

Las buenas prácticas para el tratamiento del dato de salud

The best practices of the health data treatment

Mishelle Bermeo Vivar*

Investigadora Jurídica Independiente

Información del artículo

Original – Ruptura, 2022

Artículo recibido / Received: 1 de noviembre de 2022

Artículo aceptado / Accepted: 23 de enero de 2023

Citación

Bermeo, M. (2022). *Las buenas prácticas para el tratamiento del dato de salud*. Revista Ruptura de la Asociación Escuela de Derecho PUCE. Edición 2022, p. (219-243)

DOI: 10.26807/rr.v4i4.122

Resumen: La Ley Orgánica de Protección de Datos Personales entró en vigencia el 26 de mayo de 2021, y trajo consigo una serie de derechos, obligaciones y un nuevo enfoque de cómo debemos tratar los datos personales en el Ecuador. Dicha normativa incluye una definición de cuáles

* Abogada por la Pontificia Universidad Católica del Ecuador. Especialista Superior en Derecho Procesal por la Universidad Andina Simón Bolívar. Diplomado en Estudio sobre los Datos de Salud como Categoría Especial de Datos Personales en la Tech - Universidad Tecnológica. Cuenta con amplia experiencia en el campo del Derecho Sanitario, brindando asesoría tanto al sector del uso y comercialización de medicamentos y otros productos sanitarios, así como a prestadores de salud. Tiene experiencia en resolución de asuntos sanitarios en materia administrativa y litigiosa. Actualmente es Abogada el Estudio Jurídico Cevallos & Noboa, y forma parte de su Departamento Sanitario. Correo Electrónico: mishelle.bermeo@cevallosnobo.com

son los datos que deben ser considerados como datos sensibles, siendo uno de ellos, el dato de salud¹.

Históricamente siempre se ha tratado el dato de salud con la confidencialidad que amerita por motivo de la profesión de los médicos tratantes del paciente; sin embargo, la reciente normativa ha traído consigo una categorización especial a dicho dato, lo que implica tratarlo con mucha más diligencia y cuidado.

En el presente artículo se expondrá brevemente sobre el dato de salud, el motivo de su sensibilidad, qué datos son vinculados como datos de salud y cuál es el debido tratamiento que se debe de tener con este tipo de dato. Esto, con la finalidad de que todos los lectores se informen respecto a qué engloba el dato de salud, y cómo debe ser este tratado apropiadamente. Así también, se explicarán sobre algunas buenas prácticas para el tratamiento de este dato considerado como sensible, que sobre todo buscan proteger la intimidad del titular del dato.

Palabras clave: Dato sensible, dato de salud, protección de datos personales, pacientes, consentimiento.

Abstract: *The Organic Law for the Protection of Personal Data came into effect on May 26, 2021, and brought with it a series of rights, obligations and a new approach to how we should treat personal data in Ecuador. This regulation includes a definition of which data should be considered as sensitive data, one of them being health data.*

Historically, health data has always been treated with due confidentiality and the professional secrecy of the patient's treating physicians; however, the recent regulation has brought with it a special categorization of such data, which implies treating and preserving it with much more diligence and care.

1 Se precisa que según los artículos 4, 25 y siguientes de la Ley Orgánica de Protección de Datos Personales, el dato de salud es un dato sensible y también entra dentro de la categoría especial de dato.

This article will briefly explain the health data, the reason for its sensitivity, which data are linked as health data and what is the proper treatment that should be given to this type of data. The purpose of this is to inform all readers about what health data encompasses and how it should be treated properly. Also, some good practices for the treatment of this data considered as sensitive will be explained, which above all seek to protect the privacy of the owner of the data.

Keywords: *Sensitive data, health data, patients, consent, protection of personal data.*

Introducción

Cuando hablamos en materia de protección de datos, no lo podemos hacer sin traer a colación al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (En adelante, el RGPD).

El cuarto considerando del RGPD, hace mención a un concepto interesante:

El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. ().

Esta referencia es importante, puesto que, aunque muchos creen que las normas relacionadas a la protección de datos personales buscan que se dejen de tratar los datos de las personas, eso no es así.

El 26 de mayo de 2021, el Ecuador pasó a formar parte del gran catálogo de países que están regulando el tratamiento de los datos personales, y eso lo logró por medio de la expedición de la Ley Orgánica de Protección

de Datos Personales (en adelante, LOPDP). Dicha normativa, según lo señalado en su artículo 1, tiene como objeto y finalidad:

Garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela. (LOPDP, 2021).

Es decir, esta nueva normativa no pretende limitar el uso legítimo de los datos personales, sino normar su tratamiento, de tal manera que éste sea legítimo y consensuado por parte del titular del dato.

I. Definición de dato personal

Un dato es todo lo que identifica o hace identificable a una persona natural, sea de forma directa, o de forma indirecta.² Como lo define Cristea Uivaru (2017): "Los datos de carácter personal, son la referencia que nos hace individualizables. Consiste en toda aquella información relevante concerniente a una persona que nos hace identificables". (Pág. 33).

El RGPD define como datos personales a:

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. (Art. 4.1)

Entonces, básicamente todo dato que permita identificar a una persona de otra, es un dato personal.

2 Artículo 4 de la LOPDP.

Ahora bien, dentro de los datos personales, tenemos algunas categorías de datos sensibles, como son, datos de: género, religión, crediticios, biométricos, genéticos, salud, entre otros. Es importante destacar que el dato de salud no es un dato sensible, sino una categoría especial de dato, por lo que en este artículo me enfocaré en lo que respecta al dato personal de salud.

II. El dato de salud

No se puede hablar del dato relativo a la salud, sin antes conceptualizar el concepto de salud.

La Organización Panamericana de la Salud (2018) se ha ratificado en el concepto de salud establecido por la Organización Mundial de la Salud en 1947: "un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades". (Pág. 4).

Asimismo, dicha entidad ha manifestado que: "En el campo de la salud pública existe una jerarquía de conceptos: el dato es la unidad más primaria (input) que, al trabajar con ella, genera un indicador; este, una vez analizado, genera información que, luego de interpretada, genera conocimiento". (Organización Panamericana de la Salud, 2018, pág. 6).

Entonces, esto denota que el dato relativo a salud es aquel que revela información sobre el estado de salud de una persona, sea esta pasada, presente o futura; y por medio del cual se concretan estadísticas e investigaciones.

Los datos personales, referidos a la salud, contienen información de las personas que permite conocer las dolencias o enfermedades que han padecido, padecen o incluso podrán padecer o tendrán tendencia a padecer en el futuro. Se trata, en definitiva, de datos personales que forman parte de la esfera más íntima de la persona, que pueden estar revelando situaciones críticas relativas a determinadas enfermedades a la aplicación de técnicas de reproducción asistida o relativa a información genética, cuyo potencial vulnerador de la intimidad personal nadie se atreve a poner en duda. (Piñar Mañas, 2004, págs. 42-44).

Por otro lado, el profesor Murillo De la cueva (2008) citado por Cristea Uivaru (2017) sostiene que:

Son aquellos que, por afectar a los aspectos más íntimos de la personalidad, reciben el más alto nivel de protección establecido. Y eso se debe a que se sitúan en un plano en el que confluyen dos derechos fundamentales al menos: el derecho a la intimidad y el derecho a la autodeterminación informativa. E, incluso, pueden proyectarse sobre otros estrechamente relacionados con los anteriores, como la libertad ideológica reconocida en el artículo 16 de la Constitución o con el propio derecho a la protección de la salud. Contienen, por tanto, una información personal especialmente cualificada y esencialmente ligada a la dignidad y libertad de aquél a quien pertenecen. (Pág. 44).

Dicho esto, sabemos que el dato de salud es aquel dato que identifica a una persona, se relaciona con su salud y directamente con la esfera más íntima y personal del titular del dato. Es decir, no necesariamente se limita a aquel dato que obtiene el profesional de la salud mientras trata al paciente, sino que puede ser aquel que forma parte de su genética, orientación sexual, fertilidad, entre otras esferas.

Ahora bien, tanto el RGDP, como la propia LOPDP, definen como datos relativos a la salud aquellos: “datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.” (Art. 4, LOPDP, 2021).

Tal como se mencionó previamente, por cuanto el dato de salud forma de parte de una esfera íntima y sensible de la persona, es muy común encontrar que se lo catalogue como un dato sensible. La normativa ecuatoriana ha hecho lo propio, en vista de que, si el dato es tratado indebidamente, puede causar discriminación o provocarle un riesgo grave al titular del mismo. (Ramón, P., s/f).

III. El tratamiento del dato de salud:

3.1 ¿En qué consiste el tratamiento del dato?

En líneas anteriores se mencionó que la LOPDP tiene como finalidad tratar de forma adecuada a los datos personales; más aún, aquellos que

son catalogados como datos sensibles, dado el impacto que éstos tienen en el titular del dato.

Cristea Uivaru (2017) hace hincapié en que:

El tratamiento de datos debe entenderse como el conjunto de operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. (Pág. 58-59).

Es importante destacar que, estamos frente al tratamiento de datos, aunque no los utilicemos de forma constante. Es decir, basta su almacenamiento y su utilización esporádica, y con ello ya se configura el tratamiento de datos. “Se entiende que existe tratamiento de datos por el mero hecho de poseerlos, conservarlos o visualizarlos, aunque, no exista dolo o intención de usarlos, ya sea de forma lícita o ilícita”. (Cristea Uivaru, 2017, pág. 59).

En función de ello, es importante traer a colación que nuestra normativa define al tratamiento como:

Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales. (Art. 4, LOPDP, 2021).

Es decir, toda aquella actividad que se pueda realizar con el dato personal, implica un tratamiento del mismo; por lo que lo prescrito en el artículo citado previamente no es una enumeración taxativa, sino ejemplificativa.

3.2 El consentimiento y tratamiento legítimo del dato

Ahora, ¿cuál es la forma apropiada de tratar el dato de salud? En la realidad sucede que el tratamiento del dato se puede dar de dos formas: con el consentimiento de su titular o sin él. A raíz de la expedición de la LOPDP, se busca crear una consciencia en la sociedad ecuatoriana respecto al legítimo tratamiento de los datos, lo que conlleva la necesidad de contar con el consentimiento del titular del dato para poder tratar y hacer uso de éste. Para que dicho tratamiento sea legítimo, requiere de un instrumento clave: el consentimiento.

La LOPDP trae consigo a la definición del consentimiento, entendiéndose como tal a la: "manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos". (Art. 4, LOPDP, 2021).

En concordancia con dicha definición, el artículo 8 de la mencionada normativa, menciona expresamente que se pueden tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. Dicha manifestación de la voluntad se plasma en el consentimiento, y para que éste sea válido, debe contar con cuatro requisitos fundamentales: que sea libre, específico, informado e inequívoco.

Implica que es libre cuando la manifestación de la voluntad está libre de vicios del consentimiento³; es específico cuando el consentimiento prevé la determinación concreta de los medios y fines del tratamiento; es informado cuando se socializa el consentimiento con el titular del dato respetando su derecho a la transparencia; y, es inequívoco por cuanto no debe presentar dudas sobre el alcance de la autorización otorgada por el titular del dato.

Asimismo, el mismo artículo 8 de la normativa en cuestión, establece de forma expresa que el consentimiento puede revocarse en cualquier

3 El artículo 1467 del Código Civil señala que los vicios del consentimiento son: error, fuerza y dolo.

momento, sin que ello requiera de una justificación por parte del titular. También se aclara que el tratamiento de los datos que se haya realizado con anterioridad a la revocatoria, se considerará como lícito, en vista de que el retiro del consentimiento no tiene efectos retroactivos.

Dicho esto, el consentimiento se convierte entonces en una pieza clave cuando nos referimos al tratamiento del dato, puesto que, sin él, el responsable del tratamiento del dato no puede realizar ningún tipo de tratamiento a los datos personales del titular. Cabe señalar que este consentimiento puede ser recabado de mediante firmas físicas, o por medios electrónicos, como, por ejemplo, mediante la firma electrónica. Hoy en día es bastante frecuente y común que el consentimiento se recabe, en su mayoría, por medios electrónicos. Un caso en referencia es cuando compramos un seguro para viajes, por cuanto lo podemos adquirir mediante un chat o por medio de una página web, y el contrato, que de por sí cuenta con cláusulas específicas de confidencialidad y de tratamiento de datos personales, adquiere plena validez con la sola firma electrónica que insertemos en el documento digital.

Es pertinente destacar que este consentimiento no tiene relación alguna con el consentimiento informado que suscribe el paciente para cada tratamiento médico al que decide someterse. Dicho consentimiento informado está relacionado con el derecho a la información⁴ y el derecho a decidir⁵ que tiene todo paciente cuando está ante una atención médica, ambos previstos en la Ley de Derechos y Amparo al Paciente; y también está relacionado con la obligación que tiene todo médico de recabar di-

4 Artículo 5.- Derecho a la información: Se reconoce el derecho de todo paciente a que, antes y en las diversas etapas de atención al paciente, reciba del servicio de salud a través de sus miembros responsables, la información concerniente al diagnóstico de su estado de salud, al pronóstico, al tratamiento, a los riesgos a los que médicamente está expuesto, a la duración probable de incapacitación y a las alternativas para el cuidado y tratamientos existentes, en términos que el paciente pueda razonablemente entender y estar habilitado para tomar una decisión sobre el procedimiento a seguirse. Exceptúense las situaciones de emergencia. El paciente tiene derecho a que el servicio de salud le informe quién es el médico responsable de su tratamiento.

5 Artículo 6.- Derecho a decidir: Todo paciente tiene derecho a elegir si acepta o declina el tratamiento médico. En ambas circunstancias el servicio de salud deberá informarle sobre las consecuencias de su decisión.

cho consentimiento que ratifica la explicación debida de la actividad médica que practicará en el paciente y que este último ha autorizado, puesto que conoce sus propiedades, beneficios y riesgos.⁶

Toda vez que se ha definido al consentimiento, se recalca que el artículo 26 de la LOPDP especifica de forma expresa:

Art. 26.- Tratamiento de datos sensibles.- Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias:

- a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines.
- b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social.
- c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento.
- d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos.
- e) El tratamiento se lo realiza por orden de autoridad judicial.
- f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

6 Los artículos 15 y 16 del Código de Ética Médica del Ecuador hacen mención a que no se pueden realizar intervenciones quirúrgicas sin previa autorización del enfermo o de su representante legal, e indica que dicha autorización incluye el tipo de intervención, riesgos y posibles complicaciones.

g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente ley.

Bajo este marco jurídico, el artículo 30 de la misma ley faculta a las instituciones que conforman el Sistema Nacional de Salud y a los profesionales de la salud a recolectar y tratar los datos relativos a la salud de sus pacientes. Asimismo, se especifica que tanto los responsables como encargados del dato deben guardar la confidencialidad de los datos a los que tengan acceso, obligación que se complementa con el secreto profesional.

De la misma manera, el mismo artículo prevé dos excepciones para la obtención del consentimiento por parte del titular:

No se requerirá el consentimiento del titular para el tratamiento de datos de salud cuando ello sea necesario por razones de interés público esencial en el ámbito de la salud, el que en todo caso deberá ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

Asimismo, tampoco se requerirá el consentimiento del titular cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como en el caso de amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, siempre y cuando se establezcan medidas adecuadas y específicas para proteger los derechos y libertades del titular y, en particular, el secreto profesional.

Un ejemplo de estas excepciones lo hallamos por efectos de la pandemia producto del COVID-19. Como es de conocimiento de todos, el ex Presidente, Lenin Moreno Garcés, por medio del Decreto Ejecutivo Nro. 1017 emitido el 16 de marzo de 2020, decretó el Estado de Excepción en todo el territorio ecuatoriano cuyo propósito era evitar la propagación y transmisión del coronavirus. Conforme fue pasando el tiempo, la sociedad de a poco retornó a sus actividades, hecho que se denominó como “la nueva normalidad”. Para que esto suceda, entidades estatales tuvieron acceso a las bases de datos de las personas y entidades que conformar la Red Pública Integral de Salud para analizar datos y elaborar estadísticas que servían como base para tomar decisiones en aras de modificar las

medidas dictadas por el Gobierno Nacional, y también por los Gobiernos Seccionales, acorde a la realidad mensual de la sociedad ecuatoriana.

Dicho esto, aunque no todos consentimos de forma expresa que se traten nuestros datos personales obtenidos por medio de las diferentes pruebas que detectan el virus, éstos fueron usados solamente para determinar el incremento o no del virus. Es decir, nunca se filtraron los nombres de las personas cuyo resultado era positivo, ni sus números de cédula, ni su condición de género; sin embargo, sí el resultado de la prueba que permitía crear bases de datos y a su vez contar con estadísticas de incremento o disminución de contagios. Por lo que, por parte del Estado, se configuró el tratamiento legítimo de nuestro dato de salud, en especial, porque actuaron al amparo de lo previsto en el numeral 4 del Art. 36 de la LOPDP.

3.3 Socialización de los derechos ARCO+⁷

En líneas anteriores se hizo mención a la necesidad de contar con el consentimiento del titular del dato para que su tratamiento sea legítimo, y se especificó que dicho consentimiento puede ser revocado en cualquier momento.

Pues bien, cuando el titular del dato consiente en su tratamiento, es obligación de la persona que recaba dicho consentimiento, socializarle sus derechos ARCO+. En el Ecuador, estas siglas engloban a los siguientes derechos⁸:

- a. Derecho a la información;
- b. Derecho de acceso;

7 En la doctrina, se conoce como derechos ARCO al conjunto de acciones, a través de las cuales el titular ejerce control sobre sus datos personales que se encuentran en posesión de un tercero.

8 Artículos 12 y siguientes de la LOPDP.

- c. Derecho de rectificación y actualización;
- d. Derecho de eliminación;
- e. Derecho de oposición;
- f. Derecho a la portabilidad;
- g. Derecho a la suspensión del tratamiento;
- h. Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas;
- i. Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas;
- j. Derecho de consulta; y,
- k. Derecho a la educación digital.

Por efectos prácticos, y en función del tema a abordar, explicaré brevemente sobre el derecho de acceso, de rectificación, eliminación y oposición.

El derecho de acceso consiste en la facultad que tiene el titular del dato personal para conocer y obtener, y acceder, de forma gratuita, a todos sus datos personales, sin la necesidad de presentar una justificación. Esta petición la puede realizar el responsable del tratamiento de sus datos personales, o directamente a la persona a quien entregó su consentimiento para tratar el dato.⁹

El derecho de rectificación implica que el titular del dato tiene derecho a solicitar la actualización o corrección de sus datos personales que sean inexactos, incorrectos o estén incompletos. Para este caso, no bastará su solicitud, sino que el titular deberá presentar los debidos justificativos.

9 Derecho contenido en el artículo 13 de la LOPDP.

Es importante denotar que la persona que realice esta rectificación, tiene la obligación de reportar al titular sobre dicha acción.¹⁰

El derecho de eliminación también es conocido como el derecho de eliminación. Esto conlleva al hecho de que el titular del dato puede solicitar la supresión de sus datos personales. Según la normativa ecuatoriana¹¹, este derecho se ejerce cuando:

- 1) El tratamiento no cumpla con los principios establecidos en la presente ley;
- 2) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;
- 3) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;
- 4) Haya vencido el plazo de conservación de los datos personales;
- 5) El tratamiento afecte derechos fundamentales o libertades individuales;
- 6) Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o,
- 7) Exista obligación legal.

Respecto a este derecho, se determina la obligación al responsable del tratamiento del dato de implementar cualquier método y técnicas para eliminar, hace ilegible o dejar irreconocible de forma definitiva y segura de los datos personales.¹²

Finalmente, el derecho de oposición involucra a la facultad que tiene el titular de oponerse o negarse a que se traten sus datos personales. Tal

10 Derecho contenido en el artículo 14 de la LOPDP.

11 Derecho contenido en el artículo 15 de la LOPDP.

12 A nivel informático, esto conlleva un borrado definitivo.

como sucede con el derecho anterior, la LOPDP determina cuándo el titular se puede oponer al tratamiento de sus datos personales¹³:

- 1) No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley.
- 2) El tratamiento de datos personales tenga por objeto la mercadotecnia directa; el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines.
- 3) Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, previsto en el artículo 7, y se justifique en una situación concreta personal del titular, siempre que una ley no disponga lo contrario.

Respecto de estos cuatro derechos, la propia LOPDP estipula que, a petición del titular del derecho, éstos deben cumplirse en un plazo razonable desde su solicitud, concediendo un plazo de quince (15) días para su efectivo cumplimiento.

¿Cómo se socializan estos derechos? Por medio del consentimiento o de disposiciones contractuales. Dicho esto, se debe hacer referencia en el documento respecto a estos derechos del titular y la forma en la que los puede ejercer. De la misma manera, se debe especificar en cuáles casos, el derecho de rectificación, eliminación y oposición no tienen cabida; esto, por cuanto si sus datos son necesarios para el cumplimiento de una obligación legal o contractual o para la formulación, ejercicio o defensa de reclamos o recursos, éstos no pueden ser eliminados.¹⁴

Un caso muy práctico de la socialización de los derechos ARCO+ lo encontramos cuando nos registramos como pacientes en un Hospital. El momento en el que la atención hospitalaria inicia, siempre se solicitan

13 Derecho contenido en el artículo 16 de la LOPDP.

14 El artículo 18 de la LOPDP prevé 10 causales taxativas de las excepciones a los derechos de rectificación, eliminación y oposición.

los datos identificativos de la persona que está recibiendo la atención. En dicho momento, el personal de admisiones o el personal médico (dependiendo del establecimiento y la circunstancia en la que se lleva a cabo la atención) indicará al paciente o a quien lo acompañe cuál es la finalidad del tratamiento de datos, cuáles son los derechos que puede ejercer respecto a los mismos y cómo ejercerlos.

Por ejemplo, Anita a los 22 años registró un teléfono y un correo electrónico en el Hospital por cuanto tuvo una atención ambulatoria. El día de hoy Anita tiene 30 años y acudió nuevamente al Hospital por un leve accidente y cuando validan la información previamente registrada, así como su consentimiento, Anita detecta que hay datos que deben ser modificados. Dicho esto, Anita toma contacto con el médico que la está atendiendo y le manifiesta que desea ejercer su derecho a la rectificación de datos y proporciona su nuevo teléfono y correo electrónico, por cuanto entiende y consiente que aquellos sirven como medios de contacto. Posterior a ello, el momento en el que Anita recibe su factura por los servicios prestados, puede verificar que el dato fue rectificado correctamente, así como también recibió un correo electrónico por medio del cual el Hospital notificó que se cumplió con la solicitud de ejercicio del derecho de rectificación y que los datos anteriores fueron eliminados de sus bases de datos.

3.4 Buenas prácticas para tratamiento del dato de salud

Toda vez que hemos entrado en contexto de qué es un dato de salud y los requisitos para que su tratamiento sea legítimo, me permitiré realizar un breve resumen de aquellas buenas prácticas para su correcto tratamiento.

3.4.1 Práctica del secreto profesional

Todos los médicos tienen la obligación de ejercer su profesión, respetando su deber de secreto profesional respecto de la información a la que tienen acceso durante su práctica."En el ámbito sanitario, la protección de datos y la confidencialidad de los mismos, va intrínsecamente rela-

cionado con el secreto médico”. (Vid. Sánchez Jordán citado por Cristea Uivaru, 2017, pág. 109).

Según la doctrina especializada en la materia y el derecho comparado, el secreto profesional no solo es un deber respecto del médico que interviene directamente con el paciente, sino que “se extiende hacia todo el personal sanitario que tienen acceso al paciente, ya sea la enfermera en la misma consulta, el equipo médico en una intervención, o el personal administrativo que gestionada los datos de salud del paciente”. (Cristea Uivaru, 2017, pág. 111). De la misma manera, el secreto profesional es una obligación que perdura en el tiempo, por lo que la muerte del paciente no exime al médico de este secreto médico.¹⁵ (Cristea Uivaru, 2017, pág. 111).

En el Ecuador, el secreto profesional también se encuentra regulado, puesto que el Código de Ética Médica prevé en su artículo 66 lo siguiente:

Art. 66. — El secreto profesional es un deber que nace de la esencia misma de la profesión. El interés público, la seguridad de los enfermos, la honra de las familias, la responsabilidad del profesional y la dignidad de la ciencia médica, exigen el secreto. Los médicos tienen el deber de conservar en secreto todo cuanto observen, escuchen o descubran en el ejercicio de su profesión.

Esta disposición, más la contenida en el Art. 30 de la LOPDP, garantizan que el secreto profesional del médico permite un tratamiento apropiado y legítimo del dato de salud.

Ahora, para que ambas disposiciones tomen fuerza, éstas pueden constar en los contratos de trabajo de los profesionales de salud o en un instrumento a parte que resguarde el correcto tratamiento de los datos de salud, tales como políticas internas de tratamiento de datos personales, convenios específicos de confidencialidad y uso legítimo del dato personal de salud, códigos deontológicos, entre otros. Asimismo, se puede reforzar con capacitaciones al respecto, haciendo énfasis en todo lo que

15 Esta obligación también está contenida en la Declaración de Ginebra que prevén promesas de los médicos. Una de ellas: “Guardar y respetar los secretos confiados a mí, incluso después del fallecimiento del paciente”. Disponible en: <https://www.wma.net/es/policies-post/declaracion-de-ginebra/>

engloba el secreto profesional; y, sobre todo, actuando bajo el principio de responsabilidad proactiva¹⁶.

Se destaca también que el secreto profesional aplica para quienes son abogados y ejercen en aquellas ramas de Derecho relacionados con el campo de la salud. Esto, por cuanto, dada su práctica, pueden tener acceso a historias clínicas, declaraciones de salud, entre otros documentos donde constan datos personales de salud. Así como para con los médicos, es muy común que los profesionales en derecho cuenten con convenios de confidencialidad específicos, así como contratos con cláusulas de tratamiento de datos, en especial por cuanto es muy común que actúen en calidad de encargados del dato personal.

3.4.2 Anonimización del dato

El Diccionario de la Real Academia de la Lengua nos indica que anonimizar significa “expresar un dato relativo a entidades o personas, eliminando la referencia de su identidad”.¹⁷

Acorde a la Agencia Española de Protección de Datos (2016) “la finalidad del proceso de anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos”.

De la misma manera, Cristina Gómez (s.f) indica que “la anonimización no es una alternativa a la obtención del consentimiento expreso, sino que más bien es una protección adicional para que la información confidencial sea usada únicamente de forma legítima o divulgada con consentimiento.”

16 El Art. 52 de la LOPDP estipula: “Los responsables y encargados de tratamiento de datos personales podrán, de manera voluntaria, acogerse o adherirse a códigos de conducta, certificaciones, sellos y marcas de protección., cláusulas tipo, sin que esto constituya eximente de la responsabilidad de cumplir con las disposiciones de la presente ley, su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia.”

17 Tomado de: <https://dle.rae.es/anonimizar>

En la normativa ecuatoriana, este término no resulta inadvertido, puesto que la LOPDP define a la anonimización como “la aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados”. (Art. 4, LOPDP, 2021).

Asimismo, dicha norma expresamente hace mención a que siempre que sea posible, los datos relativos a la salud, deberán ser previamente anonimizados o seudonimizados.¹⁸ Sin embargo, prevé que todo tratamiento de este tipo de datos que sean anonimizados, debe ser autorizado de forma previa por la Autoridad de Protección de Datos Personales; y, para ello, el interesado tiene que presentar ante dicha autoridad el respectivo protocolo técnico que garantice la protección de los datos y que contenga el informe previo favorable emitido por la Autoridad Sanitaria.¹⁹

En este orden de ideas, la Agencia Española de Protección de Datos (2016) menciona que el proceso de anonimización se relaciona con los siguientes seis (6) principios claves:

- *Principio de responsabilidad proactiva:* Conlleva a que la protección de la privacidad debe realizarse de forma proactiva y no reactiva;
- *Principio de privacidad por defecto:* Implica la garantía de mantener la confidencialidad de los datos que se anonimizarán.
- *Principio de privacidad objetiva:* Se relaciona con el pequeño margen de riesgo que puede existir al momento de la reidentificación; por lo que se debe procurar que en dicho margen no conste la información más importante del titular del dato.
- *Principio de plena funcionalidad:* Se debe prever que no exista una distorsión de los datos que son anonimizados, de tal manera que siempre se defina la utilidad final de los mismos.

18 Esta disposición se encuentra en el numeral 2 del artículo 31 de la LOPDP.

19 Esta disposición se encuentra en el numeral 3 del artículo 31 de la LOPDP.

- *Principio de privacidad en el ciclo de vida de la información:* Corresponde a que las medidas que garantizan la privacidad del titular del dato sean aplicables en todo el proceso, desde el momento en el que recaba el dato hasta su anonimización. Para ello, se pueden contar con auditorías que garanticen su cumplimiento.
- *Principio de información y formación:* Esto involucra la capacitación constante del personal que participa en todo el proceso de anonimización del dato.

Realizando un análisis en derecho comparado, la Presidencia de Uruguay expidió en el 2020 la Guía sobre Anonimización de Datos²⁰, misma que establece las siguientes etapas básicas para el proceso de anonimización:

- Definición del equipo de trabajo;
- Definición de objetivos y finalidad de la información anonimizada;
- Preanonimización;
- Anonimización; y,
- Control.

Si bien en el Ecuador no existe una guía de cuáles serían los pasos a seguir para anonimizar el dato, sí exige su autorización previa presentación del protocolo técnico.

Bajo mi criterio, es algo positivo puesto que cada integrante de la Red Pública Integral de Salud está en su facultad de implementar el proceso de anonimización acorde a su necesidad, operatividad y tamaño. Además, puede tomar como base la definición prevista en la LOPDP.

20 Información obtenida de: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Gu%C3%ADa%20sobre%20Anonimizaci%C3%B3n%20de%20Datos%20vf.pdf>

Por ejemplo, tomando nuevamente el ejemplo en los Hospitales, existen ciertos procesos que utilizan datos personales que pueden ser anonimizados. Pensemos en este escenario: Juanito Pérez, trabajador del Hospital ABC ha sido Jefe Administrativo por más de 5 años en dicho lugar, y está concursando para ascender a Gerente Administrativo. Por cuanto Juanito ha presentado unos síntomas extraños, decidió realizarse todos los exámenes de rutina, y dentro de ellos, incluyó las pruebas NAT, mismas que detectan la existencia o no de VIH. Él se realiza todos sus exámenes en el Hospital ABC; y, arrojó positivo para el virus. El Jefe de Laboratorio, al enterarse, toma distancia de forma real y comenta entre los demás trabajadores sobre el virus de Juanito, lo que provoca en los demás trabajadores distanciamiento, burlas y malos comentarios.

El Gerente General del Hospital ABC se entera de lo sucedido, y por cuanto le asusta compartir mismo espacio con quien sería su mano derecha, decide comunicarle a Juanito que no puede continuar con el proceso de ascenso y le ratifica que conservará su puesto “a pesar de lo que le ha sucedido”.

¿Cuál era la necesidad de que el personal del laboratorio conozca la identidad de la persona que se realizaba el examen? Ninguna. Plenamente pueden manejarse por medio de códigos que identifican al paciente ante el médico tratante y el laboratorio que analiza la muestra. El hecho que el Jefe de Laboratorio identificare a su compañero, además de su falta de confidencialidad, generó en él un perjuicio, por cuanto trató ilegítimamente su dato de salud.

Con ello, resulta bastante evidente porqué la anonimización resulta ser una buena práctica para tratar apropiadamente el dato de salud.

3.5 Relevancia de las buenas prácticas para el tratamiento del dato de salud

En este literal me permitiré desarrollar un criterio de carácter personal, puesto que, a raíz de la expedición de la LOPDP, he podido detectar que no todos los abogados que se vinculan de alguna u otra manera en el

campo de protección de datos, conocen ciertas especificaciones respecto al dato de salud.

Es muy común encontrar profesionales del derecho quienes únicamente respaldan el tratamiento del dato de salud en modificaciones de Reglamentos Internos de Trabajo, contratos, convenios de confidencialidad y formularios para recabar el consentimiento del titular del dato personal cuando ello solo es el inicio.

Las buenas prácticas del dato de salud previamente detalladas permiten que el titular tenga muchas más garantías respecto al tratamiento de su dato de salud que es mucho más sensible que un dato como el correo electrónico, por citar un ejemplo.

Muchas de las ocasiones inclusive, aunque no exista una relación con un hospital, el dato de salud forma parte de nuestro entorno laboral. Esto, por cuanto, por mandato legal, todo trabajador o trabajadora se encuentra en la obligación de la realización de exámenes ocupacionales. Principalmente pensaríamos que el Centro de Salud del establecimiento laboral guarda la confidencialidad de los resultados médicos, así como de cualquier eventual diagnóstico, pero estoy segura que el titular del dato estaría mucho más seguro o segura si se garantizaría su anonimización, y el acceso limitado al mismo.

Actualmente, no se cuenta todavía con la designación de la Autoridad de Protección de Datos Personales, sin embargo, una vez que contemos con su creación, considero que va a aportar mucho respecto de las buenas prácticas para el tratamiento de datos personales, en especial, del dato de salud. Recordemos que inclusive es quien forma parte de la aprobación cuando se implementa la anonimización, por lo que su revisión respecto de las metodologías y forma de aplicar esta práctica, ayudaría tanto al sector de salud del ámbito público y privado.

IV. Conclusiones

La normativa ecuatoriana, que es un reflejo de la europea en materia de protección de datos trae consigo un mensaje poderoso: usemos apropia-

damente los datos que nos proporcionan sus titulares. Es por ello por lo que resulta cada vez más necesario conocer la forma en la que nuestros datos personales son protegidos, especialmente aquellos que son catalogados como sensibles, tal como sucede con el dato de salud.

La LOPDP le otorga esa categoría al dato de salud, y con ello impone la obligación de que éste sea tratado con mucho más cuidado y reserva. Dicho esto, su tratamiento no solo va ligado a la obtención del consentimiento libre, específico, informado e inequívoco; sino que también presenta en la sociedad la necesidad de desarrollar técnicas que permitan su debido y legítimo tratamiento.

En este artículo se mencionaron dos buenas prácticas para el tratamiento del dato personal: la práctica del secreto profesional y la anonimización del dato. Respecto de la primera, ésta es inherente al ejercicio profesional del médico, quien a su vez debe garantizar que el personal que trabaje con él, también mantenga la confidencialidad y secreto de la información que recaba del paciente que trata; y, respecto de la segunda, resulta novedosa, puesto que de cierta manera desasocia la identidad del titular del dato y el dato *per sé*, por lo que no se podría arribar a la conclusión de que determinada persona es la titular de un dato en concreto.

No se descartan aquellas no enunciadas aquí o que puedan crearse a lo largo del tiempo, puesto que la imaginación es el límite que permite diseñar técnicas para tratar legítimamente todo dato personal; sin embargo, no hay duda de que ambas prácticas funcionan y cumplen con su finalidad de tratar apropiadamente el dato de salud, por lo que, si nosotros como ciudadanos estamos frente a ellas, podemos estar tranquilos respecto al tratamiento que se les da a nuestros datos en dicho campo.

Referencias Bibliográficas

Agencia Española de Protección de Datos. (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. Recuperado el 30 de octubre de 2022 de: <https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf>

- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos*. Publicado en el Registro Oficial Nro. 459 del 26 de mayo de 2021.
- Beltrán Aguirre, J. (2009) *Tratamiento de Datos de Salud en la Prestación de Servicios Sociales*. Revista Derecho y Salud. Volumen XVIII Enero-Junio 2009. págs.1-20. ISSN: 1133-7400. Disponible en: <https://www.ajs.es/sites/default/files/2020-05/2009-numero1.pdf>
- Congreso Nacional (1995). *Ley de Derechos y Amparo al Paciente*. Última reforma publicada en el Suplemento del Registro Oficial Nro. 423 del 22 de diciembre de 2006.
- Cristea Uivaru, L. (2017). *La Protección de Datos de Carácter Sensible en el ámbito europeo. Historia Clínica Digital y Big Data en Salud*. [Tesis Doctoral, Universitat Abat Oliba CEU]. Recuperado el 30 de octubre de 2022 de: <https://www.tdx.cat/bitstream/handle/10803/442972/Tlcu.pdf?sequence=5.xml>
- Gómez Piqueras, C. (2009). *Disociación/Anonimización de los Datos de Salud*. Recuperado el 30 de octubre de 2022 de: https://www.ajs.es/sites/default/files/2020-05/DyS-Vol18-01-estudio_03.pdf
- El Parlamento Europeo y El Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*.
- Ministerio de Salud Pública. (2016). *Acuerdo Nro. 00000115 — Manual de Seguridad del Paciente — Usuario del Ministerio de Salud Pública*. Publicado en el Registro Oficial Nro. 14 de noviembre de 2016.
- Ministerio de Salud Pública. (1992). *Código de Ética Médica*. Última reforma publicada en el Registro Oficial Nro. 300 del 20 de octubre de 1993.
- Murillo De la Cueva, P. (2008). *El Derecho a la autodeterminación informativa y la protección de datos personales*. Recuperado el 30 de octubre de 2022 de: <https://core.ac.uk/download/pdf/11501784.pdf>
- Organización Panamericana de la Salud. (2018). *Indicadores de salud. Aspectos conceptuales y operativos*. Washington, D.C.: OPS. Recupera-

do el 30 de octubre de 2022 de: https://iris.paho.org/bitstream/handle/10665.2/49058/9789275320051_spa.pdf;jsessionid=18037ACD7EB8E-27C6203BEE9ADFA2BA4?sequence=5

Presidencia de Uruguay. (2020). *Guía sobre Anonimización de Datos*. Recuperado el 30 de octubre de 2022 de: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Gu%C3%ADa%20sobre%20Anonimizaci%C3%B3n%20de%20Datos%20vf.pdf>

Ramón, P y Álvarez, M. (s.f). *Oportunidades y desafíos en la protección de datos personales*. Entrevista en página web. Recuperado el 30 de octubre de 2022 de: <https://www.pwc.ec/es/entrevistas-de-temas-de-interes/ley-de-proteccion-de-datos-personales.html#:~:text=Un%20dato%20sensible%20se%20refiere,preferencia%20sexual%3B%20que%20afectan%20la>