

SID, Simposio de Informática y Derecho

El manejo de los Datos Genéticos en la Legislación Argentina

Marina Lara Flammini

Miembro del Grupo de Estudio de la Complejidad en la Sociedad de la Información (GECSI). Facultad de Cs. Jurídicas y Sociales. U.N.L.P.

Resumen. En este trabajo se analiza el estado actual de la protección en el Ordenamiento jurídico Argentino de los datos personales, en especial de los datos genéticos. En esta línea se exponen algunos de los efectos negativos que ello ocasiona a los titulares de los datos y la desprotección en la que se encuentran ante la posible vulneración a su intimidad al ser utilizados con fines distintos para los cuales el titular del dato había consentido al momento de otorgarlos. Esta situación afecta directamente la esfera privada, la seguridad jurídica, la intimidad y la libertad. Metodológicamente se parte de un análisis de la normativa existente y de la descripción de situaciones problema que ponen en tensión los derechos de las personas. A modo de cierre, se reafirma que el respeto a la dignidad, libertad e intimidad de la persona humana, son causales suficientes para considerar necesaria la elaboración de un régimen jurídico que tenga en cuenta, particularmente, los avances de las Tecnologías de la Información y las Comunicaciones.

Palabras clave: Identidad - Datos personales - Datos genéticos - Intimidad - Privacidad - Big Data - Historia clínica electrónica

Abstract In this paper we analyze the current state of protection of personal data, specifically genetic data, in the Argentine legal system. In this line, we can find some negative effects that this causes to the owners of this information. Also, it is possible to see their lack of protection since the data given is used for different purposes, violating their privacy and the consent first granted. This situation directly affects the private sphere, legal security, privacy and freedom. In terms of methodology, we study the existing regulations and the description of problematic situations that jeopardize people's rights. In conclusion, respect for the dignity, freedom and privacy is paramount, and a legal regime that takes into account, especially, the advances of the Information and Communications Technologies must be developed.

1 Introducción

El descubrimiento del ácido desoxirribonucleico (ADN) humano supuso una verdadera revolución científica que no tardó en convertirse en un nuevo paradigma de

investigación en diversos campos científicos. Sin embargo, a pesar de haber sido descubierto hace ya más de cincuenta años, no hay en el ordenamiento nacional argentino una ley que lo proteja específicamente. Como consecuencia, ninguna persona se encuentra protegida frente a una eventual apropiación (por parte de un tercero) de su código genético. Esto supone un riesgo para la persona que podría ser víctima de tal apropiación y, en menor medida, para sus familiares cercanos.

El ADN se encuentra en todas las células del cuerpo, presentando el plan general que estructura a todo ser vivo, el cual contiene datos sensibles que hacen a la identidad[1] de la persona tales como su origen étnico, sexo, salud y expresión física. Por lo que en él se puede apreciar la potencialidad de la vida humana, tanto en su faz biológica como así también en su faz intelectual.

Desde el punto de vista del desarrollo actual de las tecnologías de la Información y comunicación (TIC) y las consecuencias que estas traen en la sociedad, podemos referirnos a la importancia de este tema frente al peligro de la apropiación de datos personales en general, y sobre todo los datos biométricos y de salud.

En este trabajo, nos referiremos al caso específico de la apropiación del genotipo (o código genético) de una persona y que, en consecuencia, pueda ser utilizado con fines distintos a los que el titular del dato había consentido al momento de otorgarlos.

2 Algunos conceptos básicos

Consideramos necesario precisar, de manera sencilla, algunos conceptos que se utilizarán a lo largo del trabajo. En este sentido, se puede definir:

- ADN y Genes [2]

* ADN: Es una molécula presente en casi todas nuestras células que contiene la información genética. Posee el código que determina todas las características y el funcionamiento de un individuo. Y su principal función es el almacenamiento de información biológica que es transmitida de generación en generación, es por ello que se la llama “la molécula de la herencia”.

* Genes: como la unidad básica de almacenamiento de información de los seres vivos, que está contenida en el ADN y que codifica en ellos a proteínas que luego realizará una función específica cada célula del organismo.

- Genotipo y fenotipo [3]

* Genotipo: es el conjunto de la información genética particular de un individuo, es esencialmente la secuencia de ADN.

* Fenotipo: es todo aquello que “vemos” (del griego, fainein, visible) y que no es secuencia de ADN. Es tanto lo macroscópico (forma, anatomía, fisiología, patología y comportamiento), como lo más pequeño (histología,

bioquímica y estructura molecular). Pudiendo definirlo entonces como el resultado de la interacción de un determinado genotipo con un determinado ambiente, lo cual se expresa con la fórmula: FENOTIPO = GENOTIPO + AMBIENTE. Cabe aclarar que, para algunos fenotipos, la influencia del componente genético es mayoritaria o determinante y, en consecuencia, la ambiental es virtualmente nula.

2.1 Información genética y singularidad

La «información genética» puede obtenerse tanto de los datos que surgen del estudio del genoma de un ser humano, como también del estudio de su historia familiar.

Entonces, se podrá clasificar a información genética en dos sentidos[4]:

* Información genética en sentido estricto «refiere a la codificación genética de los cromosomas humanos presentes en los núcleos y en las mitocondrias de las células y el estado y número de los cromosomas». Solamente abarca a los datos obtenidos mediante medios directos, por medio de análisis de ADN, ARN y proteínicos.

* Información genética en sentido amplio “todo tipo de información sobre los factores hereditarios de un individuo, que puede ser obtenida a través de: 1. la reconstrucción de la historia familiar; 2. la observación del fenotipo de una persona; y 3. del análisis de sus proteínas”, es decir, mediante métodos indirectos de obtención.

La Declaración Internacional sobre los Datos Genéticos Humanos de la UNESCO del año 2003¹, hace referencia a la “singularidad”[5] de la información genética, al referir que “Los datos genéticos humanos son singulares por su condición de datos sensibles, toda vez que pueden indicar predisposiciones genéticas de los individuos y que esa capacidad predictiva puede ser mayor de lo que se supone en el momento de obtenerlos; pueden tener para la familia, comprendida la descendencia, y a veces para todo el grupo, consecuencias importantes que persistan durante generaciones; pueden contener información cuya relevancia no se conozca necesariamente en el momento de extraer las muestras biológicas; y pueden ser importantes desde el punto de vista cultural para personas o grupos”.

Al momento de intentar definir la naturaleza de los datos contenidos en el ADN se advierte que no es tarea sencilla, y que la misma acarrea diversas problemáticas:

Primeramente por ser la “molécula de la herencia”, lo que significa que se hereda y que, en consecuencia pueden (¿pueden o lo hacen?)compartir genes los miembros de una familia e incluso toda una rama familiar, transformando la historia genética de una persona en una historia compartida por diferentes generaciones, pudiendo decir

¹La Declaración Internacional sobre los Datos Genéticos Humanos de la UNESCO del año 2003.

Disponible en: http://portal.unesco.org/es/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html (Consulta efectuada el día 17 de julio de 2019).

entonces que el ADN arroja datos referentes a la historia de una línea sucesoria, permitiéndonos llegar a conocer el origen étnico de una persona determinada.

Sumado a ello, cabe agregar que el genotipo puede ser parcialmente “reconstruido” o “deducido” a partir de muestras extraídas de una línea sucesoria, lo cual está íntimamente relacionado con el hecho de que el factor genético es la raíz de muchas enfermedades. Inclusive puede detectarse sí, a pesar de no tener riesgos, los sucesores o antecesores del individuo la pueden padecer, por lo que podría decirse que el ADN también arroja datos referentes a la salud de una línea sucesoria.

Asimismo, algunos estudios, tales como los presentados por Emil F. Coccaro[6], Miles y Carey[7], plantean que determinados genes detectados, sin estar referidos directamente a la salud de una persona, son constitutivos de sus cualidades, tales como su imagen, su psique, el coeficiente intelectual, altura, color de ojos e incluso las tendencias (vgr. a la agresividad).

En relación al factor genético entendido como la raíz de muchas enfermedades o condiciones heredadas, al poder realizar una vinculación directa con los procesos de selección laboral, créditos, seguros, entre otros, permitiría una discriminación a priori por una “potencialidad” de sufrir diversas enfermedades que generen una disminución de la capacidad laboral y costos adicionales a la empleadora, como así también condiciones o conductas “potenciales” que no le permitan al individuo aplicar a un empleo determinado.

3 Historia Clínica digital, Machine Learning y Big Data

Para definir la historia clínica se tomará la definición otorgada por la ley nacional de Derechos del paciente, historia clínica y consentimiento informado (Ley 26.529) en su artículo 12 y para definir historia clínica electrónica única se recurrirá a la ley provincial de Sistema de historia clínica electrónica única de cada persona (Ley 14.494) en su artículo 2 y a la ley de la Ciudad Autónoma de Buenos Aires de la Historia Clínica Electrónica (Ley 5.669) en su artículo 4 inciso 14:

** El Art 12 de la Ley Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud (Ley 26.529) entiende a la historia clínica como “[...] el documento obligatorio cronológico, foliado y completo en el que conste toda actuación realizada al paciente por profesionales y auxiliares de la salud”.*

** El artículo 2 de la ley de Sistema de historia clínica electrónica única de cada persona, define a la historia clínica electrónica única como “el conjunto de datos clínicos, sociales y administrativos referidos a la salud de una persona, procesados a través de medios informáticos o telemáticos”.*

**El artículo 4 inciso 14 de la Ley de Historia Clínica Electrónica. (Ley 5.669, Ciudad Autónoma de Buenos Aires), nos dice que la Historia Clínica Electrónica es aquella “cuyo registro unificado, personal y multimedia, se encuentra contenido en una base de datos,*

administrada mediante programas de computación y refrendada con firma digital del profesional tratante. Su almacenamiento, actualización y uso se efectúa en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad y acceso, de conformidad con la normativa aprobada por la autoridad de aplicación de la presente ley, como órgano rector competente. La Historia Clínica Electrónica (HCE) es sinónimo de historia clínica informatizada ó historia clínica digital. Forman parte de la Historia Clínica Electrónica (HCE) los consentimientos informados, las hojas de indicaciones médicas y/o profesionales, las planillas de enfermería, los protocolos quirúrgicos, las prescripciones dietarias, certificados de vacunación, los estudios y prácticas realizadas, rechazadas o abandonadas”. “[...] Las historias clínicas son propiedad de los pacientes, y son administradas por los establecimientos de salud o los servicios médicos de apoyo”.

Según Pérez[8], su finalidad primordial es recoger datos del estado de salud del paciente con el objeto de facilitar la asistencia sanitaria, aunque también se podrían utilizar para la evaluación de la calidad asistencial, administrativa y médico-legal e incluso la docencia y la investigación. *“Lo que distinguiría al entorno big data es, por un lado, la incorporación de otras fuentes de información como las derivados de los servicios prestados por las App de e-salud, wereables, las redes sociales o las plataformas «nube», y la posibilidad de realizar la consulta a múltiples fuentes de datos online”.*

Ante la situación recién expuesta en combinación con la actual implementación de tecnologías de Machine Learning sobre Big Data en el ámbito de la salud, surge la posibilidad de acceder a datos masivos (provenientes de múltiples fuentes de información que permitirán conocer datos relevantes en relación a la salud de la población, los cuales generalmente proceden de fuentes diseñadas “ad hoc” para la investigación o bien de fuentes secundarias, como las historias clínicas electrónicas , pruebas de laboratorio, censo de población, entre otras) y relacionarlos y estudiarlos con el objeto de que estos sean analizados y transformados en “nueva información”, lo cual es posible como consecuencia del entrecruzamiento de datos estructurados y no-estructurados.

Por lo que podría decirse que al someter los datos a este proceso “Machine Learning” (aprendizaje automático) el cual reconoce patrones de conjunto de datos y extrae información o decide acciones a realizar en base de dichos patrones, su valor va aumentando, ya que al combinarse datos dan como resultado una nueva información la cual genera un valor agregado. En este proceso el sistema “aprende” y se perfecciona a través de sus propios resultados, la información que resulta de este proceso puede transformarse en un dato de entrada del mismo algoritmo y ser procesada como un nuevo dato, arrojando como resultado una nueva información (y permitiendo búsquedas cada vez más exactas), y en consecuencia seguiría aumentando el valor del dato.

4 Big Data en otras áreas

Lo antes expuesto sería también aplicable a otras sectores o áreas que reciben datos sensibles como ser el Sistema de Identidad Digital (SID)[9], una plataforma

recientemente implementada por el Estado Nacional en conjunto con el ReNaPer que tiene por objetivo la validación remota y en tiempo real de la identidad del individuo, a partir de la utilización de datos biométricos (tales como el reconocimiento facial) y fotografía del DNI, logrará dicha autenticación. En este caso titular de los datos los otorga de manera voluntaria para acceder a servicios o realizar Trámites a Distancia (TAD) desde cualquier dispositivo móvil con conectividad. En cuanto a la protección, aseguran desde su página informativa que los datos proporcionados serán utilizados únicamente con el fin al que se otorgan. En lo referido a la seguridad describen la tecnología utilizada e intentan generar en el usuario una confianza tal, para que este pueda brindar sus datos sin temores. Pero bien sabemos que esta seguridad puede sufrir fallas -involuntarias o no- y ante ellas pueden producirse posibles intromisiones, que al igual que en el ámbito de salud, ocasionan a sus titulares los mismos daños y para lo cual será necesaria mayor protección.

Creemos válido hacer mención a esta plataforma de acumulación de datos sensibles, como tantas otras que existen o se crearán en función del desarrollo de la sociedad tecnológica, que si bien no son específicamente del ámbito de salud, tienen a su disposición base de datos sensibles, los cuales requerirán el prudente tratamiento instrumental y legislativo necesario.

5 Anonimización de los datos personales, y la posibilidad de ser reidentificados

El actual régimen de datos personales en Argentina, el que será tratado más adelante, protege a la *“información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables”* (art. 2 de la Ley de Protección de Datos Personales LPDP N° 25.326), pero si el objetivo es garantizar la privacidad de los datos, el procedimiento a utilizar es la anonimización de los mismos. Para ello se aplica una técnica de disociación de datos, entendida como aquel tratamiento de datos personales que hace que la información obtenida no pueda asociarse a persona determinada o determinable (art. 2 de la LPDP), los datos dejan de tener el carácter de *“personales”* y por lo tanto ya no se encuentran amparados por el régimen argentino y tampoco se requiere el consentimiento del titular de dichos datos para que la información pueda cederse (Art.11 inc.3e de la LPDP).

A pesar de ser posible la anonimización de los datos personales, puede resultar insuficiente, ya que si bien estos pierden su carácter personal, no garantiza la privacidad de los mismos en virtud de que es factible volver a conectarlos con la persona a la que pertenecen a través de una reidentificación de los mismos, siendo posible a través de la utilización de los datos de un Dataset sobre el cual se han aplicado técnicas de anonimización. Esto podría llevarse a cabo siempre y cuando se cuente con los medios necesarios y los conocimientos técnicos.

Por lo que podría decirse que por más que en los procesos de protección una persona consienta el uso de sus datos bajo la condición que su identidad sea preservada (anonimización), estos podrán resultar insuficientes e ineficaces.

6 Nuevos manejos de la información: la situación actual

Es evidente que previo a la digitalización de los datos en tratamiento, los efectos eran más limitados, con las nuevas TICs y Big Data, el paciente puede disfrutar de ciertas comodidades (en cuanto a distancias y tiempo), como así también una mejora en la forma de satisfacción de sus intereses y necesidades. Por otra parte, los usuarios que la empleen (por ejemplo las empresas, organizaciones y administraciones públicas) pueden anticipar los comportamientos y desarrollar políticas y estrategias basándose en esos datos. También pueden reducir costes y tener un aumento de los ingresos, esto supone un nuevo punto de inflexión tanto para las empresas como así también para los nuevos manejos en el mercado, viendo entonces la importancia de la información considerándola centro de diversas decisiones, por lo que se están adoptando estas nuevas posibilidades de procesamiento de grandes volúmenes de datos, para acercarse más a los gustos y necesidades del cliente, generando así un “nuevo mercado” o nueva forma de ver al mismo.

Dicho esto, cabe recordar que los sistemas de gestión de bases de datos tradicionales son incapaces de procesar este nuevo contexto, lo que ha hecho necesaria la aparición de nuevas formas de manejo de datos masivos basadas en la compilación y explotación de datos personales a gran escala.

Esta nueva situación ha generado un mercado monetizado respecto de datos sensibles. Ello directamente relacionado con la informatización de las historias clínicas, y los datos biométricos que estas contienen.

Como ya hemos adelantado, ante la falta de protección legal acorde a las nuevas realidades y prácticas sociales que ofrecen las TICs en conjunción con la ausencia del secreto profesional, pueden ser utilizados para propósitos que exceden el ámbito sanitario o de investigación. Como así también, con fines diferentes para los que su titular había prestado consentimiento en un momento de especial vulnerabilidad, en el cual asiste a un servicio sanitario preocupado por su salud y aporta datos que piensa que serán utilizados específicamente para su tratamiento. Situación que pone en peligro la relación de confianza médico - paciente. Consecuentemente, se genera en cabeza del titular de los datos cierta inseguridad/desconfianza ante posibles fallas del sistema que ocasionen la divulgación de su información personal y el uso no autorizado de sus datos. En este sentido, toma noción del peligro que significa que éstos lleguen a posibles empleadores, agencias de marketing, aseguradoras, etc.

La realidad nos refleja que en muchas oportunidades dicho datos son “cedidos” para otros fines[10], por lo que habrá que comprender la magnitud del daño que

significa el hecho de que corporaciones acopien y rentabilicen información de los particulares, lo cual significa un factor de poder (político y económico), reflejado en la toma de decisiones que pueden afectar a la sociedad en su totalidad. Un ejemplo de ello son los datos de diagnóstico genético que identifican a portadores de enfermedades genéticas hereditarias, o determinan riesgo o susceptibilidad de padecer enfermedades más complejas. En este punto, se ven expuestos a potenciales situaciones discriminatorias que afectan directamente a la igualdad de oportunidades, por ejemplo frente a la búsqueda de aplicar a un empleo o un préstamo y la selección previa de personal, basadas en perfiles y patrones de comportamiento creados con fines que el afectado no puede controlar.

6.1 Actores intervinientes, y la posibilidad de acceder a datos sensibles

Al avanzar en el tema, advertimos que los actores intervinientes en la gestión, tratamiento y aprovechamiento de los datos personales en estudio, no pertenecen exclusivamente al sector sanitario sino que provienen de otros sectores tales como el financiero, educativo, comercial, etc. El problema se presenta al notar que poseen intereses diversos sobre los datos en cuestión, entrando en conflicto dichos intereses, diversos derechos y la disputa por el poder. Considerando al poder como conjunto de recursos de cualquier índole, del que dispone o cree disponer cada actor para procurar su objetivo[11]. Desde esta perspectiva, encontramos a la información (dominio y manejo) como un recurso especial en este contexto social, y el acceso a las Tecnologías de la Información y Comunicaciones.

En consecuencia, el uso indebido y malicioso de las TICs en el ámbito de salud amenaza a la privacidad de los ciudadanos, quienes tienen derecho a conocer quién dispone de sus datos personales y con qué finalidad, generando una problemática en la Sociedad de la Información[12] y por otro lado, surgen en cabeza de los demás intervinientes en el proceso de recolección, tratamiento y protección de datos, deberes y responsabilidades atinentes a la actividad que desarrollen, que en el caso de realizar su función de manera deficiente o ilícita debieran verse directamente involucrados y en su caso alcanzados por la sanción o penalización pertinente.

Por lo aquí desarrollado, podemos apreciar la consecuente tensión entre el avance de la tecnología en el ámbito de salud y la Protección de Datos Personales y su privacidad.

La consecuencia directa de la situación recién enunciada afecta tanto los titulares de dichos datos como a quienes establecen una relación de confianza tal, que hacen posible la recolección de los mismos.

En relación a los titulares de los datos sensibles, se ven afectados directamente sobre su esfera privada, seguridad jurídica, intimidad y la libertad. En este punto, podríamos preguntarnos “¿qué es privado o cuán privados pueden ser determinados

datos?”, desde el punto de vista de la teoría alemana de las esferas de privacidad², la respuesta podrá variar según la respuesta de un migrante o un nativo digital, teniendo en cuenta el uso del entorno digital y el acostumbramiento de estos usuarios a distintos niveles de exposición. La diferencia podrá darse en el grado de afectación que sufra el titular del dato en cuestión y aquella información que pretendía que quede en el ámbito de lo privado/intimidad. En términos de responsabilidad legal, esta distinción no sería útil, ya que con el sólo hecho de verse utilizados los datos con fines distintos para los cuales fueron otorgados, debiera sancionarse independientemente del daño que ocasione en cada caso en particular.

En lo referido a los operadores de salud, podemos ver cómo se ven responsabilizados directamente ante la falla del secreto profesional. Pero a su vez también serán responsables aquellos operadores destinados a la recolección, gestión y custodia de datos. Como así también la institución que nuclea a los recién mencionados. En este punto, ya no estaríamos hablando de una afectación en la esfera de la intimidad/privacidad, sino que estaríamos incurriendo en la responsabilidad profesional.

Pero no tenemos que dejar de hacer mención a terceros actores o partes intervinientes, como el Estado, ONGs, laboratorios, agencias de marketing, ART, farmacias, empleadores, los programadores, entre otros, que tienen gran injerencia e influencia en esta situación y que a pesar de no formar parte de la relación mencionada con anterioridad, se ven involucrados directamente ante esta situación.

Se puede concluir en que se encuentran presentes una serie de actores, que dependiendo de las obligaciones y funciones que desarrollen, podrá recaer sobre ellos una cuota de responsabilidad. Pudiendo establecerse a su vez un paralelismo con la “cadena de custodia”, y la relación al daño por ellos ocasionado, en este punto se ha entrevistado a distintos operadores de salud sobre la existencia de protocolos de las instituciones médicas en las que desarrollan sus actividades y planteaban total desconocimiento sobre la existencia del mismo, haciendo alusión solamente al hecho de la cuestión del secreto y ética profesional de no divulgar datos de los pacientes.

6.2 Intimidad/privacidad. Desarrollo Jurisprudencial y doctrinario

Desde el punto de vista del desarrollo jurisprudencial y doctrinario, se ha expresado que el derecho a la privacidad e intimidad se fundamenta en el art. 19 de la

² El Dr. Adolfo Roberto Vázquez en el fallo “Maradona, Diego Armando s/lesiones leves, agresión, daño y amenazas reiteradas” postula que: “corresponde reconocer la existencia de tres esferas dentro de las cuales las personas realizan su existencia: pública la primera, privada la segunda, íntima la tercera. La primera y la segunda se interseccionan con un espacio común que puede ser mínimo o máximo, según las circunstancias. En cambio la tercera respecto de la segunda tiene una relación de inclusión. Se encuentra dentro de lo privado y no admite la intromisión ilegítima de la prensa. La intimidad no es simplemente el derecho a la soledad sino un conjunto de aspectos de la vida individual y familiar de las personas que no deben ser conocidos por los demás, pertenecen por entero a cada cual y a partir de ese segmento de vida liberada de la mirada y opinión de los demás todo ser humano tiene el dominio de su imagen, su identidad y personalidad”. (CSJN, 03-10-2002. Maradona, Diego Armando s/lesiones leves, agresión, daño y amenazas reiteradas).

Constitución Nacional. En relación directa con la libertad individual se encuentra la protección jurídicamente un ámbito de autonomía individual constituida por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o actos que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para la intimidad[13].

Nadie puede inmiscuirse en la vida privada de una persona, tampoco puede afectar áreas no destinadas a ser difundidas sin su consentimiento o el de sus familiares autorizados para ello (sólo podrá justificarse tal intromisión por ley, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la lucha contra del crimen).

Por lo que se podría afirmar la estrecha relación entre el derecho a la intimidad con la noción de libertad, como lo hace Vidal Martinez[14] quien sostiene que el bien jurídico protegido por el derecho a la intimidad es una libertad soberana, a que el hombre es acreedor en el ámbito de lo íntimo, y en el caso de ser ésta última eliminada, la persona se reduciría a ser un simple objeto o cosa.

En consonancia, la CSJN se ha pronunciado al respecto sosteniendo que es fundamental para la existencia de una sociedad libre, el derecho a la privacidad, consagrado en el art. 19 de la CN, así como también el art. 11, incisos 2 y 3, del ya mencionado Pacto de San José de Costa Rica, según los cuales nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación, además, toda persona tiene derecho a estar protegida contra esos ataques por la ley, y que el derecho a la vida privada fue observado por nuestro más Alto Tribunal, desde el punto de vista de su fundamento constitucional, de su contenido, de sus titulares, y de sus límites. No podemos dejar de hacer mención a lo referido a los Derechos y actos personalísimos del Capítulo 3, agregado al Libro Primero, Título I, en el CCyCN, recoge un concepto totalmente distinto del contenido en el antiguo Código Civil apuntado en sus artículos 51 y 52, en conjunción con el artículo 1770.

En los arts. 51 y 52 exponen que la tutela de la dignidad se extiende en los derechos personalísimos a la integridad espiritual, denominación utilizada en doctrina para distinguirlos de aquellos que están relacionados con la integridad física, la vida y la libertad de las personas comprendiendo todo menoscabo a la dignidad que es, entonces, objeto de prevención y reparación, entre los que figuran la intimidad y la privacidad. El interés jurídico tutelado es el derecho que tiene toda persona de poder gozar de un sector privado ajeno al conocimiento del Estado o de terceros. Por su parte, el art. 1770 del CCyCN plantea la posibilidad de fijar mecanismos judiciales de prevención o de tutela inhibitoria del daño futuro y previsible en relación a derechos personalísimos. Esto es importante porque en este ámbito el resarcimiento o la indemnización difícilmente logran reparar el perjuicio y no existe la reparación en especie[15].

6.3 Revisión normativa vigente a nivel nacional

Una revisión de la normativa vigente a nivel nacional involucra la Ley 26.529 (Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud), Ley 23.511 (Banco Nacional de Datos Genéticos), Ley 26.529 (Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud), Decreto 1089/2012 (Reglamentación de la Ley N° 26.529. Derechos del Paciente en su relación con los Profesionales e Instituciones de la Salud.), presenta ausencias de esta cuestión particular.

El proceso de reforma de la ley 25.326 del año 2016, impulsado por la Agencia de Acceso a la Información Pública (AAIP), la cual remplazo a la desaparecida Dirección Nacional de Protección de Datos Personales (DNPDP), anterior autoridad de aplicación de la Ley, creando una plataforma colaborativa abierta al sector público, privado y académico, para que los diferentes referentes expusieran los cambios a ser considerados en la Ley, proceso que se denominó "Justicia 2020", el sitio de participación ciudadana del Ministerio de Justicia y Derechos Humanos de la Nación.

El resultado de tales intercambios fue la redacción de un anteproyecto de reforma de ley, el cual tuvo dos versiones, la última del año 2017. El 19 de septiembre de 2018, el Poder Ejecutivo Nacional presentó el Proyecto MEN-2018-147-APN-PTE (el "Proyecto") con la intención de sustituir la Ley de Protección de Datos Personales N° 25.326 promulgada en el año 2000.

Los argumentos del Proyecto señalan la necesidad de derogar la Ley 25.326, por haber quedado desactualizada en relación a los progresos tecnológicos y normativos, en especial la aprobación del Reglamento General de Protección de Datos de la Unión Europea (el "RGPD").

Pensamos que para evitar un "vacío legal" podrían aplicarse las disposiciones de la ley vigente relativa a los datos sensibles, por analogía, a la información genética. Por lo que la ley N° 25.326 (B.O. 2/11/00) de Datos Personales, tiene por objeto: «la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre».

Pero cabe aclarar que la normativa no incluye como dato personal a la información genética, ni la menciona expresamente, pero haciendo una interpretación amplia, podría entenderse analizando su artículo 2, que se encuentra protegida de modo implícito en la categoría establecida de dato sensible, además consagra derechos de los titulares de datos, identificando y determinando obligaciones de los responsables del tratamiento de datos.

En esta ley tratan el principio de reserva (art. 7) y el de confidencialidad, que debe ejercerse en conjunto con el otorgamiento del consentimiento por parte del titular de los datos personales.

Por su parte, el proyecto de modificación de la Ley de Protección de Datos Personales antes mencionado[16], incorpora en su artículo 2 la definición de datos genéticos: “son aquellos datos personales relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona”, otorgándoles un tratamiento especial y restrictivo por lo que son considerados datos sensibles reconociendo la “potencialidad que tienen ese tipo de datos para afectar la esfera íntima de sus titulares”, originando una discriminación ilícita o arbitraria.

En relación al consentimiento, el proyecto establece que debe ser otorgado por el titular de los datos, y que debe ser informado y expreso para una o varias finalidades específicas, siendo requisito de licitud para el tratamiento de datos sensibles, y que la revocación del mismo podrá efectuarse sin limitaciones, en cualquier momento y sin efecto retroactivo.

En relación a la seguridad de los datos, en el artículo 19 del proyecto refiere a la «responsable del tratamiento y, en su caso, del encargado, adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales (...), considerándolos siguientes factores: 1. el riesgo inherente por el tipo de dato personal; 2. el carácter sensible de los datos personales tratados; 3. el desarrollo tecnológico; 4. las posibles consecuencias de una vulneración para los titulares de los datos; 5. las vulnerabilidades previas ocurridas en los sistemas de tratamiento; 6. el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada a su posesión.

El 16 de enero de 2019 se publicó en el Boletín Oficial la Resolución 4/2019[17] de la Agencia de Acceso a la Información Pública, que tiene por finalidad establecer criterios orientadores de mejores prácticas en la aplicación de la Ley 25.326, regula siete aspectos puntuales relacionados con el tratamiento de los datos personales: I) el ejercicio del derecho de acceso con relación a bases de datos de video vigilancia; II) el tratamiento automatizado de datos personales; III) el concepto de “persona determinable”; IV) el concepto de “datos biométricos”; V) la obligación de validar a la identidad por parte del titular de la bases de datos; VI) la cesión de datos personales en el ámbito público, y VII) el tratamiento de datos personales de menores.

La Resolución no prevé un régimen especial para los datos biométricos, pero los define como “aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única”. Además establece que, cuando los datos biométricos puedan revelar datos potencialmente

discriminatorios para su titular, serán considerados como datos sensibles, en los términos del artículo 2 de la Ley 25.326.

A su vez, cabe hacer mención a la reciente aparición del Reglamento General de Protección de Datos (RGPD o GDPR, siglas en inglés) de Europa, y la modificación que se ha ocasionado en los servicios en línea los cuales se busca que otorguen mayor visibilidad a sus términos y condiciones, a nivel local se espera que sea un incentivo a la actualización de la vigente Ley 25.326 de Protección de Datos Personales para adaptarla al GDPR respecto del tratamiento y procesamiento de datos personales y facilitar el intercambio de información y teniendo en cuenta las amenazas y vulneraciones posibles en materia de datos, como las que conocemos hoy.

Los fundamentos de la nueva regulación europea han servido como fuente para la elaboración de la propuesta de reforma de la ley 25.326, los cuales aumentan y mejoran las herramientas para proteger los datos personales, y se la ha tenido en cuenta como una guía para la actualización de los “Estándares Iberoamericanos de Protección de Datos Personales”, los cuales buscan convertirse en un marco de referencia para la homogeneización de las regulaciones sobre protección de datos personales en la región.

7 Conclusiones

Entendemos que hay que tomar conciencia de la importancia que significan los datos de carácter personal, encontrándose afectados datos biométricos y de salud, como lo son aquellos datos sobre la imagen, la voz, el propio cuerpo, así como también el honor, reputación, y tener como objetivo principal su protección, respetando los principios de proporcionalidad, autonomía de la voluntad, consentimiento informado, necesidad, limitación del propósito, seguridad, minimización, conservación de los datos, igualdad y no discriminación, para lo cual deben establecerse garantías que eviten el tráfico de datos y cualquier uso indebido por las empresas del ámbito de la salud (seguros médicos, corporaciones farmacéuticas, entidades financieras y otros). En suma, habrá que perseguir y lograr la protección eficaz de la libertad, la cual no debe limitarse al ámbito de lo íntimo sino que es necesario extenderla a toda manifestación exterior, para lo cual se debería dar fortalecimiento de sistemas de prevención que permitan desalentar las amenazas a la privacidad, sentando bases que tiendan a una real seguridad jurídica.

El respeto a la dignidad, libertad e intimidad de la persona humana, son causales suficientes para considerar necesaria la elaboración de un régimen jurídico destinado a tutelar específicamente la temática relacionada con la información genética.

¿Cómo podrían ser protegidos estos datos?

Creemos que haciendo base en el Proyecto de modificación de la Ley de Protección de Datos Personales previamente mencionado, debería confeccionarse un

marco legal en el cual los ciudadanos encuentren protección a los derechos mencionados con anterioridad. Entre los temas a tratar se debería incluir:

- a) Consentimiento expreso por parte del titular de los datos. El cual debe ser efectuado en forma expresa, libremente y por escrito. El mismo será efectuado en un instrumento en el que conste que dichos datos podrán ser utilizados únicamente para el uso convenido.
- b) Instrumentación por escrito del consentimiento.
- c) Obligaciones, responsabilidades y eventuales sanciones civiles y/o penales, de los actores intervinientes en el proceso y sus diversas etapas tales como la recolección, tratamiento y protección de los datos.
- d) Formas de reparación del daño ocasionado al titular de los datos.

En relación al estado de la situación actual, creemos que ante el vacío legislativo y los eventuales conflictos que puedan suscitarse, los actores afectados quedarían en manos del arbitrio del juzgador que intervenga en el mismo, pudiéndose obtener resultados disímiles e insatisfactorios ante situaciones similares atentando contra la igualdad y la seguridad jurídica.

Atento a que las Tecnologías de la Información y la Comunicación van evolucionando, y que el derecho siempre se hace presente como respuesta a las necesidades de la sociedad, creemos sumamente importante que se analicen estos temas en profundidad y se puedan dar garantías reales de protección a la libertad, la intimidad y la seguridad jurídica a través de un marco normativo capaz de regular estas situaciones.

Referencias

- [1] LICEDA, Ernesto. “La identidad digital”. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/20717/Documento_completo.pdf?sequence=1&isAllowed=y (Consulta efectuada el 17 de julio de 2019).
- [2] MORÁN, Alberto. “ADN, genes, cromosomas...” Disponible en: <http://www.dciencia.es/adn-genes-cromosomas/> (Consulta efectuada el 10 de junio de 2019).
- [3] KORNBLIHTT, Alberto, “Genoma humano”. Disponible en: <http://www.salud.gob.ar/dels/printpdf/127> (Consulta efectuada el 17 de julio de 2019).
- [4] Informe titulado «Confidencialidad de los Datos Genéticos», elaborado por el Comité de Ética en la Ciencia y Tecnología (CECTE) en el año 2002.
- [5] LAFFERRIERE, Jorge N.: «La información genética y sus características especiales», Microjuris 2012 (MJ-DOC-5791-AR | MJD5791) . Citado en el trabajo de Bernardita Berti García . Cita: MJ-DOC-11914-AR | MJD11914 .(Julio de 2017). <https://aldiaargentina.microjuris.com/2017/07/31/la-informacion-genetica-en-el-proyecto-de-reforma-a-la-ley-de-proteccion-de-datos-personales-en-la-argentina-beriti-garcia-bernardita/> (Consulta efectuada el 30 de junio de 2019)
- [6] COCCARO EF. “A family history study of intermittent explosive disorder.” J Psychiatr Res. 2010;44:1101–5.
COCCARO EF, BERGEMAN CS, MCCLEARN GE. “Heritability of irritable impulsiveness: a study of twins reared together and apart.” Psychiatr Res. 1993;48:229–42.

- [7] MILES DR, CAREY G. “Genetic and environmental architecture of human aggression.” *J Pers Soc Psychol.* 1997;72:207–17.
- [8] STANDEN A. “How big data is changing medicine listen: KQED Science (Internet). 2014. Citado por PÉREZ, Glòria Pérez. “Peligros del uso de los big data en la investigación en salud pública y en epidemiología” (7 de septiembre de 2015). Disponible en: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0213-91112016000100014 (Consulta efectuada el 30 de junio de 2019)
- [9] <https://www.argentina.gob.ar/sid-sistema-de-identidad-digital> (Consulta efectuada el 30 de junio de 2019)
- [10] <https://www.iprofesional.com/impuestos/275327-cuit-afip-renta-financiera-Escandalo-por-boicot-en-la-AFIP-ordenan-una-investigacion-interna-tras-la-filtracion-de-datos-de-contribuyentes>
<https://www.latercera.com/noticia/filtracion-de-datos-del-minsal/>
<https://www.lanacion.com.ar/opinion/mas-proteccion-para-los-datos-personales-nid2145578>
<https://andina.pe/agencia/noticia-ministerio-justicia-investiga-posible-filtracion-datos-la-onpe-719892.aspx>
https://elpais.com/internacional/2017/07/27/actualidad/1501155942_203526.html
<https://ayudaleyprotecciondatos.es/2018/03/08/filtraciones-mir-investigadas-aepd/>
https://www.clarin.com/sociedad/filtracion-datos-personales-gigantes-internet-castigados_0_Wt5LNwtc8.html (Consultas efectuadas el 17 de julio de 2019)
- [11] ENTELMAN, R. F., 2005, “Teoría de Conflictos. Hacia un nuevo paradigma.”, Ed. Gedisa., Barcelona, Primera edición 2002.
- [12] NSSM 200 - “El Plan por el Control”. Informe Kissinger.
- [13] Fallo “Ponzetti de Balbin, Indalia c/ Editorial Atlantida S.A.” - (CSJN, año 1984) - Disponible en: <http://thomsonreuterslatam.com/2015/09/fallo-clasico-indalia-ponzetti-de-balbin-c-editorial-atlantida-s-a/> (Consulta efectuada el 30 de junio de 2019)
- [14] VIDAL MARTINEZ, Jaime, “El derecho a la intimidad en la ley orgánica del 5/5/82”, Madrid, 1984, pág. 23, citado por RIVERA, Julio Cesar, op. cit., pág. 117.
- [15] LEZCANO, José María, LICEDA, Ernesto y GERLERO, Mario S. “Redes y derecho” - Capítulo 6 “Intimidad y Privacidad en el Código Civil y Comercial Argentino” 2018.
- [16] <https://www.infobae.com/tecno/2018/06/23/en-la-era-de-la-big-data-cuales-son-los-5-cambios-que-buscan-modernizar-la-ley-de-proteccion-de-datos-personales/> (Consulta efectuada el 13 de junio del 2019)
- [17] <https://www.abogados.com.ar/mejores-practicas-en-la-aplicacion-de-la-ley-de-proteccion-de-datos-personales-resolucion-42019-de-la-agencia-de-acceso-a-la-informacion-publica/23000> (Consulta efectuada el 30 de junio de 2019)
<https://www.marval.com/publicacion/proyecto-de-ley-de-proteccion-de-datos-personales-13237> (Consulta efectuada el 30 de junio de 2019)

Bibliografía y demás documentos consultados

1. Itziar de Leucona “Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (big data)”
2. LLÀCER MR, Casado M, Buisán L, editores. Documento sobre bioética y Big Data en salud: explotación y comercialización de los datos de los usuarios de la sanidad pública. Barcelona: Publicacions i Edicions Universitat de Barcelona; 2015. p. 72.
3. PÉREZ G. Peligros del uso de los big data en la investigación en salud pública y en epidemiología. *GacSanit.* 2016;30:66–8. (<http://www.gacetasanitaria.org/es-peligros-del-uso-los-big-articulo-S02139111150020466>.)

4. STANDEN, A. How big data is changing medicine listen: KQED
<http://ww2.kqed.org/science/2014/09/29/how-big-data-is-changing-medicine/>
5. GIL GONZÁLEZ, Elena. “Big Data. Privacidad y Protección de Datos” Ed. Agencia Española de Protección de Datos (año 2016) ISBN: 978-84-340-2309-3.
6. PUYOL MORENO, Javier. Una aproximación a Big Data. Universidad Nacional de Educación a Distancia. España. Revista de Derecho UNED nro. 14 (año 2014)
<http://revistas.uned.es/index.php/RDUNED/article/view/13303/12174> (Última consulta 19 de Agosto de 2017)
7. LEZCANO, José María. OLIVEIRA, Noemí Luján. La Historia Clínica Electrónica: Entre la e-Salud y la Privacidad
8. PLOMIN, Robert. DeFries, John C. McClearn, Gerald E. y McGuffin, Peter. Genética de la conducta.
9. BERTI GARCÍA, Bernardita. Cita: MJ-DOC-11914-AR | MJD11914 .(Julio de 2017).
10. CSJN, 03-10-2002. Maradona, Diego Armando s/ lesiones leves, agresión, daño y amenazas reiteradas. Disponible en: <http://www.csjn.gov.ar/jurisprudencia.html>