del ciudadano, por lo que se debe avanzar en una regulación que lleve el balance aceptable para la sociedad. Una regulación clara, promueve la investigación, la inversión y la innovación, al mismo tiempo que eleva la confianza de las personas en este tipo de herramientas.
2. **Tratamientos de datos personales para el combate de pandemias:** se debe crear una regulación especial que permita crear una política pública moderna en el uso de la tecnología para combatir pandemias, utilizando los derechos digitales como pilares, con el fin de reducir el impacto en la economía y al mismo tiempo promoviendo la innovación. En un futuro, no se debería perder tiempo para discutir sobre temas como la notificación de exposición, Certificado Covid, uso de inteligencia artificial para medición de distanciamiento social o aforo en lugares públicos y la publicación de datos abiertos para analizar el avance de una enfermedad desde una perspectiva colectiva, entre otros.
3. **Reglas más robustas para las transferencias de datos personales relacionados con personas infectadas con una enfermedad transmisible de denuncia obligatoria:** Los médicos tratantes, privados o públicos, tienen permitido comunicarle la información de personas infectadas con este tipo de enfermedades al Ministerio de Salud, sin embargo, la ley debe establecer más reglas desde la perspectiva de la privacidad y la ciberseguridad.
4. **Política pública sobre TIC:** para brindar mayor seguridad jurídica a la ciudadanía en cuanto a la creación de política pública relacionada con la tecnología, se debe establecer por ley que todo proyecto, aplicación y/o política pública relacionada con el uso de las TIC debe tener como pilar el respeto de los derechos digitales reconocidos en nuestro ordenamiento jurídico, como la privacidad, el secreto de las comunicaciones y documentos privados, autodeterminación informativa, derecho de acceso universal a internet, entre otros.
5. **Derechos digitales:** el avance de la pandemia en la utilización de tecnología por parte de la población en su vida diaria también conlleva una responsabilidad para los gobernantes para que se aseguren que en el desarrollo de la vida personal o laboral de toda persona pueda defenderse ante las injusticias que pueden afectarle en su dignidad como ser humano y ver a su vez restringidas sus libertades individuales. Al igual que en España, se debe incluir dentro de la futura reforma integral a la ley de protección de datos personales nacional e inclusive abordar temas tan innovadores como los presentados en su Carta de Derechos Digitales, sobre la propuesta de regulación de la implantación y empleo en las personas de las neurotecnologías.
6. **Regulación sobre inteligencia artificial:** el país debe aprender de los debates y propuestas regulatorias que se están teniendo en el continente europeo en esta materia. Una propuesta de regulación de la I.A, toma como base el riesgo de ciertas tecnologías para así definir las reglas que se le aplicarán, evitando al mismo tiempo que se convierta la normativa en un obstáculo para la innovación.
7. **Expediente digital único de Salud (EDUS):** se debe crear una reforma a la ley de tal forma que el derecho a la seguridad digital, autodeterminación informativa, confidencialidad, con respecto a la información personal de los ciudadanos se encuentra en los sistemas informáticos de la CCSS tenga mayores garantías.

El futuro de nuestro país depende del avance en la educación, cultura digital, regulación de la informática y la ciencia, por los que se deben hacer esfuerzos más grandes por promover la discusión y la investigación multidisciplinaria en estas materias si queremos estar listos para los retos del futuro.

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

Agencia Española de Protección de Datos. (30 de abril del 2020) Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos. Recuperado de https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos

Agencia, (6 de abril del 2021). Atención turista: Así funciona el Código QR que es requisito para ingresar al país Recuperado de https://www.crhoy.com/nacionales/atencion-turista-asi-funciona-el-codigo-qr-que-es-requisito-para-ingresar-al-pais/

Agencia Española de Protección de datos Personales (2016). Orientaciones y garantías en los procedimientos de anonimización e los datos personales.

Agencia AFP (15 de junio de 2020). Noruega suspende aplicación de rastreo de covid-19 tras preocupaciones por privacidad de los usuarios. Recuperado de https://www.elcomercio.com/actualidad/mundo/noruega-privacidad-aplicacion-rastreo-coronavirus.html

Aguirre, M. (8 abril de 2020). Coronavirus: por qué la pandemia de covid-19 podría fortalecer los autoritarismos y debilitar las democracias. Recuperado de https://www.bbc.com/mundo/noticias-internacional-52184947

Aministía Internacional (16 de junio de 2020). Las aplicaciones de rastreo de contactos de Bahréin, Kuwait y Noruega, entre las más peligrosas para la privacidad. Recuperado de https://www.amnesty.org/es/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

BBC News Mundo. (2 de enero del 2021). Cómo la inteligencia artificial "supera a médicos" en el diagnóstico de cáncer de mama. Recuperado de https://www.bbc.com/mundo/noticias-50969239

Bosque, D. (20 de julio de 2021). Hospital de Niños desoyó desde 2015 alertas sobre pérdida de datos. Recuperado de https://www.nacion.com/el-pais/salud/hospital-de-ninos-desoyo-desde-2015-alertas-sobre/M5DDZIY6YRCTVF2DEJRGY43VEU/story/

Casa Presidencial (9 de enero de 2020). Integración de edus y SINIRUBEfortalecerá atención en salud Recuperado el 1 de julio del 2021 de https://www.presidencia.go.cr/comunicados/2020/01/integracion-de-edus-y-sinirube-fortalecera-atencion-en-salud/

Castillo, A. (18 de marzo del 2021). Desarrollan una tecnología de escaneo de retina para identificar autismo en los niños Recuperado el 09 de mayo del 2021 de https://www.20minutos.es/noticia/4621909/0/desarrollan-una-tecnologia-de-escaneo-de-retina-para-identificar-autismo-en-los-ninos/

Chacón et al. (2015). La Inteligencia Artificial y sus Contribuciones a la Física Médica y la Bioingeniería. Revista Mundo FESC, Edición N° 9.

Consejo de Europa (27 de marzo del 2020). Cybercrime and Covid-19 Recuperado el 31 de julio del 2021 de https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19.

Constitución Política de Costa Rica, Asamblea Nacional Constituyente, 1949.

ConSalud.es (4 de julio del 2021) Secuelas respiratorias persistentes tras superar la Covid-19, una preocupante realidad. Recuperado de https://www.consalud.es/pacientes/especial-coronavirus/secuelas-respiratorias-persistentes-superar-covid-19-preocupante-realidad_99165_102.html

Comisión Europea (9 de marzo de 2021). Certificado COVID Digital de la UE. Recuperado de https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_es

Cyphers y Gebhart (12 de mayo de 2020) Los gobiernos no deben usar la tecnología "centralizada" de seguimiento de la proximidad. Recuperado de https://www.eff.org/es/deeplinks/2020/05/governments-shouldnt-use-centralized-proximity-tracking-technology

Encuentro Anual de autoridad de Protección de Datos Personales, Boletín informativo, diciembre del 2018. Recuperado de http://www.oas.org/es/sla/ddi/boletines_informativos_DDI_protec-

cion_datos_personales_Encuentro_Anual_Costa_Rica_2018_Diciembre-2018.html

Fernandez, J. (24 de noviembre 2020). Examen ocular con IA para diagnóstico temprano de Parkinson. Recuperado de https://biotechmagazineandnews.com/examen-ocular-con-ia-para-diagnostico-temprano-de-parkinson/

Hao, K (8 de febrero de 2019). Cómo se produce el sesgo algorítmico y por qué es tan difícil detenerlo. Recuperado de https://www.technologyreview.es/s/10924/como-se-produce-el-sesgo-algoritmico-y-por-que-es-tan-dificil-detenerlo

Hernandez (14 de junio de 2021). Desarrollan una app capaz de detectar síntomas de depresión solo con la voz. Recuperado de https://computerhoy.com/noticias/tecnologia/desarrollan-app-capaz-detectar-sintomas-depresion-solo-voz-882609

Hidalgo, F. (2 de abril del 2021) Una IA entrenada para detectar la covid-19 desde muestras de voz. Recuperado de https://wwwhatsnew.com/2021/04/02/una-ia-entrenada-para-detectar-la-covid-19-desde-muestras-de-voz

Ley № 8968. "Ley de Protección de la Persona frente al Tratamiento de sus datos personales. Diario Oficial La Gaceta, San José, Costa Rica, 5 de setiembre de 2011.

Ley N° 9137. "Crea Sistema Nacional de Información y Registro Único de Beneficiarios del Estado (SINIRUBE)", Diario Oficial La Gaceta, San José, Costa Rica, 5 de setiembre de 2013.

Ley N° 6227. "Ley General de Administración Pública". **Colección de leyes y decretos, de 1978, primer Semestre, tomo 4, página 1403.**

Ley N° 9234. "Ley Reguladora de Investigación Biomédica. Diario Oficial La Gaceta, San José, Costa Rica, 25 de abril de 2014.

Ley N° 9162. "Expediente digital único de salud". Diario Oficial La Gaceta, San José, Costa Rica, 23 de setiembre de 2013

La Tercera (2021). "Secuestro de datos" se duplicaron en pandemia según informe de ciberataques a industrias, Recuperado el 24 de febrero del 2021 de https://www.latercera.com/que-pasa/noticia/secuestro-de-datos-se-duplicaron-en-pandemia-segun-informe-de-ciberataques-a-industrias/6RYTYHJCH5B-T7O6Z6LRLBD5SA4/

La Nación. (30 de julio del 1998). Ley limita divulgar datos privados. Periódico La Nación. Recuperado de https://www.nacion.com/el-pais/ley-limita-divulgar-datos-privados/HHJCTQDIWNEV-3GAKTQLCGR7GSU/story/

Madrigal, L. (29 de febrero de 2020) IMAS desmiente de nuevo a Defensoría: datos de salud no se usan para fijar condición socioeconómica. Recuperado de https://delfino.cr/2020/02/imas-desmiente-otra-vez-a-la-defensoria-informacion-medica-no-se-usa-para-fijar-condicion-socioeconomica

Martinez et la. (2019). Avances de la inteligencia artificial en salud. Revista científica Dominio de las Ciencias.

Marcos, A. (11 de octubre del 2018). Los test genéticos de tus familiares te pueden delatar. Recuperado de https://www.agenciasinc.es/Noticias/Los-test-geneticos-de-tus-familiares-te-pueden-delatar

Medrano, J (2020). Retos regulatorios en la protección de datos personales en Costa Rica. En: Informe Hacia la Sociedad de la Información y el Conocimiento 2020. Programa Sociedad de la Información y el Conocimiento.

Ministerio de Salud. (2021). LS-VS-009. Lineamiento general para la realización de eventos futbolísticos internacionales en el marco de la alerta por COVID-19.

Ministerio de Salud (2020). MRLB-02. Protocolos para la operación paulatina del Aeropuerto Internacional Daniel Oduber Quirós durante la pandemia por COVID-19 posterior a la apertura de fronteras, Costa Rica.

Ministerio de Salud de Costa Rica (2020). Ministerio de Salud publica base anonimizada de positivos COVID-19. Recuperado de https://www.ministeriodesalud.go.cr/index.php/centro-de-prensa/noticias/741-noticias-2020/1875-ministerio-de-salud-publica-base-anonimizada-de-positivos-covid-19

Murillo, A. (2010). Las duras (y valiosas) lecciones de la epidemia que golpeó a Costa Rica hace 100 años. Recuperado de https://semanariouniversidad.com/pais/las-duras-y-valiosas-lecciones-de-la-epidemia-que-golpeo-a-costa-rica-hace-100-anos/ Polo, J. (16 de diciembre del 2020). Hospitales hackeados muestran exámenes de pacientes en internet. Recuperado de https://wwwhatsnew.com/2020/12/16/hospitales-hackeados-muestran-examenes-de-pacientes-en-internet/

Parlamento Europeo. (8 de setiembre de 2020). ¿Qué es la inteligencia artificial y cómo se usa? Recuperado de https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa

Segu-info (10 de setiembre de 2020). Estado de la exposición de la industria de la ciberseguridad en la Dark Web. Recuperado de https://blog.segu-info.com.ar/2020/09/estado-de-la-exposicion-de-la-industria.html

Resolución Nº 8996- 2002. Sala Constitucional, del 13 de septiembre del 2002.

Sala Constitucional, Resolución Nº 01345 – 1998, del 27 de febrero de 1998.

Saldaña M. (2007). La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de la información personal en los Estados Unidos. Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades. Sanz, J. (17 de marzo de 2020). Israel recurre al espionaje para vigilar los movimientos de los infectados por coronavirus. Recuperado de https://elpais.com/sociedad/2020-03-17/israel-recurre-al-espionaje-para-vigilar-los-movimientos-de-los-infectados-por-coronavirus.html

Sánchez, D. (2015) Análisis de la Sentencia U.S. Supreme Court, Griswold vs. Connecticut, 381 U.S. 478 (1965). Recuperado de https://www.academia.edu/34312831/An%C3%A1lisis_de_la_Sentencia_U.S._Supreme_Court_Griswold_vs._Connecticut_381_U.S._478_1965_.pdf

Schuager, M. (19 de mayo del 2021) Nueva herramienta de google para detectar afecciones cutáneas. Recuperado de https://wwwhatsnew.com/2021/05/19/nueva-herramienta-de-google-para-detectar-afecciones-cutaneas/

Polo, J. (9 de julio de 2021). Detectar el cáncer de próstata en segundos ya es posible. Recuperado de https://wwwhatsnew.com/2021/07/09/detectar-el-cancer-de-prostata-en-segundos-ya-es-posible/

Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, Reglamento № 37554-JP, 2016.

Reglamento General de Protección de Datos, 2016, Parlamento Europeo.

Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales N° 37554-JP, 2012.

Reglamento del expediente digital único en salud -№ 8954-, 2018, Caja Costarricense del Seguro Social.

Reuters (28 de setiembre de 2020) Noruega planea aplicación de COVID-19 en base a tecnología de Google y Apple. Recuperado de https://www.reuters.com/article/salud-coronavirus-noruega-idLTAKBN26J1ZU

Valenzuela y Villacencio (2015). La constitucionalización de los derechos sexuales y reproductivos. Hacia una igual ciudadanía para las mujeres. Revista Ius et Praxis, Año 21.

20 Minutos (19 de diciembre del 2020). ¿Cuánto puede costar tu historial médico en la darkweb? Menos que un café. Recuperado el 14 de junio del 2021 de https://www.20minutos.es/noticia/4518195/0/coste-historial-darkweb-cafe/

Vízcaino, I. (27 de febrero de 2019). Presidente ejecutivo del IMAS: 'Hoy no podemos decir que no sabemos dónde están los pobres'. Recuperado de https://www.nacion.com/dialogos/presidente-ejecutivo-del-imas-hoy-no-podemos/2PNR3O6ERRAN3MO5CQWPVMU4TA/story/

Zúñiga, I. (2007). Reseña Histórica, Ministerio de Salud 1927-2007. Ministerio de Salud.