Revista Bioética
ISSN: 1983-8042
bioetica@portalmedico.org.br
Conselho Federal de Medicina
Brasil

Outomuro, Delia; Mirabile, Lorena M.
Confidencialidad y privacidad en la medicina y en la investigación científica: desde la bioética a la ley.
Revista Bioética, vol. 23, núm. 2, 2015, pp. 238-243
Conselho Federal de Medicina
Brasília, Brasil

Confidencialidad y privacidad en la medicina y en la investigación científica: desde la bioética a la ley

Delia Outomuro [1], *Lorena M. Mirabile* [2]

Resumen

A partir del Juramento Hipocrático, la ética médica y la bioética se han ocupado de la confidencialidad y de la privacidad. Luego, el Principialismo las ha entendido como reglas bioéticas derivadas de la autonomía entendida como autogobierno. El derecho positivo también se ha ocupado de ellas. Entre las normativas legales relacionadas con el tema, se destaca en Argentina la Ley 25.326 de protección de datos, por su relación con la práctica médica y la investigación. Ésta tiene su base en el *habeas data*, garantía constitucional que permite a las personas pedir explicaciones a los organismos públicos o privados que poseen datos o información sobre ellas y en el artículo 19 de la Constitución Nacional.

Palabras-clave: Confidencialidad. Privacidad. Sistemas de computación-Información. Protección-Leyes. Seguridad.

Resumo

Confidencialidade e privacidade na pesquisa médica e científica: da bioética ao direito

Desde o Juramento de Hipócrates, a bioética e a ética médica têm-se ocupado da confidencialidade e privacidade. Mais tarde, foram consideradas pelo principialismo regras bioéticas derivadas da autonomia, entendida como autogoverno. O direito positivo também se ocupou delas. Entre as normas legais relativas ao assunto existe, na Argentina, a Lei 25.326 de protecção de dados, importante por sua relação com a prática médica e pesquisa. Ela tem no *habeas data* garantia constitucional que permite que as pessoas procurem explicações de organismos públicos ou privados que tenham dados ou informações sobre elas, com base também no artigo 19 da Constituição.

Palavras-chave: Confidencialidade. Privacidade. Sistemas de computação-Informação. Proteção-Leis. Segurança.

Abstract

Confidentiality and privacy in medicine and scientific research: from bioethics to the law

Since the Hippocratic Oath, medical ethics and bioethics have been concerned with confidentiality and privacy. Thereafter, principialism has understood them as bioethical rules derived from bioethical rules derived from the autonomy understood as self-governance. Positive law is also concerned with them. Among the legal norms related to the topic, Argentinian Law 25,326, on protection of data because of their relationship with medical practice and research, stands out. It is grounded in *habeas data*, the constitutional guarantee that permits persons to request explanations from public or private bodies that have data or information regarding them, and in Article 19 of the National Congress.

Keywords: Confidentiality. Privacy. Computer systems-Information. Protection-Laws. Safety.

1. Doutora deliaoutomuro@gmail.com **2. Doutora** lmirabile@fmed.uba.ar – Universidad de Buenos Aires (UBA), Ciudad Autónoma de Buenos Aires, Argentina.

Correspondência
Instituto de Bioética – Facultad de Medicina (UBA); Calle Paraguay 2.155 (Primer piso sector Uriburu) CP 1121. Ciudad Autónoma de Buenos Aires, Argentina.

Declaram não haver conflito de interesse.

La ética médica y la bioética se han ocupado exhaustivamente de la confidencialidad y de la privacidad, en especial en lo referente a la práctica de la medicina. Basta recordar el Juramento Hipocrático en el que se instruye a los médicos del siguiente modo: *Guardaré silencio sobre todo aquello que en mi profesión, o fuera de ella, oiga o vea en la vida de los hombres que no deba ser público, manteniendo estas cosas de manera que no se pueda hablar de ellas* [1] . Desde Hipócrates en adelante, aunque con altibajos, se ha pugnado por respetar estos derechos. Recientemente, el derecho positivo se ha ocupado de ellos. Entre las normativas legales relacionadas con el tema destacan en Argentina la ley 25.326 [2] de protección de datos que, a su vez, tiene fundamento en el *habeas data* (HD).

En este trabajo nos proponemos describir en qué consiste esta normativa, su vinculación con las reglas bioéticas de privacidad y confidencialidad y su aplicación a la clínica y a la investigación. En primer lugar elucidaremos el concepto de HD, su finalidad, clases y excepciones. Luego nos ocuparemos de la citada ley nacional de protección de datos y nos centraremos en aquellos artículos de interés por su relación con la práctica médica y la investigación.

Concepto de *habeas data*

HD es un término latino que significa "tienes tus datos", "tened la información o los datos". Se trata de una garantía constitucional que permite a las personas pedir explicaciones a los organismos públicos o privados que poseen datos o información sobre ellas, y así averiguar *qué* datos tiene, *cómo* los han obtenido, *por qué* y *para qué* los tienen. Esta garantía encuentra su fundamento en el artículo 19 de la Constitución Nacional Argentina [3] y se incorporó explícitamente en la Carta Magna con la reforma de 1994, en el artículo 43 (3º párrafo), regulándose luego la ley 25.326 de 2000 [2].

La legitimación activa – *quién* puede reclamar – corresponde a toda persona, sea ésta persona física o jurídica, transeúnte o habitante de la nación. Cualquier persona puede entonces tomar conocimiento de los datos referidos a ella y de su finalidad para exigir la supresión, rectificación, actualización o la confidencialidad de los datos, si ellos fueren falsos o discriminatorios. La legitimación pasiva – *a quién* se reclama – corresponde a los bancos de datos públicos y a los bancos de datos destinados a producir informes. Nótese que en el caso de los bancos de datos no públicos se exige que los mismos sean "destinados a producir informes", cosa que no ocurre cuando se trata de bancos de datos públicos.

Su finalidad es proteger el derecho a la intimidad y a la privacidad, aunque para algunos autores [4] el bien protegido es más amplio, pues la divulgación de información podría provocar en algunos casos daños patrimoniales o profesionales. El HD permite: 1) acceder al registro de datos; 2) actualizar los datos; 3) corregirlos; 4) solicitar que la información, obtenida legalmente, no se exponga públicamente a terceros; 5) suprimir datos sobre información sensible (ideología política, religión, sexualidad etc.) que afecte la intimidad o que pueda usarse para discriminar. Se entiende por "datos sensibles" aquellos que revelan origen racial y étnico, los referentes a opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Clases de HD y excepciones

Con base en la finalidad, podemos distinguir los siguientes tipos de HD:

1) HD informativo: permite solicitar al organismo que posee los datos qué datos tiene, cómo los obtuvo, para qué los quiere etc. Como su nombre lo indica, es informativo pues el organismo que reserva los datos debe informarnos sobre cuales son;
2) HD rectificador: permite actualizar los datos o corregir la información errónea, es decir, rectificar la información que en ellos reside;
3) HD confidencial o preservador: permite solicitar la no exposición pública de los datos, hacer reserva de los datos.

Como todo principio, y sin perjuicio de lo expuesto, existen excepciones a esta garantía. Así, la Ley 25.326 establece:

1. *Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.*
2. *La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obliga-*

ciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. *Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa* [2].

Otros ámbitos no cubiertos por la garantía son:

- Documentación histórica consultada por científicos o investigadores;
- Documentación referida a la actividad comercial o financiera de una persona;
- Secreto de la fuente periodística.

Relevancia para la medicina y la investigación sobre la Ley 25.326

Antes de comentar aquellos aspectos de la ley que pueden relacionarse con la práctica de la medicina y con la investigación médica, es preciso recordar que la Argentina es un estado federal. Por tanto, ciertas competencias son exclusivas de la nación, otras lo son de las provincias y de la Ciudad Autónoma de Buenos Aires; siendo unas compartidas y otras concurrentes [5].

En el caso de la ley que nos ocupa, la misma norma en su artículo 44 señala que sólo *los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional. Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional* [2]. Por lo tanto, lo referido a partir del artículo 29, y que es atinente a organismos de control y sanciones, es de competencia local.

El artículo 5º hace referencia al consentimiento y establece que *el tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias* [2].

Dicho consentimiento debe ser informado, es decir, debe estar precedido de la información a la que hace referencia el artículo 6º. Entre la información que ha de suministrarse cuando se recaben datos personales cabe mencionar: su finalidad, quiénes pueden ser sus destinatarios, si se almacenarán o no en un archivo o registro, quién es el responsable del mismo, el carácter obligatorio o facultativo de las respuestas al cuestionario que se proponga, las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos y la posibilidad de ejercer los derechos de acceso, rectificación y supresión de los datos.

La reglamentación del Decreto 1.558/016 [6] en el artículo 5º aclara que la información se brindará adecuándose al nivel social y cultural de la persona y que *el órgano de control establecerá los requisitos para que el consentimiento pueda ser prestado por un medio distinto a la forma escrita, el cual deberá asegurar la autoría e integridad de la declaración. El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo. La revocación no tiene efectos retroactivos*.

Asimismo, la ley exceptúa la obtención de consentimiento en ciertos casos, a saber: cuando *a) los datos se obtengan de fuentes de acceso público irrestricto; b) se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526*. Hemos destacado el inciso "d" pues en ese punto se inscribiría la actividad médica [2].

El artículo 7º categoriza los datos y establece que ninguna persona puede ser obligada a proporcionar datos sensibles excepto que *medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares* [2]. Creemos que la investigación médica y epidemiológica encuadraría en este apartado.

Por su parte, el artículo 8º hace referencia explícita a los datos relativos a la salud y dice: *los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado*

 http://dx.doi.org/10.1590/1983-80422015232062

bajo tratamiento de aquéllos, respetando los principios del secreto profesional [2].

Este punto es importante en relación con la digitalización de la historia clínica, práctica que poco a poco se va imponiendo en nuestro medio. Sin embargo, nótese que la ley exige respetar el secreto profesional y es aquí donde deben centrase los esfuerzos informáticos para cumplir con este requisito.

Es así como el articulo 9º legisla sobre la seguridad de los datos: *El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad* [2].

En la misma línea, al artículo 10º menciona el deber de confidencialidad: *El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública* [2].

Finalmente, es interesante destacar que los datos personales no pueden ser cedidos a terceros salvo previo consentimiento revocable de su titular, a quien se le debe informar sobre la finalidad de la cesión e identificación del cesionario. El cesionario tiene las mismas obligaciones legales y reglamentarias del cedente y responde solidariamente por la observancia de las mismas ante el organismo de control y el titular de los datos.

Conforme al art. 11 de la Ley 25.326 [2], el consentimiento no es exigido cuando: *a) Así lo disponga una ley; b) En los supuestos previstos en el artículo 5º inciso 2 ; c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados; e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables*.

El artículo 5º inciso 2 de la ley [2] establece que no será necesario el consentimiento cuando: *a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526*.

El artículo 12 de la ley [2] se refiere a la transferencia internacional de datos y la prohíbe explícitamente cuando no se proporcionen niveles de protección adecuados. No obstante establece algunas excepciones y, entre ellas, el *intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior (Artículo 11, inciso e: Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables).*

El artículo 31 de la ley [2] hace mención de las sanciones administrativas y multas que, como hemos dicho al comienzo, dependerán de la normativa de cada jurisdicción en razón del federalismo. Por su parte, el artículo 32 es de aplicación en toda la Nación y establece las sanciones penales, a saber:

1. *Incorpórase como artículo 117 bis del Código Penal, el siguiente:*

   '1º Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

   2º La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

   3º La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

   4º Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones,

se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena'.

2. *Incorpórase como artículo 157 bis del Código Penal el siguiente:*

   'Será reprimido con la pena de prisión de un mes a dos años el que:

   1º A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

   2º Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley'.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años.

Consideraciones finales

El derecho a la intimidad no sólo debe ser entendido desde el punto de vista legal. La bioética y en especial el Principialismo se han ocupado de constituirlo como norma ética. Así, del principio de autonomía se derivan las reglas de privacidad, de confidencialidad y de consentimiento informado, todas ellas estrechamente vinculadas con las normas legales que hemos descrito.

El Principialismo entiende que el derecho a la privacidad salvaguarda el acceso, por parte de terceros y sin el consentimiento del sujeto, a la información sobre la persona, sus pertenencias y relaciones íntimas con amigos, pareja y otros. Tiene su principal fundamento en la autonomía, entendida como autogobierno. Así, una persona autónoma tiene derecho a no ser observada, tocada etc. y/o a que no se obtenga información sobre ella o su entorno íntimo sin su autorización; la invasión de su privacidad implicaría atentar contra su autonomía. Por su parte, si bien la regla de confidencialidad se relaciona con la de privacidad, no es exactamente idéntica. La bioética nos dice que *la información* X *es confidencial si y sólo si A revela* X *a B y B promete abstenerse de revelar* X *a cualquier otra persona C sin el consentimiento de A* [7].

En el marco de la disciplina ética suele distinguirse entre lo legal y lo legítimo, exigiéndose legitimidad ética a toda normativa legal. Asimismo, se sostiene que las personas deberían comportarse correctamente por convencimiento moral y no por el temor al castigo frente a una norma legal trasgredida. Lamentablemente este *desideratum* se cumple con poca frecuencia en nuestro medio y los legisladores se ven obligados a "reforzar", mediante leyes, los imperativos éticos que deberían guiar nuestra conducta por sí mismos.

Así las cosas, en el ámbito de la medicina, la confidencialidad tiene correlato legal con el secreto profesional tipificado en el artículo 156 del Código Penal [8]. Sin embargo, no siempre es respetado, justificándose su violación en la promoción de ciertas actividades, por cierto valiosas, como la educación médica o de la investigación.

Entramos aquí en un terreno de límites imprecisos entre los derechos individuales y los derechos de la sociedad, terreno históricamente conflictivo y marcado por ideologías contrapuestas y tesis opuestas sobre la teoría del Estado. La tendencia actual, tanto a nivel legal como bioético, consiste en priorizar los derechos de los pacientes y de las personal en general. El derecho positivo de los derechos humanos, el liberalismo y el pensamiento kantiano con su defensa de la persona como fin en sí mismo y nunca como medio para ningún fin – por más loable que ese fin fuera –, otorgan fundamento a esta inclinación de la balanza.

Una vez más, somos absolutamente conscientes de que la mirada ética es distinta a la legal, y que no siempre se verifica el correlato deseado entre una y otra: muchas veces el derecho positivo no es ético, y viceversa. Pero también sabemos que la Bioética es una transdisciplina, con afluentes varios, como la filosofía, la antropología, la sociología, la comunicación social y el derecho, entre otros y que, como saber transdisciplinario, no puede desarrollarse sobre una estructura reduccionista ni filosófica, ni legal. Sin duda abogamos por una construcción transdisciplinaria [8].

Sin embargo, y sin perjuicio de lo antedicho, en este trabajo ponderamos el discurso jurídico porque la realidad de los miembros del equipo de salud (médico, enfermeros, integrantes de comités de bioética) reclama este discurso en la toma de decisiones frente al paciente concreto. A la hora de *practicar* la Bioética se hace muy difícil sostener posturas teóricas legítimas pero ilegales [9]. Entendemos que este trabajo otorga herramientas concretas y obligatorias (por su legalidad) para que aquellos que debaten en la práctica sobre casos reales tengan instrumentos de trabajo útiles. Así, la Bioética "de escritorio" – teórica, formal y abstracta – se planta firmemente en el terreno de la acción.

 http://dx.doi.org/10.1590/1983-80422015232062

Una vez entendida la necesidad de contar con herramientas jurídicas para afrontar casos concretos, esperamos que este trabajo motive a los lectores a investigar lo propio en sus respectivos países. La Argentina tiene estrechísimos vínculos con Brasil y, junto con otros estados, participa del Mercado Común del Sur (MERCOSUR). Así, recibe año tras año ciudadanos de las jurisdicciones vecinas que deciden emprender sus vidas académicas, laborales y personales en territorio colindante. Lo mismo sucede con personas que migran de paraje en paraje temporalmente con fines turísticos. Todos ellos son potencialmente "pacientes" y pueden verse afectados por la legislación del país en que se encuentran como tales. A ello se suma la gran cantidad de estudios clínicos multicéntricos que se desarrollan conjuntamente en nuestros países. No escapa a la lógica que es absolutamente requirente conocer el marco jurídico que envuelve tal actividad.

Este trabajo es parte del proyecto Normativa Ética y Legal para la Investigación en Ciencias Sociales, Epidemiología Y Salud Pública UBACYT 2011-2014 GC, *desarrollado en el Instituto de Bioética de la Facultad de Medicina de la Universidad de Buenos Aires.*

Referências

1. Perellón C. Juramento Hipocrático. [Internet]. Buenos Aires: Ministério de Educación; 2001 [acesso 20 dez 2012]. Disponível: http://www.me.gov.ar/efeme/medico/juramento.html
2. Argentina. Ley nº 25.326, de 4 de octubre de 2000. Disposiciones generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Boletín Oficial. [Internet]. 2 nov 2000 [acesso 21 dez 2012];(29517):1. Disponível: http://www.infoleg.gov.ar/infolegInternet/verNorma.do?id=64790
3. Argentina. Constituición 1994. Ley nº 24.430, de 15 de diciembre de 1994. Ordénase la publicación del texto oficial de la Constitución Nacional (sancionada en 1853 con las reformas de los años 1860, 1866, 1898, 1957 y 1994). Buenos Aires; 1994.
4. Sola JV. Manual de derecho constitucional. Buenos Aires: La ley; 2010. p 604.
5. Sola JV. Op. cit. p. 603.
6. Argentina. Decreto 1.558, de 29 noviembre de 2001. Apruébase la reglamentación de la Ley nº 25.326. Principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Boletín Oficial. [Internet]. 3 dez 2001 [acesso 21 dez 2012];(29787):6. Disponível: http://www.infoleg.gov.ar/infolegInternet/verNorma.do?id=70368
7. Outomuro D. Manual de fundamentos de bioética. Buenos Aires: Magister EOs; 2004. p. 144-65.
8. Argentina. Ley 11.179, de 30 septiembre 1921. Código Penal. Boletín Oficial. [Internet]. 3 nov 1921 [acesso 21 dez 2012];(8300). Disponível: http://www.infoleg.gov.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#19
9. Outomuro D. Reflexiones sobre el estado actual de la ética en investigación en argentina. Acta bioethica. [Internet]. 2004 [acesso 21 dez 2012];10(1). Disponível: http://dx.doi.org/10.4067/S1726-569X2004000100011

Participação das autoras
As autoras trabalharam em conjunto tanto no levantamento bibliográfico e na análise crítica quanto na redação do artigo.

Recebido: 8.10.2014
Revisado: 21. 4.2015
Aprovado: 8. 5.2015