Protección de datos personales. Investigación penal

TEDH, *Case of Gaughran v. United Kingdom*, 13 de febrero de 2020

Por Juan Agustín Otero[1] *y Mauro Meloni*[2]

I. Introducción

Es innegable que existe una tensión activa entre el derecho a la privacidad y el deber que tiene todo Estado de prevenir, perseguir y, eventualmente, castigar los delitos tipificados por ley. La puja entre privacidad y seguridad permea debates jurídicos y éticos en todo el mundo e incide en regulaciones tanto locales como internacionales. Pero los resultados de esa puja no siempre han sido equilibrados. Como señala Solove (2011),

> con frecuencia, la privacidad es injustamente vencida por la seguridad. Las personas entienden los intereses asociados a la seguridad sin mayores dificultades porque la vida y el cuerpo están en juego. En cambio, los derechos vinculados a la privacidad resultan más difusos y abstractos. Muchos piensan que deben ceder su privacidad para estar más seguros.[3]

1 Abogado (UDESA). Profesor de Ética (UDESA). Asesor Legal en la Agencia de Acceso a la Información Pública.
2 Abogado (UDESA). Asesor Legal en la Agencia de Acceso a la Información Pública.
3 Véase Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff between Privacy and Security*. Londres: Yale University Press, p. 2. La traducción de la cita es nuestra.

Afortunadamente, la balanza se ha ido inclinando hacia el centro en los últimos años. El uso cotidiano de nuevas tecnologías que extraen y procesan información ha colocado a los ciudadanos de todo el mundo en una situación de vulnerabilidad sin precedentes, pero también ha obligado a los reguladores a desarrollar soluciones legales que se adapten a los nuevos tiempos. En este contexto, el derecho a la privacidad ha ganado mayor visibilidad, sobre todo a través de una de sus vertientes más modernas: el derecho a la protección de los datos personales.

Desde que la Directiva de Protección de Datos de la Unión Europea[4] entró en vigor en 1998, el peso específico del derecho a la privacidad en su ya histórica pugna con la seguridad solo ha ido en aumento. Prueba de ello es que, actualmente, los Estados miembros del Convenio de Ciberdelito –entre los que se encuentra la Argentina– se encuentran discutiendo un Segundo Protocolo Adicional en el que establecerían salvaguardas de protección de datos personales que condicionarían el libre intercambio de información entre las autoridades de aplicación de la ley penal de los distintos países.[5]

Otro ejemplo, no menos notable, es el caso "Gaughran c. Reino Unido" que aquí comentamos, en el que el TEDH declaró que la política de retención de datos personales del Servicio de Policía de Irlanda del Norte violaba el derecho a la privacidad contemplado en el artículo 8 del Convenio para Protección de Derechos Humanos y de las Libertades Fundamentales (CEDH). En particular, el Tribunal destacó la necesidad de equilibrar las políticas de seguridad con salvaguardas que aseguren a los individuos un plazo determinado en la conservación de sus datos por parte de las autoridades policiales. Asimismo, consideró que era imperativo tomar otros recaudos, tal como la posibilidad de ejercer una acción de revisión real y efectiva.

Entendemos que el análisis de esta sentencia es relevante para la Argentina por dos razones. En primer lugar, a diferencia de los países de la Unión Europea, que han discutido y aprobado normativas específicas sobre el uso de datos personales por parte de autoridades públicas con fines de aplicación de la ley penal, Argentina solo cuenta con reglas generales de protección de datos personales, con las garantías genéricas de los Códigos Procesales Penales y con la antigua Ley N° 22117 que regula el Registro Nacional de Reincidencia. Por el momento, la Agencia de Acceso a la Información Pública –Autoridad de Control de la Ley N° 25326 de Protección de Datos Personales– no se ha expedido en profundidad sobre la puja entre privacidad y seguridad. Tampoco lo ha hecho la Corte Suprema de Justicia de la Nación.

En segundo lugar, el TEDH es el máximo órgano jurisdiccional del CEDH. Si bien la jurisprudencia emanada del TEDH no es vinculante para Argentina, entendemos que sus decisiones deberían orientar la interpretación local de las garantías de datos personales que surgen del convenio firmado por Argentina, en particular, la futura versión del Convenio de Ciberdelito y el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108).[6]

4 Directiva 95/46/CE del Parlamento Europeo y del Consejo.

5 Convenio de Ciberdelito, adoptado en Budapest, Hungría, el 23 de noviembre de 2001 (comúnmente denominado "Convenio de Budapest"), ratificado por Argentina en 2017 mediante la Ley N° 27411.

6 A través de la Ley N° 27483, Argentina aprobó la ratificación del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, instrumento adoptado por los Estados miembro del Consejo de Europa en 1981. Junto con el Protocolo Adicional al Convenio para

A la luz del debate entre el derecho a la privacidad y el deber que tiene el Estado de prevenir el delito, en este artículo procuraremos: (i) describir la sentencia del TEDH en el caso "Gaughran c/ Reino Unido"; (ii) considerar cómo el caso podría haber sido resuelto bajo el derecho argentino de protección de datos personales, estableciendo una comparación con la solución del TEDH; y (iii) relevar los problemas que existen en las políticas argentinas de conservación de datos con el fin de prevenir, perseguir y castigar delitos. En particular, a lo largo del artículo, veremos cómo la colisión entre la privacidad y la seguridad, en ocasiones, puede ser resuelta equilibrando los derechos en juego, por medio de una solución intermedia.

Pensamos que un correcto entendimiento de este fallo puede resultar útil para informar futuras políticas públicas sobre el tratamiento de datos personales con fines de aplicación de la ley penal en Argentina.

II. Hechos del caso

El Sr. Fergus Gaughran fue arrestado en octubre de 2008 por conducir alcoholizado, delito considerado como "registrable"[7] bajo la legislación del Reino Unido. Según surge de la sentencia, los "delitos registrables" son aquellos que producen un antecedente penal. En otras palabras, la policía debe mantener un registro de los "delitos registrables" en los que incurrió cada ciudadano; en su gran mayoría, estos delitos son punibles con pena de prisión.

Después de ser arrestado, el Sr. Gaughran fue llevado a una comisaría, donde proporcionó una muestra de aliento (que resultó positivo), su fotografía, huellas dactilares y una muestra de ADN. En noviembre de 2008 se declaró culpable, recibió una multa y se le prohibió conducir por doce meses. Conforme a lo dispuesto por la legislación relevante, cumplió su condena formalmente luego de cinco años, en noviembre de 2013.

En enero de 2009, dos meses después de declararse culpable, el Sr. Gaughran solicitó al Servicio de Policía de Irlanda del Norte (PSNI) que o bien le devolviera o bien destruyera los datos personales que en su momento había recolectado. En febrero de 2009 el PSNI denegó el requerimiento del Sr. Gaughran.

En el año 2015 el PSNI destruyó la muestra de ADN del Sr. Gaughran. Hasta la fecha del dictado de la sentencia del TEDH, el PSNI continuaba reteniendo de forma indefinida el perfil de ADN de forma digital extraído de su muestra de ADN, sus huellas dactilares y su fotografía.

En consecuencia, el Sr. Gaughran cuestionó la retención indefinida de sus datos por parte del PSNI en los tribunales nacionales. Alegó que constituía una interferencia injustificada a su derecho al respeto de su vida privada y familiar, consagrado en el artículo 8 del CEDH.

la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal adoptado en Estrasburgo en 2001, ambos instrumentos son comúnmente denominados conjuntamente "Convenio 108". Asimismo, recientemente Argentina firmó otro instrumento del Consejo de Europa, el Protocolo Adicional que modifica el Convenio 108 (que resulta en el denominado "Convenio 108+" o "Convenio 108 Modernizado").

7 TEDH, *Case of Gaughran v. United Kingdom*, Application no. 45245/15, 13 de febrero de 2020, párr. 6.

De este modo, solicitó a la Alta Corte de Justicia de Irlanda del Norte: (a) una declaración de que la retención indefinida de los datos era ilegal y constituía una interferencia injustificable con su derecho a la privacidad; y (b) una orden de prohibición que impida al demandado hacer uso de los datos relevantes.

En noviembre de 2012, la Alta Corte estableció que, si bien la retención indefinida de los datos biométricos del solicitante constituía una interferencia bajo el artículo 8 del CEDH, estaba justificada y no era desproporcionada. Frente a un recurso del Sr. Gaughran, la Corte Suprema de Reino Unido se expidió en 2015, concluyendo que la política de retención de datos del PSNI era proporcional. Así, ratificó la sentencia previa de la Alta Corte.

III. Decisión y argumentos del TEDH

En esta instancia, el Sr. Gaughran reiteró los argumentos expuestos en sede interna y sostuvo que la retención indefinida de sus datos biométricos y fotografía constituía una medida desproporcionada que no podía justificarse bajo el presupuesto de que no afectaba a la mayor parte de los ciudadanos.

El Gobierno de Reino Unido aceptó que la retención indefinida de los datos del Sr. Gaughran constituía una interferencia con sus derechos, pero argumentó que era una interferencia "de muy baja intensidad".[8] Así, el Gobierno sostuvo que estaba amparada en la ley doméstica y que dicha ley era accesible y sus consecuencias podían ser previstas por los ciudadanos. Adicionalmente, argumentó que la retención de los datos biométricos y la fotografía del Sr. Gaughran tenía el fin legítimo de mejorar la "prevención de las infracciones penales", previsto específicamente en el artículo 8, inciso 2 del CEDH como una excepción al derecho a la privacidad.

Asimismo, argumentó que constituía una medida razonable y proporcional, ya que el Reino Unido goza de un amplio margen de apreciación para regular internamente el derecho consagrado en el artículo 8 del CEDH. Ello así, en primer lugar, porque no existía un consenso fuerte entre los Estados sobre cómo regular la retención de datos biométricos de personas condenadas por cometer un delito. En segundo lugar, porque el régimen de retención de datos de Irlanda del Norte no es inusualmente intrusivo a la privacidad comparado con otros Estados de jurisdicciones europeas que también prevén la retención de datos biométricos, y en algunos casos, de muestras de ADN, por períodos de tiempo indefinidos o a veces muy extensos, como, por ejemplo, durante la vida de la persona que haya cometido el delito. En tercer lugar, el régimen previsto en Irlanda del Norte únicamente prevé la recolección de esos datos en casos de delitos registrables, es decir, delitos cuya pena implica el encarcelamiento de la persona condenada. Por último, el Gobierno sostuvo que la retención de datos biométricos y fotografías constituye una herramienta muy valiosa para combatir el crimen, particularmente teniendo en cuenta que las estadísticas de Irlanda del Norte demuestran que existe un alto porcentaje de reincidencia dentro de los primeros dos años de haberse cometido el primer delito.

8 Ídem, nota 7, párr. 61.

Vistos los argumentos de las partes, el TEDH consideró que la retención de datos personales del Sr. Gaughran constituía una interferencia en su vida privada, no solo por la doctrina previamente sentada en "S. y Marper c/ Reino Unido" (2008),[9] sino también porque –como se expuso antes– ese hecho había sido pacíficamente aceptado por las partes de la controversia.

En particular, el TEDH consideró oportuno aclarar que la retención de la fotografía del Sr. Gaughran era tan intrusiva como la de su perfil de ADN y sus huellas dactilares. El Tribunal precisó que la retención indefinida de la fotografía, sumada a la posibilidad eventual de aplicarle una tecnología de reconocimiento facial (aun cuando dicha aplicación se efectuase por fuera de la base de datos original), configuraba una vulneración del artículo 8 del CEDH.

Ahora bien, determinar la existencia de una interferencia con la vida privada del Sr. Gaughran no es equivalente a demostrar que es injustificada. Por eso, en un segundo término, el Tribunal procuró demostrar que el accionar del PSNI configuraba una infracción infundada del tratado. Si bien acordó con el Gobierno que la retención de datos de personas que hayan cometido "delitos registrables" era una medida amparada en la legislación doméstica y que perseguía un fin legítimo, también consideró que no podía realizarse sin tomar ciertos recaudos y salvaguardas para proteger la privacidad de las personas.

Así, el TEDH estableció que, aun cuando existe un margen de apreciación del que dispone cada Estado miembro para reglamentar las excepciones al artículo 8 del CEDH, la extensión de dicho margen depende de dos factores. Por un lado, cuando una dimensión importante de la vida o la identidad de un individuo se encuentra afectada, el margen de apreciación es más bien estrecho. Por el otro, cuando no haya un consenso entre los Estados miembros sobre qué peso asignarle al derecho afectado o cómo protegerlo, el margen es más amplio.

Como se narró antes, el Reino Unido arguyó que la retención indefinida efectuada por el PSNI estaba justificada porque no había consenso entre los Estados miembros sobre cómo y en qué circunstancias conservar los datos biométricos de una persona condenada por un delito. Esa afirmación, de acuerdo al TEDH, se basó en la suposición del Gobierno de que un régimen que prevé la retención de datos durante la vida biológica o la vida biológica más un cierto número de años es comparable a un régimen de retención indefinida. Sin embargo, el Tribunal expresó que, para determinar si ambos regímenes eran equiparables, debía evaluarse la naturaleza de los datos recolectados y el impacto de retenerlos después de la muerte de su titular.

En relación con las huellas dactilares, el Tribunal expresó que esta categoría de datos no revela tanta información como los perfiles de ADN. Además, hasta el momento, no se ha sugerido que sea posible identificar relaciones entre individuos a partir de datos de huellas dactilares o fotografías. Por lo tanto, el Tribunal aceptó que, en relación con las huellas dactilares y las fotografías, los períodos de retención que terminan poco después de la muerte podrían considerarse comparables a la retención indefinida.

9 TEDH, *Case of S. and Marper V. The United Kingdom*, Applications nos. 30562/04 and 30566/04, 4 de diciembre de 2008. Allí el TEDH determinó que la retención de huellas dactilares, celulares, muestras y perfiles de ADN de personas sospechosas, pero no condenadas, constituía una interferencia desproporcionada con el derecho a la privacidad de las personas.

Ahora bien, el Tribunal explicó que la situación es diferente con respecto a los perfiles de ADN. Hay una distinción entre retener estos perfiles indefinidamente y establecer un límite al período de retención vinculado a la vida biológica de la persona en cuestión. Esto se debe a que la retención de datos genéticos después de la muerte del titular de los datos continúa afectando a los individuos biológicamente relacionados con el interesado, es decir, a sus parientes cercanos.

Adicionalmente, el TEDH precisó que solo hay un pequeño número de Estados miembro que operan regímenes de retención indefinidos. La mayoría tienen plazos determinados de conservación de la información biométrica.

Sin perjuicio de lo anterior, concluyó que, con respecto a los regímenes de retención de los datos biométricos de las personas condenadas, la duración del período de retención es un factor entre otros para evaluar si un Estado ha sobrepasado margen de apreciación aceptable. También es importante que el régimen de retención tenga en cuenta la gravedad del delito y establezca un *test* respecto de la necesidad de conservar los datos, disponiendo de acciones disponibles para el individuo. Cuando un Estado pretende reglamentar y, de ese modo, limitar el alcance de los derechos establecidos en el CEDH, la existencia y el funcionamiento de ciertas salvaguardas se vuelven decisivos.

En cuanto a si las razones aducidas por las autoridades nacionales para justificar la medida de retención indefinida fueron "relevantes y suficientes", el Tribunal señaló que el Reino Unido afirmó que cuantos más datos se conserven, más se evitará el delito, proporcionando pruebas para apoyar esa afirmación general.[10] El Tribunal juzgó que aceptar dicho argumento en el contexto de un esquema de retención indefinida equivaldría en la práctica a justificar el almacenamiento de información sobre toda la población y sus familiares fallecidos, lo que definitivamente sería excesivo.

Habiendo optado por establecer un régimen de retención indefinida, el Tribunal consideró que era necesario que Reino Unido garantizara acciones y salvaguardas reales y efectivas para los individuos. Sin embargo, los datos biométricos y las fotografías del Sr. Gaughran se conservaron sin referencia a la gravedad de su delito y sin tener en cuenta la necesidad real de conservar esos datos indefinidamente. La policía solo tenía la potestad de eliminar datos biométricos y fotografías en circunstancias excepcionales. Además, no existía ninguna disposición que permitiese al Sr. Gaughran solicitar que se eliminasen sus datos si la conservación ya no parecía necesaria en vista de la naturaleza del delito, la edad, el período de tiempo transcurrido o el estado actual de la persona en cuestión.

Por las razones expuestas, el Tribunal consideró que la petición era procedente en razón de la naturaleza indiscriminada de la retención del perfil de ADN, las huellas dactilares y la fotografía del Sr. Gaughran. El TEDH estimó que el régimen cuestionado no había tenido en cuenta la gravedad del delito ni la necesidad real de efectuar una retención indefinida y, en ausencia de una posibilidad real de revisión, no había logrado un equilibrio justo entre los intereses públicos y privados en juego.

10 Ídem, nota 7, párr. 89.

En consecuencia, juzgó que el Estado demandado había sobrepasado el margen de apreciación aceptable a este respecto y la retención en cuestión constituía una interferencia desproporcionada con el derecho a la privacidad del Sr. Gaughran.

IV. El caso "Gaughran c/ Reino Unido" en Argentina

Creemos que, en la Argentina, una interpretación razonable de la Ley N° 25326 de Protección de Datos Personales (LPDP) habría ofrecido una solución similar a la del TEDH. Es indudable que la solicitud del Sr. Gaughran habría sido tramitada como el ejercicio de un derecho de supresión bajo el artículo 16, inciso 1 de la LPDP, que establece que "[t]oda persona tiene derecho a que [cuando corresponda] sean suprimidos [...] los datos personales de los que sea titular, que estén incluidos en un banco de datos".

Por su parte, bajo el derecho local, el PSNI habría opuesto las excepciones contenidas en los artículos 16, inciso 5, y 17, inciso 1 de la LPDP para negarse a borrar la información retenida. La primera norma sostiene que "[l]a supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos". La segunda que

> [l]os 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.

A su turno, con respecto a las huellas dactilares y los datos identificatorios del Sr. Gaughran, el PSNI habría invocado el artículo 7 de la Ley N° 22117 que regula el Registro Nacional de Reincidencia y que establece que

> [l]as comunicaciones y fichas dactiloscópicas [de las personas que cometan delitos] integrarán los legajos personales, que bajo ningún concepto podrán ser retirados del Registro. Estos sólo serán dados de baja en los siguientes casos: (a) Por fallecimiento del causante; (b) Por haber transcurrido cien (100) años desde la fecha de nacimiento del mismo.

Como se expresó en las Resolución N° 1/2020 y N° 191 de la Agencia de Acceso a la Información Pública, las excepciones al derecho de supresión previstas en el artículo 16, inciso 5 y artículo 17, inciso 1 de la LPDP suponen la necesidad "de realizar una ponderación de los intereses y derechos que están en juego". En este caso, del derecho a la privacidad del Sr. Gaughran junto con la finalidad legítima de prevenir, perseguir y castigar delitos en cabeza del PSNI.

Un adecuado equilibrio entre los dos valores en pugna indica que es razonable que las autoridades de aplicación de la ley penal conserven los datos de las personas que hayan cometido delitos para optimizar la identificación en caso de reincidencia. Ello así en la medida en que la conservación de los datos cumpla con el artículo 4, incisos 1 y 7 de la LPDP, que establecen respectivamente que "[l]os datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido" y que "[l]os datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados". Adicionalmente, ha de tenerse en cuenta que el artículo 23 de la LPDP especifica que "[l]os datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

De las normas precedentes, que establecen principios de carácter general, es necesario extraer, por medio de la interpretación, salvaguardas concretas. En este caso, estimamos que el plazo de conservación debe estar limitado en el tiempo; que su duración debe ser razonable; que debe tenerse en cuenta la gravedad del delito para ver si es necesario registrarlo y por cuánto tiempo; y, por último, que se tiene que garantizar que el ciudadano tendrá una instancia de revisión real cuando ejerza su derecho de supresión ante las autoridades penales.

Sin embargo, en relación con las huellas dactilares y la identidad de los criminales registrados, la ley argentina, por un lado, no discrimina entre delitos registrables y no registrables, por lo que no hace diferencias en razón de la gravedad del ilícito; y, por otro, establece un plazo determinado, pero excesivo, que dura cien años o la totalidad de la vida biológica del titular de los datos. En relación con el perfil de ADN, el derecho local no prevé plazos de duración para la conservación de esta información, por lo que el accionar del PSNI es más bien discrecional.

Por todo lo expuesto, consideramos que el derecho de supresión del Sr. Gaughran sería procedente y que el derecho de protección de datos personales vigente es apto para resolver el caso en términos similares a los expresados por el TEDH. No obstante, la situación legal argentina está lejos de ser la ideal. En primer lugar, el derecho vigente carece actualmente de disposiciones específicas sobre la retención de datos personales por parte de autoridades de aplicación de la ley penal. En segundo lugar, con respecto a las huellas dactilares y los datos identificatorios del titular, el plazo establecido por el artículo 7 de la Ley N° 22117 es excesivo y no guarda un equilibrio entre la privacidad de las personas y el interés en prevenir, perseguir y castigar delitos. En tercer lugar, no se encuentra establecido el plazo de conservación de las muestras y perfiles de ADN –entre otros datos que podrían ser considerados sensibles–. En cuarto y último lugar, debería modificarse la Ley N° 22117 de modo que establezca una diferencia entre delitos registrables y no registrables en orden a su gravedad.

V. Conclusión

Si bien el derecho argentino cuenta con reglas generales de protección de datos personales, no existen normas específicas y modernas en el ámbito de las autoridades de prevención y aplicación de la ley penal. La Ley N° 22117 resulta obsoleta y los Códigos Procesales Penales vigentes no establecen normas claras sobre la retención y tratamiento ulterior de datos derivados de las investigaciones penales.

El caso "Gaughran c/ Reino Unido" es un antecedente internacional que indica que sería conveniente que se legislaran salvaguardas concretas relativas a: (i) los plazos por los cuales la información puede ser guardada por las autoridades; (ii) las razones por las cuales dicha información debe ser guardada, discriminando los delitos por su gravedad; y (iii) distintos regímenes de almacenamiento para distintas categorías de datos, según el grado de intrusión en la privacidad de las personas.

No obstante, a nuestro juicio, el fallo del TEDH no desarrolla en profundidad el *quid* del caso. Esto es, no examina en detalle las consecuencias gravosas que la existencia y la eventual divulgación de un registro de delitos puede tener sobre las personas registradas, en particular, sobre su vida profesional y familiar. Tampoco tiene en cuenta que existe un derecho de acceso a la información pública que puede justificar que se instaure un plazo de conservación extenso para asegurar el control de las instituciones y de los funcionarios encargados de aplicar la ley penal. En futuros trabajos, sería interesante evaluar este aspecto en los fallos del TEDH y en la jurisprudencia argentina.