Derecho a la salud. Derecho a la vida privada. Protección de datos personales

TEDH, *Case of Y. G. v. Russia*, 30 de agosto de 2022

Por Facundo Gabriele[1]

1. Introducción. Antecedentes del caso

El presente trabajo se efectúa en virtud de la sentencia dictada por el TEDH en el caso Y.G. v. Rusia.

La trama en ciernes de los autos de referencia tiene que ver con una denuncia realizada por el ciudadano Y. G., residente de la ciudad de Moscú, quien en virtud de patologías médicas se atendía en el Centro Médico de Moscú.

En febrero del año 2011 un conocido del accionante le informó que había adquirido, en el Mercado Savelovskiy de Moscú, una base de datos en la que figuraban las condiciones de salud de este. Para verificar esta información, Y. G. compró un disco compacto que contenía una base de datos de dicho mercado.

La base de datos adquirida contenía datos sobre 213.355 personas registradas como residentes en Moscú; 203.604 personas registradas viviendo en otro lugar pero que habían habitado la ciudad en Moscú; y personas extranjeras que vivían en Moscú. También contenía información sobre 281 personas con VIH, 30 personas con SIDA y 750 personas con hepatitis.

1 Abogado (UADE). Diplomado Superior en Derecho de los Usuarios y Consumidores (UNS). Diplomado en Liderazgo y Análisis Político (CIAS). Especializando en Derecho Administrativo y Administración Pública (UBA). Prosecretario Administrativo en la Unidad Especializada en Relaciones de Consumo del Ministerio Público de la Defensa del Poder Judicial de la Ciudad Autónoma de Buenos Aires.

Y. G. fue registrado en la base de datos y la información sobre él que allí se encontró fue: (1) su nombre y apellido; (2) fecha y lugar de nacimiento; (3) nacionalidad; (4) lugar de residencia y domicilio; y (5) una condena que había transitado por vandalismo, robo y posesión ilegal de drogas. En el apartado titulado "Notas", se decía que Y. G. era "un gamberro, ladrón y drogadicto, padecía sida y hepatitis", entre otros datos.

Es importante resaltar que esta base se correspondía a datos pertenecientes a diferentes organismos del Estado ruso y que se comercializaba como "Base de datos del Centro de Información del Departamento del Interior de Moscú".

En virtud de ello, Y. G. requirió que el Centro de Información aclarara por qué su base de datos contenía información sobre su estado de salud y que se eliminara la información sobre que padecía SIDA (ya que no era cierto), como así también con relación a la hepatitis, ya que no había dado consentimiento para la divulgación de dicho dato.

Ante dicha solicitud, el Centro de Información negó los hechos.

El demandante eleva una queja ante el Comité de Investigación de la Federación Rusa, que entendió que los asuntos denunciados no eran de su competencia, por lo que remitió el caso al Fiscal General, y este al Fiscal de Moscú, que consideró que no existían pruebas de que alguno de los funcionarios del Departamento del Interior de Moscú hubiera comedio un delito.

Por lo tanto, en agosto del 2011 el Tribunal de la ciudad de Moscú desestimó la demanda judicial, sin ningún tipo de investigación.

Ante ello, el señor Y. G. presentó una demanda ante el TEDH, en la que acompañó artículos de noticias de medios rusos (los cuales no fueron cuestionados por el gobierno ruso), de los que se desprendía que la Federación Rusa –luego de la denuncia realizada por Y. G.– llevó a cabo procedimientos en el mercado Savelovskiy que revelaron la venta ilícita de base de datos de varios organismos estatales que contenían información sobre ciudadanos de la Federación Rusa.

2. Marco jurídico aplicable en materia de datos personales

El Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales (Convenio 108), del 28 de enero de 1981, que entró en vigencia para la Federación Rusa el 1 de septiembre del año 2013, define en su artículo 2.a. los "datos personales" como "cualquier información relativa a una persona física identificada o identificable ("sujeto de datos").

En lo que aquí nos interesa, establece lo siguiente:

> Artículo 5. Calidad de los datos. Los datos de carácter personal que sean objeto de un tratamiento automatizado: a) Se obtendrán y tratarán leal y legítimamente; b) se registrarán para finalidades determinadas

y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; d) serán exactos y si fuera necesario puestos al día; e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Artículo 6. Categorías particulares de datos. Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales.

Artículo 7. Seguridad de los datos. Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Artículo 8. Garantías complementarias para la persona concernida. Cualquier persona deberá poder: a) conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero; b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio; d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.

Artículo 9. Excepción y restricciones 1. No se admitirá excepción alguna en las disposiciones de los artículos 5, 6 y 8 del presente Convenio, salvo que sea dentro de los límites que se definen en el presente artículo. 2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática: a) para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales; b) para la protección de la persona concernida y de los derechos y libertades de otras personas. 3. Podrán preverse por la ley restricciones en el ejercicio de los derechos a que se refieren los párrafos b), c) y d) del artículo 8 para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.

Artículo 10. Sanciones y recursos. Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

3. El fallo del TEDH

El TEDH admitió la demanda entendiendo que existió una violación del Convenio (en particular del artículo 8, por lo que condenó a la Federación Rusa a abonar al accionante –dentro de los tres meses de que la sentencia adquiera firmeza– el equivalente a moneda del Estado demandando de 7.500 euros, más el importe de 2.000 euros, más cualquier otro impuesto que pudiera corresponder, en concepto de costas y gastos.

En primer lugar, cabe poner de resalto que la información personal relacionada con un paciente pertenece a su vida privada y, como tal, debe ser respetada.

Por otro lado, en el presente caso no ha sido discutido que la base de datos adquirida por el accionante en un mercado de Moscú contenía recopilación de los datos personales del solicitante (incluidos datos de su salud), como así también de miles de personas más. Por ende, el presente caso cae dentro de la esfera de la vida privada del señor Y. G., que como tal debe ser protegida.

Tampoco se encontraba discutido que los datos de salud de Y. G. se habían registrado en la base de datos del Ministerio del Interior de Moscú en el año 1999, después de que el Hospital de Enfermedades Infecciosas de esa misma ciudad se los proporcionara. La base de datos comprada por el solicitante en el mercado había pertenecido al Ministerio del Interior, ya que contenía información que solo podía ser conocida por este.

Así, no puede obviarse que la protección de los datos personales, en particular los datos médicos, son de fundamental importancia para que una persona goce de su derecho al respeto de la vida privada y familiar garantizado por el artículo 8 del CEDH, entre otros.

Por otra parte, es dable resaltar que las autoridades estatales tienen la obligación de investigar este tipo de denuncias, máxime cuando la información "filtrada" se da por datos con los que –solo ellos– contaban. Por lo que el Estado encuentra comprometida su responsabilidad, sin resultar necesario analizar si hubo dolo o culpa en esa filtración.

Es un agravante el hecho de que las autoridades públicas nunca hayan investigado el asunto. Por lo tanto, hubo una falta en la obligación positiva de garantizar una protección adecuada del derecho del demandante al respeto de su vida privada.[2]

No solo es doloroso ver tus datos personales comercializarse sin ningún tipo de control en un mercado de tu ciudad, sino que la indignación se acrecienta cuando ese dato comercializado, no solo indefectiblemente estaba en custodia del Estado, sino que además, ante la denuncia del hecho, ese mismo Estado que tiene el deber de custodia y cuidado, no investiga dicha denuncia.

La gravedad aumenta, ya que no solo no investigó la denuncia realizada por Y. G. el Poder Ejecutivo de la Federación Rusa, sino tampoco, el Poder Judicial.

2 TEDH, *Case of Y. G. v. Russia*, Application N° 8647/12, Court (Third Section), 30 de agosto de 2022, párr. 51.

4. A modo de cierre

Es de vital trascendencia realizar acciones tendientes a respetar la confidencialidad de los datos relacionados con el derecho a la salud, ya que todos los ordenamientos jurídicos lo han incorporado como un principio vital.

A su vez, es crucial no solo respetar el sentido de privacidad de una persona, sino también –y creo que con este fallo queda bien establecido– es obligación del Estado preservar la confianza de los ciudadanos en la profesión médica y en los servicios de salud en general. Caso contrario, nadie estaría seguro de que sus datos no puedan ser divulgados, con el riesgo que ello podría significar: disuadir a los ciudadanos/as a acercarse a los centros médicos en busca de un diagnóstico o tratamiento por miedo a su publicidad.

En particular, los datos de salud son extremadamente sensibles, de los más. Así, las enfermedades como el SIDA o la hepatitis tienen grave potencialidad discriminatoria y son datos que deben registrase con métodos de codificación o encriptamiento que restrinjan al máximo posible su acceso.

Es dable poner de resalto

> [e]l alto impacto que ha tenido –y aún tiene– la presencia del SIDA en nuestra sociedad ha generado reacciones que afectaron prácticamente todos los derechos humanos. Por ello, por primera vez en la historia, una estrategia de lucha contra una enfermedad incluye la promoción y protección de los derechos humanos. Así, la lucha contra el SIDA es también una lucha contra el miedo, contra el prejuicio y contra las acciones irracionales nacidas de la ignorancia, porque estas son las causas de algunas de las violaciones más críticas de los derechos humanos.[3]

A su vez, toda información referida a la salud de una persona merece un doble nivel de protección. Así, su recolección, conservación, ordenamiento, almacenamiento, modificación, bloqueo, destrucción y, en general, todo tipo de procesamiento, debe realizarse conforme a los principios de calidad, consentimiento e información.

El fallo aquí comentado resulta un gran avance en el reconocimiento, no solo de acudir a tribunales internacionales en defensa de violaciones legales realizadas por los Estados a sus ciudadanos, sino también porque pone énfasis en la protección de los datos personales de los individuos y reconoce la obligación del Estado de investigar denuncias de estos tipos; caso contrario, su responsabilidad por los daños causados es total.

3 Cahn, P.; Bloch, C. y Weller, S. (1999). *El sida en la Argentina. Epidemiología, subjetividad y ética social.* Buenos Aies: Arkhetypo, p. 140.