PRINCIPIO DE FINALIDAD Y RETENCIÓN DE DATOS EN EL MINISTERIO PÚBLICO

SCS 23 DE MAYO DE 2023, ROL N° 51.809-23

MATÍAS ARÁNGUIZ VILLAGRÁN[1]

RESUMEN. En este comentario se analiza la sentencia de la Corte Suprema de mayo de 2023, que rechaza la apelación de un recurso de protección que se presentó contra la Fiscalía Regional de La Araucanía, debido a que el recurrente, que había sido sobreseído en 2021 por el Juzgado de Garantía, mantenía la calidad de imputado en la causa consultada en el Registro del Sistema de Información y Atención a Usuarios. En el trabajo se analiza el funcionamiento del Sistema de Apoyo a los Fiscales (registro SAF), la interpretación respecto del tratamiento de datos que han hecho los Tribunales de justicia, cuestionándose la legalidad del tratamiento de esos datos de acuerdo a los estándares de garantía de derechos fundamentales e internacionales en materia de protección de datos personales.

PALABRAS CLAVE. Registro del Sistema de Información y Atención a Usuarios del Ministerio Público; protección de datos; derecho a la privacidad; dignidad de la persona; retención de datos; juicio objetivo.

> No system of mass surveillance has existed in any society that we know of to this point that has not been abused[2].
>
> Edward Snowden
>
> [Data retention] represents a greater threat to democracy than it does to criminals[3].
>
> Roger Clarke

---

1 Profesor asistente de Derecho, Pontificia Universidad Católica de Chile. Correo electrónico: matias.aranguiz@uc.cl. Agradezco el trabajo de revisión jurisprudencial hecha por el investigador Christian Yepsen del Programa Derecho, Ciencia y Tecnología UC y de los comentarios y conversaciones con los abogados Iván Meleda y Belen Huaracán.

2 Snowden (2014).

3 Clarke (2015) p. 121.

1. INTRODUCCIÓN

Es común entre los especialistas en materia de protección de datos personales repetir sobre la inadecuación a nuestros tiempos de la frase «quien nada hace, nada teme». Dicha frase se sustenta en la idea de justicia y causalidad: si nada malo he hecho, nada malo puede ocurrirme. Presume que el mundo es justo y que nadie puede escapar a ello. Usando el argumento contrario, el dicho popular presume que quien ha hecho algo, debe temer. Los temores deberían venir de aquellos casos en donde sí se ha hecho algo indebido.

Sin embargo, la época de la información permite que dicha presunción de justa causalidad no sea del todo justificada. La acumulación de información permite ganar poder sobre individuos. En la era de la información no se requiere haber hecho algo malo para ser víctima de manipulaciones o extorsiones, la información acumulada de una persona abre flancos de riesgos. En los casos en que existe suficiente información, es fácil predecir el actuar de un individuo en base a sus acciones u omisiones, perfilar según las preferencias y, en caso de ser mal administrados, poner en riesgo la dignidad de la persona por medio de una filtración de sus datos.

En un contexto de sobreexposición digital, la dignidad de las personas, manifestada en cada una de las huellas que vamos dejando en nuestro interactuar electrónico, peligra. Cada vez que damos un *like*, compartimos una foto o miramos más un *post* que otro estamos alimentando algún sistema informático con nuestras preferencias. Siempre estamos siendo observados y cada momento en que interactuamos con un dispositivo inteligente, nuestros datos son capturados.

Bajo la amenaza de daño al individuo en su libertad, privacidad y autodeterminación es que el derecho ha respondido con la protección de datos personales. Inicialmente pensado como un derecho frente al Estado y la acumulación de información que este tenía de sus ciudadanos, hoy ha evolucionado a un derecho frente a cualquiera, en donde es el individuo o titular quien tiene control sobre su información en aquellos casos en que sus intereses no chocan con bienes jurídicos mayores. Este derecho se manifiesta en un sentido positivo, en la autodeterminación informativa, y en su sentido negativo, por los requisitos y limitaciones que se impone a todos quienes tratan datos o intentan hacerlo.

Recientemente, la Constitución Política de la República incorporo el año 2018 al artículo 19 N° 4[4] la garantía de la protección de los datos personales. Este derecho busca resguardar la dignidad de la persona humana en contexto digitales. Toda

[4] Constitución Política de Chile, Artículo 19 N°4: "El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".

proyección de información que emane de una persona es, por extensión, parte de esta y, por tanto, la protección de los datos personales es un resguardo de la esencia del ser humano. La importancia de la protección de datos personales es, en el contexto de una vida digitalizada, en extremo relevante puesto que cada interacción humana con plataformas o dispositivos electrónicos deja huellas en forma de datos.

En este trabajo discutiremos sobre uno de esos casos en donde, en mi impresión, es necesario actualizar la interpretación que tienen los tribunales de justicia y adecuar el funcionamiento institucional del registro (o "base de datos") que mantiene el Ministerio Público (o "Fiscalía"), de personas que han participado en procesos penales como imputados, pero que finalmente no han sido condenadas. Cuestionaremos la legalidad del tratamiento de esos datos y los intentaremos adecuar a los estándares de garantía de derechos fundamentales e internacionales en materia de protección de datos personales.

Analizaremos el funcionamiento del Registro del Sistema de Información y Atención a Usuarios (en adelante SAF), para luego tomar como referencia las decisiones de la tercera sala de la Corte Suprema y la evolución, de parte de sus miembros, que incorpora una visión moderna de la protección de la dignidad humana en contextos digitales, desde el entendido de la protección de datos personales. Posteriormente se analizarán decisiones insignes del continente europeo, para con tal conocimiento, avanzar a la caracterización de los principios de finalidad y retención de datos. En los últimos puntos se relacionará el conocimiento expuesto con los efectos de incluir personas en bases de datos y los argumentos que la Corte Suprema podría incorporar en futuros razonamientos.

2. EL REGISTRO SAF

El Ministerio Público, desde los inicios de la Reforma Procesal Penal implementó el Sistema de Apoyo a los Fiscales o registro SAF. Al momento de la redacción de este trabajo, el sistema busca ser reemplazado por el proyecto informático llamado Red de Gestión Penal (RGP)[5].

Se fundamenta la creación y el uso del sistema SAF en el artículo 227 del Código Procesal Penal[6], que le mandata a la institución mantener un registro

---

5 Fiscalía (2022) p. 2.

6 Código Procesal Penal, Artículo 227: Registro de las actuaciones del ministerio público. El ministerio público deberá dejar constancia de las actuaciones que realizare, tan pronto tuvieren lugar, utilizando al efecto cualquier medio que permitiere garantizar la fidelidad e integridad de la información, así como el acceso a la misma de aquellos que de acuerdo a la ley tuvieren derecho a exigirlo. La constancia de cada actuación deberá consignar a lo menos la indicación de la fecha, hora y lugar de realización, de los funcionarios y demás personas que hubieren intervenido y una breve relación de sus resultados.

de las actuaciones hechas, de forma tal que permita mantener la fidelidad e integridad de la información y el acceso a terceros que estén facultados.

Sobre la referencia normativa, es la Ley Orgánica Constitucional del Ministerio Público en su artículo 17 letra d) la que le otorga al Fiscal Nacional facultades reglamentarias[7], que son el antecedente de la reglamentación que da origen al registro SAF. Dichas facultades reglamentarias se enmarcan en su función constitucional del artículo 83, que indica que el Ministerio Público dirigirá en forma exclusiva la investigación de los hechos constitutivos de delito, los que determinen la participación punible y los que acrediten la inocencia del imputado y, en su caso, ejercerá la acción penal pública en la forma prevista por la ley. De igual manera, le corresponderá la adopción de medidas para proteger a las víctimas y a los testigos.

En uso de dichas facultades el Fiscal Nacional dictó el Reglamento sobre Procedimiento de Custodia, Almacenamiento y Eliminación de Registros, Documentos y Similares, que regula todos los registros y documentos y demás antecedentes que forman parte de las investigaciones del Ministerio Público. En el artículo 3° inciso cuarto[8] y 14[9] del referido Reglamento se repite la instrucción de que la información contenida en los sistemas informáticos del Ministerio Público se mantendrá permanentemente y no se borrará.

En el proyecto original del Código Procesal Penal presentado al Congreso Nacional, la regulación del actual artículo 277 se encontraba en el artículo 52[10], de forma levemente diferente. En la propuesta original, se establecía que las actuaciones de los fiscales debían registrarse de forma resumida. Este último concepto, se eliminó al unirse el artículo en un párrafo especial dedicado a los

---

7 Ley Orgánica Constitucional del Ministerio Público, Artículo 17: Corresponderá al Fiscal Nacional: d) Dictar los reglamentos que correspondan en virtud de la superintendencia directiva, correccional y económica que le confiere la Constitución Política. En ejercicio de esta facultad, determinará la forma de funcionamiento de las fiscalías y demás unidades del Ministerio Público y el ejercicio de la potestad disciplinaria correspondiente.

8 Reglamento sobre Procedimiento de Custodia, Almacenamiento y Eliminación de Registros, Documentos y Similares, Artículo 3 inciso 4:"En caso de eliminación, se indicará además, la cantidad, si existe registro en el sistema informático institucional asociado a ellos y si la eliminación es total o parcial. En todo caso, se mantendrá el registro electrónico de dicha causa en el referido sistema informático".

9 Reglamento sobre Procedimiento de Custodia, Almacenamiento y Eliminación de Registros, Documentos y Similares, Artículo 3 inciso 14 "La eliminación o destrucción de los registros de las investigaciones no comprenderá aquellos antecedentes que se encuentren contenidos en el sistema informático institucional, los cuales se mantendrán almacenados indefinidamente".

10 Historia de la Ley (2000) Mensaje Proyecto de Ley, p. 28: "Registro de las actuaciones del ministerio público. Las actuaciones realizadas por los fiscales del ministerio público se registrarán en forma resumida y contendrán la indicación de la fecha, hora y lugar de realización de la respectiva actuación, como, asimismo, de los funcionarios que hubieren tomado parte en ella y, finalmente, una breve relación de los resultados obtenidos".

registros de las actuaciones de la policía[11]. La idea de registro en forma resumida no daba luces sobre una limitación a la cantidad de información que se podía almacenar, pero –aunque imperfecta– era un avance desde el reconocimiento a una limitación de dicha información.

El Ministerio Público justifica la conservación de estos datos para aquellos casos en que sea un tribunal el que pueda requerir información de copias de antecedentes de causas que no se encuentren vigentes, en cuyo caso se entregarán sin más trámite[12]. Por otra parte, también ha reconocido la necesidad de resguardar los derechos contenidos en la Ley N° 19.628 sobre Protección de la Vida Privada, al hacer referencia al hecho de que, aun siendo la sentencia de los tribunales pública, no significa que la carpeta de investigación penal lo sea para terceros no intervinientes[13]. En ese mismo sentido, el Ministerio Público ha planteado que, en caso de recibir solicitudes de acceso a la información de investigaciones penales cerradas, se debe notificar a los terceros que pudieran verse afectados en sus derechos[14]. Tal actuar sigue la lógica de protección de datos personales del artículo 20 de la Ley N° 20.285 sobre Acceso a la Información Pública.

En concreto, el registro SAF incorpora información de las actuaciones de los fiscales, como indica la norma legal, y de personas que tienen alguna relación con causas que conocen los tribunales, como indica la regulación reglamentaria. En el segundo grupo de datos se registran:

1. Domicilios (todos los registrados, ya sean nuevos o antiguos): tipo (profesional o personal), dirección, comuna, región y teléfono asociado.
2. Casos asociados: RUC, tipo de sujeto, fiscalía, fiscal, fecha de recepción, estado, fecha de término, número de parte, fecha de parte, nombre caso.
3. Delitos asociados: delito, fecha de delito, dirección delito, RUC, fiscalía, fiscal, tipo de sujeto, motivo término, violencia intrafamiliar (VIF) y otros detalles como lugar de ocurrencia, requerimiento, forma, edad con que cometió delito, fecha término, Responsabilidad penal Adolescente (RPA).
4. Órdenes de detención: RUC, fiscalía, fiscal delito, estado de caso, fecha orden, estado orden, fecha termino orden, tribunal.
5. Suspensiones condicionales del procedimiento: RUC, fiscalía, fiscal,

11 Historia de la Ley (2000) Mensaje Proyecto de Ley, p. 762.
12 Ministerio Público (2014) p. 6.
13 Ministerio Público (2011) p. 2.
14 Ministerio Público (2011) p. 2.

delito, fecha suspensión condicional procedimiento, vencimiento, solicitud revisión o sobreseimiento, fecha orden detención, otros detalles.

6. Medidas cautelares: RUC, fiscalía, fiscal, delito restricción, estado fecha medidas cautelares, plazo días, otros.
7. Sentencias: RUC, fiscalía, fiscal, delito, término, procedimiento, fecha de sentencia, detalle.
8. Prisión preventiva decretada imputado evadido: RUC, tipo sujeto, fiscalía, fecha recepción, estado, nombre caso, estado actividad.
9. Otros intervinientes relacionados con el imputado: RUC, fiscal, estado, tipo de sujeto (demandante, imputado, víctima, denunciante, etc), RUT, nombre.

Además, se suman los datos de licencia de conducir, sea o no evidencia, e información de familiares en caso que un interviniente haya fallecido o quien invoque título suficiente para solicitar el retiro de la causa. En ese mismo sentido, el Ministerio Público no hace distinción si los datos corresponden a mayores o menores de edad, en cuanto a su base de licitud para el almacenamiento, se registra la información de menores de edad de igual forma[15].

Adicionalmente, el Ministerio Público argumenta que en base a las funciones que se le da a la Fiscalía para la creación y operación del Sistema de Análisis Criminal y Focos Investigativos establecido en los tres literales del artículo 37 bis de su ley orgánica constitucional, incorporado en 2015 por la Ley N° 20.861 que Fortalece el Ministerio Público, está autorizado para realizar tratamiento de datos personales[16]. Sin embargo, los tres literales de la norma no son antecedentes posibles para el registro indicado por el Ministerio Público, por tanto, la implementación del registro actual de la norma cae en tres errores, que describiremos individualmente: primero, la norma del 37 bis hace referencia al Sistema de Análisis Criminal y Focos Investigativos, que actualmente tiene un Fiscal Jefe y cinco fiscales de foco a cargo del sistema; dicho registro es distinto en su naturaleza, finalidad y regulación al registro SAF, por tanto, no se podría presumir ni usar como antecedente la regulación de uno en el otro, ya que reglamentan bases de datos distintas.

Segundo, la norma del artículo 37 bis, al establecer las funciones de las unidades de análisis criminal, que forman parte del Sistema, es clara respecto a los tres supuestos informativos y sus limitaciones de tratamiento. En la letra a), se indica que se generará información mediante el análisis estratégico de los datos

---

15 CS (2021) ROL 94.897-2021.

16 CS (2021) ROL 94.897-2021, considerando sexto.

agregados provenientes de delitos contra la propiedad y en general, de aquellos de mayor connotación social, calificados por el Fiscal Nacional, ya sea que su investigación se encuentre vigente o terminada. El artículo habla de datos agregados, los cuales, para el Reglamento Europeo de Protección de Datos, se usan cuando se requieren fines estadísticos de tratamiento, en aquellos casos en que no se necesitan datos personales[17]. Para la Agencia de Protección de Datos Personales de Singapur, la agregación de datos se refiere a la conversión de un conjunto de datos en una lista de registros a valores resumidos y se utiliza cuando no se requieren registros individuales[18]. En nuestra normativa, el concepto se asemeja a la definición de datos estadísticos, es decir, aquellos que, en su origen o como consecuencia de su tratamiento, no pueden ser asociados a un titular identificado o identificable[19]. No es posible escapar del adjetivo que se le impone como límite a la base de datos.

Luego, la letra b) del artículo 37 bis indica que se deberán efectuar reportes de la información analizada sobre criminalidad regional, identificación de patrones comunes en ciertos tipos de delitos, reconocimiento de imputados y cualquier otro que se requiera en relación con un tipo de criminalidad específica. Sin embargo, la norma incorpora de forma indirecta la proporcionalidad en el registro de la información, al señalar que no es una base de todos los delitos, sino de cierto tipo y con algún nivel de criminalidad específica, lo que directamente reduce la omnicomprensión de la base de datos. El estándar de criminalidad no queda delimitado por la norma, solo se hace referencia a la necesidad de definición, pero la proporcionalidad parece ser un antecedente que debería preceder el criterio de determinación.

Finalmente, la letra c) indica que la función es la de formular orientaciones y diseñar procedimientos estándares de gestión eficiente de la información que permitan el logro de los resultados propuestos por el Ministerio Público. Esto significa que son datos de gestión de procesos y no datos de individuos procesados.

Por tanto, la norma del 37 bis incorpora tres limitantes al tratamiento de datos: (i) que los datos deberán provenir de información agregada; (ii) que en otros, su tratamiento sea proporcional a cierto tipo de crímenes y, finalmente; (iii) que el último grupo sea de datos que tienen como finalidad mejorar la gestión.

---

17 RGPD, recital 162.
18 PDPC (2022) p. 49.
19 Ley 19.628, Artículo 2 e).

3. HISTORIA DEL CASO

La Corte Suprema, en sentencia del 23 de mayo de 2023, resolvió rechazar la apelación de un recurso de protección que se presentó contra la Fiscalía Regional de La Araucanía.

El recurrente habría recibido, en septiembre de 2021, la resolución que decreta el sobreseimiento definitivo en procedimiento simplificado conocido por un juzgado de garantía. Un año más tarde, en junio de 2022, se solicitó información por transparencia a la Fiscalía sobre si aún existían registros del sobreseído en el Registro del Sistema de Información y Atención a Usuarios o cualquier otro sistema de apoyo que utilice dicha institución. La respuesta de la Fiscalía Regional, a través de su Director Ejecutivo Regional, confirmó que el sobreseído tenía la calidad de imputado en la causa de consulta.

En este contexto, se presentó un recurso de protección contra el Ministerio Público, en razón que la retención de datos, aun cuando el imputado había sido sobreseído, produce una vulneración a las garantías y derechos constitucionales. Se aduce que, existe un desconocimiento de los efectos del sobreseimiento definitivo, en el sentido de que éste pone término al procedimiento y tiene autoridad de cosa juzgada. Particularmente, se cita el artículo 250 letra c) del Código Procesal Penal que ordena se decrete por el Juez de Garantía sobreseimiento definitivo cuando el imputado esté exento de responsabilidad criminal, en conformidad al artículo 10 del Código Penal o en virtud de otra disposición legal y el artículo 240 inciso segundo del mismo cuerpo legal en cuanto señala que, si ha transcurrido el plazo que el tribunal hubiera fijado para el cumplimiento de las condiciones de la suspensión condicional, sin que esta haya sido revocada, se extinguirá la acción penal, debiendo el tribunal dictar de oficio o a petición de parte el sobreseimiento definitivo.

En virtud de no existir razón, ni jurídica ni lógica, para mantener en el registro la calidad de imputado, el recurrente finaliza argumentando una vulneración del principio de legalidad del artículo 6° de la Constitución Política de la República.

A los argumentos jurídicos se suma en la presentación del recurso de protección, que el actuar de la entidad es perturbador, dañino y frustra todo lo conseguido en el procedimiento con el sobreseimiento definitivo, al mantener la calidad de imputado por una mera, arbitraria e injustificada decisión de la entidad recurrida.

3.1 Argumentos del Ministerio Público

Según explica la sentencia de primera instancia de la Corte de Apelaciones de Temuco, la Fiscalía responde que no se solicitó el estado de vigencia de la

causa, pues si la parte lo hubiera solicitado, habría aparecido la información del registro SAF, vale decir, hubiera aparecido la causa como "terminada". Como no pidió dicha información, no se le podía entregar. En ese orden de cosas, no se ha afectado la cosa juzgada, por no haberse invocado diligencias investigativas ni actuaciones judiciales posteriores a la resolución del sobreseimiento definitivo.

La Fiscalía Regional es consistente con las justificaciones de casos anteriores, sobre los antecedentes de los artículos 227 y 246 del Código Procesal Penal y el artículo 37 bis de la ley orgánica del Ministerio Público. Además de agregar que para la Ley N° 19.628, al referirse a los datos de carácter personal, los organismos públicos solo podrán tratar datos materia de su competencia y con sujeción a las demás reglas de la ley, en cuyo caso no requieren el consentimiento del titular.

Agrega la Fiscalía Regional, como antecedente, el mandato de la Ley 20.931 de 2016, conocida como la Ley de Agenda Corta Antidelincuencia, que en su artículo 11 crea un sistema compartido de información entre instituciones que participan de la persecución penal por medio de la Base Unificada de Datos o BUD[20]. Este sistema se materializó a través del Decreto N°899 de 2018 del Ministerio de Justicia. El sistema recoge información de imputados y condenados para apoyar la labor investigativa de las etapas del proceso penal.

Luego argumenta que la obligación de procesamiento y entrega de información y estadísticas construidas a partir de los registros del SAF sirven de fundamento para la Ley de Presupuestos y recursos que serán asignados.

---

[20] Ley 20.931, Artículo 11: El Ministerio Público, Carabineros de Chile, la Policía de Investigaciones de Chile, Gendarmería de Chile y el Poder Judicial deberán intercambiar, de conformidad con el artículo 20 de la ley N°19.628, los datos personales de imputados y condenados, con el objeto de servir de elemento de apoyo a la labor investigativa en las diversas etapas del proceso penal y de colaboración para una eficaz y eficiente toma de decisiones de los tribunales de justicia, de sustento a las políticas de reinserción y en la atención, custodia y asistencia de detenidos, sujetos a prisión preventiva y condenados en recintos penitenciarios. El funcionamiento de este banco de datos se regirá por un decreto supremo del Ministerio de Justicia, que llevará la firma del Ministro del Interior y Seguridad Pública, el que podrá determinar otras instituciones u órganos de los señalados en el artículo 1º de la ley orgánica constitucional de Bases Generales de la Administración del Estado, con excepción de aquellos que gocen de autonomía constitucional, para que dentro de la esfera de su competencia, integren el mismo.
Corresponderá al Ministerio Público la administración del banco de datos que se forme y que se configurará con los datos señalados en el inciso anterior, el que deberá mantener unificado y actualizado y podrá ser consultado o requerido por los organismos referidos en dicho inciso, dentro de la esfera de su competencia, garantizando la interoperatividad de los bancos antes referidos.

Finalmente hace referencia al artículo 246 del Código Procesal Penal, CPP[21], el cual indica que se deberá llevar un registro de los casos en que se decrete suspensión condicional o se aprobaren acuerdos reparatorios. La finalidad de este registro es verificar que el imputado cumpla las condiciones que se le imponen o reúna los requisitos para acogerse a una nueva suspensión condicional o a un acuerdo reparatorio.

3.2 Razonamiento de las cortes

La Corte de Apelaciones de Temuco indica que sobre la información del registro SAF recae una presunción de veracidad, y que no tiene la aptitud para dañar la honra del recurrente. Por ello, no podría ser considerada arbitraria, la que debería suponer irracionalidad o falta absoluta de justificación, pero en este caso el antecedente legal y su veracidad sería suficiente para desestimarlo. Además, considera, que el tratamiento de los datos se ajusta a los requisitos del artículo 20 de la Ley N° 19.628, debido a que el Ministerio Público trata los datos bajo sus competencias. En ese sentido, la retención de dichos datos parece un imperativo al funcionamiento del Ministerio Público. Por todo lo anterior, se rechaza el recurso de protección.

Al conocer la apelación del recurso, la Corte Suprema en su voto de mayoría confirma la decisión de la Corte de Apelaciones sin agregar contenido a la resolución.

3.3 Razonamiento del voto de minoría

Cabe enfocarse en el voto en contra de la ministra Ángela Vivanco. Para ella, primero es preciso clarificar el alcance del registro SAF. Cita las normas del 227 y del 37 bis del CPP y de la ley orgánica del Ministerio Público y aclara que estas facultan la creación de registros de datos personales de quienes hayan tenido la calidad de intervinientes o de imputados[22].

Agrega que dichas normas no son antecedentes del registro SAF y, por tanto, no existe norma legal que lo autorice. Según se indica, el registro SAF se ha

---

21 Código Procesal Penal, Artículo 246: Registro. El ministerio público llevará un registro en el cual dejará constancia de los casos en que se decretare la suspensión condicional del procedimiento o se aprobare un acuerdo reparatorio.
El registro tendrá por objeto verificar que el imputado cumpla las condiciones que el juez impusiere al disponer la suspensión condicional del procedimiento, o reúna los requisitos necesarios para acogerse, en su caso, a una nueva suspensión condicional o acuerdo reparatorio.
El registro será reservado, sin perjuicio del derecho de la víctima de conocer la información relativa al imputado.

22 Considerando 2°.

implementado por la sola potestad reglamentaria del Fiscal Nacional mediante la dictación del Reglamento sobre procedimiento de custodia, almacenamiento y eliminación de registros, documentos y similares, en el cual se posibilita la eliminación de datos de los registros, pero que se decidió que en el caso de los del registro SAF, se mantengan de forma indefinida[23].

La ministra Vivanco señala que, no obstante lo anterior, cumple con el requisito de actuación dentro de sus competencias para el tratamiento de datos de la ley N° 19.628. Sin embargo, el artículo 21 de la misma ley[24] prohíbe la comunicación de datos relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena, salvo, dice el párrafo segundo del mismo artículo, en aquellos casos en que la información sea requerida por tribunales de justicia u otros órganos dentro de su competencia. Por lo mismo, nada dice sobre la excepción de la resolución que sobresee definitivamente la causa. Es decir, es aplicable la norma de excepción del inciso segundo solo a resoluciones indicadas y nada hace presumir que se le aplique a la retención indefinida del registro SAF relativo a investigaciones culminadas por sobreseimiento definitivo[25].

Finaliza argumentando que al no existir norma legal que autorice la mantención indefinida de los datos de investigación del recurrente, la mantención indefinida de los datos configura un acto ilegal y arbitrario que lesiona el derecho a la honra y a la privacidad, y por tanto es una vulneración al artículo 19 N° 4 de la Constitución Política de Chile.

4. LAS DIVIDIDAS LÍNEAS JURISPRUDENCIALES DE LA CORTE SUPREMA EN EL ASUNTO

Se pueden reconocer dos grandes líneas jurisprudenciales en la Tercera Sala de la Corte Suprema. Una primera línea histórica es la que acepta las solicitudes de eliminación de información de los registros SAF para aquellos casos de sobreseimiento definitivo. Postura que, en base a nuestras búsquedas, parte con el voto de mayoría de la causa Rol N° 50.001-2016.

---

23 Considerando 3°.

24 Ley 19.628, Artículo 21: Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena.
Exceptúase los casos en que esa información les sea solicitada por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5º, 7°, 11 y 18.

25 Considerando 4°.

La decisión del 2016 levantó los mismos argumentos descritos en la decisión en comento y que se repetirían en las siguientes decisiones: (i) que las normas del artículo 37 bis de la ley orgánica del Ministerio Público, el artículo 11 de la Ley N° 20.931, más el artículo 277 del CPP eran antecedentes claros del funcionamiento del Ministerio Público, pero sin el alcance que este le da a los registros permanentes de datos personales; (ii) que no existe norma legal que autorice la elaboración y mantención del registro con la modalidad del SAF y que su única fuente es la potestad reglamentaria del Fiscal Nacional; (iii) que el Ministerio Público debe actuar bajo los preceptos de la Ley N° 19.628, específicamente los artículos 20 y 21; (iv) que el inciso primero del artículo 6° de la Ley 19.628 ordena que los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado; (v) que no existe norma legal que autorice la mantención indefinida del registro SAF; y (vi) que la mantención indefinida de datos de investigación del registro SAF, en casos que haya sentencia condenatoria, sobreseimientos definitivos, acogido al Decreto Ley Nº 409 de 1932 o acción penal prescrita, lesiona el derecho a la honra y a la privacidad.

Esta primera línea de argumentación ha sido replicada en otras tres decisiones, incluida la decisión en comento (Rol N° 34.756-2021, 85.215-2020, 25.763-2019 y en cuatro votos de minoría Rol N° 5-2018, 76.378-2020, 76.209-2020 y 51.809-2023).

La segunda línea comienza con el voto de minoría de la ministra María Eugenia Sandoval en la causa Rol N° 50.001-2016, en la que se argumenta lo siguiente: (i) se justifica la retención de información en el mandato del artículo 227 del CPP que ordena al Ministerio Público llevar registro de las actuaciones; (ii) que el artículo 14 del Reglamento sobre procedimiento de custodia, almacenamiento de registros, documentos y similares del Ministerio Público impide borrar los datos almacenados electrónicamente, lo que se le aplica al registro SAF; (iii) que el listado de causas del registro SAF no es secreto, lo que ha sido sostenido por la jurisprudencia de la Segunda Sala de la Corte; (iv) la norma del inciso segundo del artículo 8° de la Constitución Política de la República[26] sobre publicidad de los actos como regla general, y; (v) finalmente argumenta que la información que la parte requirente solicita eliminar se encuentra disponible en la página *web* del Poder Judicial.

[26] "Son públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y los procedimientos que utilicen. Sin embargo, sólo una ley de quórum calificado podrá establecer la reserva o secreto de aquéllos o de éstos, cuando la publicidad afectare el debido cumplimiento de las funciones de dichos órganos, los derechos de las personas, la seguridad de la Nación o el interés nacional".

Esta argumentación ha sido repetida en al menos tres decisiones en voto de mayoría en los roles 5-2018, 76.378-2020 y 76.209-2020 y en otra minoría 25763-2019.

Que la respuesta de la Tercera Sala de la Corte Suprema haya sido dividida, podemos colegir que dependiendo de la conformación de la sala se llega a una interpretación más adecuada con la protección de la privacidad y su consagración constitucional moderna o bien podemos encontrar una sala que resguarda el actuar y protocolos de retención de datos del Ministerio Público.

5. DEL MANEJO DE DATOS POR LAS FISCALÍAS: CUESTIONAMIENTOS

La vigilancia masiva es la conducta en la cual el Estado recopila constantemente información de sus ciudadanos sin que exista un antecedente de duda razonable o antecedentes que justifiquen la violación de privacidad. Esta acción, tal como explica Amnistía Internacional, normaliza la idea de que todos son sospechosos de posibles delitos hasta que se demuestre su inocencia y, por tanto, invierte el principio y garantía de presunción de inocencia[27]. La vigilancia masiva permite intromisiones injustificadas por el Estado en la vida de los ciudadanos que dice proteger.

La presunción de inocencia está consagrada en nuestra Constitución[28], en los distintos tratados internacionales de derechos humanos[29] y en el Código Procesal Penal[30]. Asimismo, el artículo 10 del mismo Código indica que el juez de garantía debe de oficio o a petición de parte adoptar las medidas necesarias para proteger las garantías judiciales consagradas en la Constitución Política, en las leyes o en los tratados internacionales ratificados por Chile.

La presunción de inocencia tiene directa relación con la información que se retiene. Si no existe un hecho que anteceda y justifique la retención de su información, en los casos en que se ha desestimado la acción penal o se ha dado termino al proceso siendo certificado por un tribunal de la república u otra forma procesalmente equivalente, la presunción de inocencia impone la obligación de respetarlo no solo en su contenido estrictamente procesal, sino

---

27 Amnesty International (2015).

28 Constitución de la República de Chile, Artículo 19 N° 3 inciso 6°: La ley no podrá presumir de derecho la responsabilidad penal.

29 Declaración Universal de Derechos Humanos, Artículo 11; Convención Americana de Derechos Humanos, artículo 8, N° 2; y Pacto Internacional de Derechos Civiles y Políticos, artículo 14 N° 2.

30 Código Procesal Penal, Artículo 4º: Presunción de inocencia del imputado. Ninguna persona será considerada culpable ni tratada como tal en tanto no fuere condenada por una sentencia firme.

en aquellas aristas relacionadas que de igual manera permiten su materialización. Es en ese sentido que el artículo 122 del CPP[31] que se encuentra en los principios generales de las medidas cautelares personales, mandata que estas se impondrán solo cuando fueren absolutamente indispensables para asegurar los fines del procedimiento y solo durarán mientras subsistiere la necesidad de su aplicación.

La norma anterior guarda una regulación similar a la contenida en el inciso final del artículo 223 del CPP que indica que las comunicaciones interceptadas que contengan informaciones relevantes para otros procedimientos seguidos por hechos que puedan constituir un delito al que la ley le asigne pena de crimen, no deberán ser destruidas. La norma en estos casos también incorpora la proporcionalidad, de forma indirecta, y deja fuera la posibilidad que durante las escuchas se hagan hallazgos casuales de faltas o simples delitos[32]. Sin embargo, en el caso del inciso final no se determina un plazo para la conservación de la información, por lo que se podría retener de forma indefinida.

Respecto a este caso podríamos plantear una situación extrema, en aquellas en que el registro SAF guarda información que ha sido obtenida previa autorización de un juez de garantía y cuyos antecedentes no se borran. Podríamos llegar al absurdo que una vez obtenida la información por una orden precautoria esta quede liberada para el Ministerio Público para causas siguientes.

Resulta interesante que, en el caso de la interceptación de comunicaciones por medio del registro remoto de equipos informáticos, el literal e) del artículo 225 ter del CPP, exige que se solicite al juez de garantía que dicte la resolución judicial que autoriza el acceso y se fije el tiempo de supresión de los datos, requisito que no se encuentra en las disposiciones anteriores.

El riesgo de afectar la percepción presente del fiscal a cargo de una investigación en base a hechos pasados se contrarresta en la prohibición de utilizar registros pasados como medio de prueba. Es el principio de que la prueba que sirve de base a una sentencia debe haber sido producida durante el mismo procedimiento y no incorporar medios de prueba o dar lectura en el debate a los registros y demás documentos que dieran cuenta de diligencias o actuaciones realizadas por la policía o el Ministerio Público previamente en otros procedimientos. Tal como Horvitz y López indican, se quiere asegurar la centralidad del juicio, evitando que el debate se

---

31 Código Procesal Penal, Artículo 122.- Finalidad y alcance. Las medidas cautelares personales sólo serán impuestas cuando fueren absolutamente indispensables para asegurar la realización de los fines del procedimiento y sólo durarán mientras subsistiere la necesidad de su aplicación.
Estas medidas serán siempre decretadas por medio de resolución judicial fundada.

32 Horvitz y López (2006) p. 531.

transforme en una ratificación de actuaciones de la investigación, tal como ocurría en el antiguo plenario criminal[33]. En esa línea, el inciso segundo del artículo 334 del CPP indica que no se podrá incorporar como medio de prueba o dar lectura a actas o documentos que dieren cuenta de actuaciones o diligencias declaradas nulas, o en cuya obtención se hubieren vulnerado garantías fundamentales. En razón de esto, parece evidente que la retención de información de procesos anteriores constituiría una violación a garantías fundamentales por no contar con autorización de un juez para la investigación o proceso particular.

La realidad del tratamiento descrito en los casos que ha conocido la Corte Suprema da cuenta de un tratamiento de datos excesivo, donde no solo se registra información de responsables penales, sino de cualquier persona que haya estado relacionada activa o pasivamente en la comisión de un delito.

En la doctrina nacional, la ministra Vivanco, en su calidad de profesora de Derecho Constitucional y en un asunto jurídico similar, cuestionó el decreto presidencial que ordenaba a las compañías de telecomunicaciones almacenar datos de sus clientes por dos años y a los que iba a ser posible acceder sin orden judicial. En este sentido planteaba que el almacenamiento que se aplique a todos los usuarios de un sistema sin distinción alguna y no a aquellos que estén bajo una investigación o hayan sido sujetos de imputación penal, representa una desconfianza colectiva que repugna a la presunción de inocencia[34].

El almacenamiento permanente de datos personales crea un estado de supervigilancia que destruye la presunción de inocencia. No es posible escapar si no existen limitaciones, sobre todo cuando son estos órganos públicos quienes autoimponen sus propias limitaciones, con un control cuestionable a lo menos de las mismas, más aún, se evidencia en el caso en comento que la reglamentación autodefinida determina que la información electrónica no se elimine. Y, como consecuencia de esta "autolimitación", se creó un estado de vigilancia permanente, contrario a los principios constitucionales y penales.

6. PRINCIPIOS EN MATERIA DE PROTECCIÓN DE DATOS: HORIZONTES COMPARADOS

Parece adecuado para este análisis hacer referencia a la normativa y razonamientos realizados por el Tribunal Europeo de Derechos Humanos (o "TEDH") en casos similares y compararlos con la realidad que estamos intentando abordar.

---

33 Horvitz y López (2006) p. 318.
34 Vivanco Martínez (2017b).

El derecho europeo es similar en familia al nuestro, pero han tenido mayor posibilidad de discutir sobre asuntos relacionados con el tratamiento de datos personales por parte de órganos públicos, en particular órganos que trabajan en materias criminales. La lógica de protección de la dignidad humana aplicada por el derecho comparado debería ser similar, o al menos ser antecedente de nuestros razonamientos.

Incluso, a mayor abundamiento, la justificación para encontrar conclusiones útiles a partir de la revisión de decisiones internacionales nace de varias aristas. Primero, la lógica de protección al ser humano y entender a este último como un sujeto de derecho se instaló de manera definitiva como una aseveración incuestionada, desde el término de la Segunda Guerra Mundial. Segundo, las tradiciones legales europeas son diversas entre sí, al menos en lo que respecta al Derecho Civil y al Anglosajón, incluyendo estados unitarios y otros federales en su estructuración. Esta última circunstancia es valiosa para nuestro análisis, ya que las decisiones que se han dado tienen en consideración las diferentes realidades, es decir, han dado soluciones a situaciones de relevancia jurídica provenientes de distintos orígenes. Tercero, podemos encontrar que las decisiones de las Cortes citadas utilizan fuentes legales similares a las que usaría o está llamada a usar un tribunal chileno, esto es, catálogos de derechos, tratados internacionales, leyes y principios contenidos en estas, entre otros.

Desde los primeros casos que conoció el TEDH sobre vigilancia –hace casi 45 años atrás– que se ha construido y fijado el criterio que se deben adoptar las medidas adecuadas y efectivas para que cualquier sistema de supervigilancia evite y no permita abusos en su empleo[35]. Es necesario aclarar que la obligación de adopción de medidas adecuadas y efectivas no se da debido a que necesariamente hayan existido abuso en el sistema, sino más bien buscan reducir la posibilidad de que estos ocurran.

El TEDH ha argumentado constantemente, incluso desde antes de la actual regulación en materia de protección de datos, que la información pública puede entrar en el ámbito de la vida privada cuando se recoge y almacena sistemáticamente en archivos estatales[36]. Mientras más información se recoja, por muy pública y accesible que sea, quien almacena se encuentra en posibilidad de violar la privacidad de los individuos. No es solo desde dónde viene y se obtiene la información, su acumulación también es un problema.

Por nuestra parte, el Tribunal Constitucional de Chile definió la autodeterminación informativa como aquel derecho que protege el control que tenga

---

35 European Court of Human Rights (1978), considerando 50.
36 European Court of Human Rights (2012), considerando 187.

un titular de la circulación de sus datos[37]. Hay límites obvios que demarcan el concepto, como lo son la autorización por terceros del tratamiento, tener control sobre la finalidad del tratamiento en la medida en que no exista un interés público o particular mayor a la privacidad y la posibilidad de quitar la autorización de uso.

Es de la esencia de la autodeterminación informativa que existan dos principios: que el titular sepa para qué se guardan sus datos y que sepa por cuanto tiempo se almacenan. Si ambas respuestas no son claras, no se puede hablar de la existencia de autodeterminación informativa. Cuando no existe una limitación temporal del uso de los datos, es decir, no existe un tiempo cierto de número de años para ser borrados y ajustarse a los principios de finalidad, entonces se elimina la autodeterminación informativa.

El Tribunal Constitucional Federal Alemán, en la famosa y trascendental sentencia de 15 de diciembre de 1983, conocida como la sentencia de Ley de Censo, consagró el concepto de autodeterminación informativa, estableciendo que no sería conciliable con la dignidad humana que el Estado pudiera arrogarse el derecho a registrar y catalogar coactivamente al hombre con relación a su entera personalidad[38].

En lo atingente a los temas expuestos, nos enfocaremos en los títulos sucesivos en el principio de finalidad o de limitación de finalidad y en la retención de datos.

6.1 Principio de finalidad o de limitación de finalidad

El principio de finalidad o de limitación de finalidad tiene un doble efecto: (i) es para el titular una garantía respecto del uso que se le va a dar a sus datos; y (ii) es para el responsable una limitación de los fines para los que se pueden utilizar y por cuánto tiempo deben ser retenidos.

Este principio ha ido de la mano desde los inicios de la formulación del derecho a la protección de los datos personales. Ya se encontraba en el artículo 9 de la *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* de 1980, donde se requería a los países miembros que los fines para los que se recogen los datos personales deben especificarse a más tardar en el momento de su recopilación, y su uso posterior debe limitarse al cumplimiento de dichos fines o de otros que no sean incompatibles con ellos y que se especifiquen en cada cambio de finalidad.

---

37 Tribunal Constitucional (2011) rol 1894-2011, N° 30.

38 Heredero Higueras (1983) p. 147.

En la Unión Europea, la Directiva 2016/680 sobre Protección de Datos en el Ámbito Penal[39], en su considerando 26 indica que los datos personales deben ser adecuados y pertinentes a los fines, que no deben ser excesivos ni que se conserven más tiempo del necesario. Agrega que solo deberían tratarse si la finalidad no puede conseguirse por otros medios razonables.

En España, según el artículo 8° de la Ley Orgánica 7/2021[40], cualquier dato personal que haya sido recolectado para fines de prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, se deberá cancelar cuando dejen de ser necesarios para investigaciones concretas que antecedan su almacenamiento. Para ello, el análisis de proporcionalidad deberá tomar en consideración la edad del afectado, los tipos de datos almacenados, la urgencia de retención hasta el fin de la investigación o un procedimiento particular, el tipo de resolución judicial con especial preocupación de la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad[41]. Además, se fija como límite máximo para la supresión de datos el plazo de veinte años. Agrega el artículo 22.3 de la Ley Orgánica 3/2018[42] que los datos con fines de videovigilancia captados por personas físicas o jurídicas, públicas o privadas que tengan la finalidad de preservar la seguridad de las personas y bienes deberán ser suprimidos en un máximo de un mes desde su captación, salvo cuando sean necesarios para acreditar actos que atenten contra la integridad de las personas, bienes o instalaciones. En este último caso, serán puestas a disposición de la autoridad competente.

En nuestra legislación el principio de limitación de finalidad se encuentra en el artículo 9 de la Ley N°19.628 donde se indica que los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público.

En nuestra doctrina nacional, el profesor Reusser revisando decisiones de casos de personas que figuraban en el registro SAF, afirma que la finalidad del tratamiento de datos es lo fundamental[43], en especial como antecedente de resolución de varios de los conflictos resueltos por los tribunales. Agrega que el análisis debe hacerse cargo de una finalidad determinada, explícita y legítima

---

39 Directiva 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

40 De Protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

41 Álvarez Hernando (2019) pp. 17-18.

42 de Protección de Datos Personales y garantía de los derechos digitales.

43 Resusser Monsálvez (2021) p. 179.

que compete tener al responsable del tratamiento de los datos[44]. Los fines en el caso de los órganos públicos son determinados por ley y deberán ser informados a los titulares.

En nuestro caso existe referencia a al menos un caso en que se ha usado el registro SAF para un fin distinto del indicado en el 277 del CPP. Según información de la sección de noticias de la página de la Fiscalía, se han usado los datos del Registro SAF para entregar un modelo matemático "que busca construir una red de vínculos entre personas con historial delictivo e identificar a potenciales miembros de una agrupación asociada a un hecho criminal específico"[45].

Dicho modelo matemático también busca "validar hipótesis investigativas" y no crear estas hipótesis. La validación de la información en base a métodos probabilísticos es incorrecta, ya que estos últimos solo pueden ser entendidos como antecedentes a demostrar por evidencia directa. Si el uso del sistema es el indicado, ratifica parte de los riesgos –y miedos– que generan los sistemas de supervigilancia masiva. Si la hipótesis de participación en un delito está "probada" por un sistema automático, es muy probable que sea el imputado quien tenga que probar que no participó en caso que sea inocente, desvirtuando o llevando a ser ilusoria la presunción de inocencia, al tener el acusado que probar su inocencia y no siendo el ente persecutor quien debería rendir prueba para desvirtuar la presunción y así llegar a la convicción del tribunal. En la práctica, esto podría llegar a transformar en la eliminación de la presunción de inocencia.

Si el sistema funciona como es descrito en la nota periodística antes citada, en el que se identifican personas de quienes se desprenden vínculos con terceros con los que haya participado en al menos un delito previamente, se estaría retrocediendo a la idea de un derecho penal de autor. En este último, existe una presunción de responsabilidad por elementos que no son derivados del hecho particular, sino de condiciones sociales o relacionales del individuo. Una persona, aun cuando se intente desvincular de alguien, por el solo hecho de haber sido relacionado durante la comisión de un delito con anterioridad, en este nuevo sistema, pasará a ser sospechoso o un candidato de participación. Esto nos hace cuestionarnos frente a la urgencia de, al menos, retirar de los registros SAF a aquellos que no han sido declarados autores ni a quienes se les haya demostrado culpabilidad penal.

La creación de modelos matemáticos que ayuden a determinar sospechosos es una finalidad que debería al menos ser ajustada a tres adjetivos: determinado,

---

44 Resusser Monsálvez (2021) p. 180.
45 Fiscalía Nacional (2023).

explícito y legítimo. ¿Cómo justificamos hacer un modelo de predicción criminal que cumpla con estas tres condiciones? No parece, de un primer análisis, que sea un fin determinado por ley los registros SAF, ya que no se ajusta a la norma del 277 del CPP, el que únicamente busca ser un registro de las actuaciones de la fiscalía y en caso que se pudiera justificar, en alguna de las funciones del 37 bis de la LOC del Ministerio Público; dicha información no hace referencia al registro SAF sino al BUD, que como bases de datos tienen regulaciones distintas.

Como bien explica la matemática Catherine O'Neil, los modelos como los reseñados, se basan en datos del pasado y bajo el supuesto que los patrones se van a repetir[46]. En este sentido es claro que no existe otro antecedente científico que permita predecir comportamiento o participación.

Pareciera ser que los sistemas científicos dan una presunción de justicia[47]y la idea de prueba científica parece ser más certera que la no científica. Siempre asumimos que la ciencia es objetiva y no tiene ninguna ganancia con el resultado que pueda tener un proceso[48]. Ejemplos como este abundan en la historia del Derecho en que se sancionaron personas por ciencia, pero sin responsabilidad penal. El problema no se produce por quienes quedan fuera de la predicción por error, sino por quienes quedan dentro y no tienen la forma de salir.

6.2 Retención de datos

La misma normativa europea 2016/680[49], en su considerando 26 indica que para garantizar que los datos no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su eliminación o revisión periódica. La normativa establece asimismo y reitera en su artículo 5 que los Estados miembros deben fijar plazos para la supresión de los datos personales o para una revisión periódica de la necesidad de conservar dichos plazos.

En el caso del Derecho Español, la transposición normativa se produjo en la Ley Orgánica 7/2021, que en su artículo 8 señala que el responsable del tratamiento determinará que la conservación de los datos personales tenga lugar sólo durante el tiempo necesario para cumplir con los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución

46 O'Neil (2016) p. 38.
47 O'Neil (2016) p. 79.
48 Fabricant (2022) p. 26.
49 Directiva 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

de sanciones penales. Asimismo, en el segundo párrafo del artículo se establece que el responsable deberá revisar cada tres años la necesidad de conservar, limitar o suprimir los datos personales, bajo su responsabilidad. Esta revisión debe tomar en consideración la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal. Finalmente, la norma pone un límite máximo de conservación de veinte años, con excepción de aquellos casos en que las investigaciones sigan abiertas o de delitos que no hayan prescrito, entre otros.

En ese sentido, el TEDH ha conocido de diversos casos que delimitan la retención de datos de una forma práctica. En un caso reciente, el Gobierno Inglés alegó en el caso *Gaughran v The United Kingdom*, que cuantos más datos se conserven, más se podía prevenir la delincuencia. Para el TEDH, este argumento no solo era contrario al texto expreso, sino que también significaría un sinsentido, ya que dicho razonamiento permitiría que se conservara indefinidamente información sobre toda la población y sus familiares fallecidos, lo que sería excesivo e irrelevante para las finalidades expuestas[50].

En esa misma línea, el mismo TEDH ha argumentado que en caso de que sea importante retener ciertos datos, ello debe ser concordante con los delitos que anteceden la acción[51]. Además, solicita que se incorporen criterios de proporcionalidad en la conservación de antecedentes criminales, por ejemplo, que no sería razonable llevar un registro con información de infractores de delitos menores, pero sí se justifica en aquellos que puedan tener que ver con terrorismo o delitos de carácter sexual.

Similar discusión se dio en relación a la retención de datos que se puede efectuar respecto de huellas dactilares, perfiles genéticos y muestras celulares de personas que han sido sospechosas, pero no condenadas[52]. Indica el TEDH que en la mayoría de los países de la Unión Europea se recogen muestras celulares solo en procedimientos de sospechosos de crímenes de cierta gravedad y muestras de ADN que deben destruirse inmediatamente o en un plazo limitado tras la absolución o sobreseimiento[53]. Incluso, en aquellos casos en que se permite la conservación de ADN por mayor tiempo, como son los casos de connotación sexual, se debe contar con un período de conservación estrictamente definido y proporcional. También hace notar la Corte que solo Inglaterra, Gales e Irlanda del Norte parecen ser las únicas jurisdicciones del Consejo de Europa que per-

---

50 The European Court of Human Rights (2020), considerando 86.

51 The European Court of Human Rights (2013), considerando 41; The European Court of Human Rights (2017), considerando 43, y; The European Court of Human Rights (2020).

52 European Court of Human Rights (2008), considerando 106.

53 European Court of Human Rights (2008), considerando 108.

mitiría la conservación indefinida de huellas y ADN de personas sospechosas de cualquier edad de delitos registrables[54]. Es importante destacar que dicha referencia es previa a la publicación de la Directiva 2016/680, que afianzó principios en el tratamiento de datos personales diametralmente contrarios a los expuestos en casos por los países del norte.

En estos casos, el TEDH ha razonado que la conservación general e indiscriminada de huellas, muestras de células y ADN de personas sospechosas, pero no condenadas por delitos, no logra un justo equilibrio entre los intereses públicos y privados en conflicto y que el actuar de las autoridades de Reino Unido no da cumplimiento a los estándares conocidos y aceptados por la Unión Europea. La retención de los datos personales es una injerencia desproporcionada a la privacidad y no puede considerarse necesaria en una sociedad democrática[55].

El TEDH ha repetido y ampliado en otro caso sus razones de reforzar la idea de una limitación en la retención de datos criminales, aduciendo que una retención indefinida aumenta el riesgo de estigmatización, derivado del hecho que aún cuando las personas que se encuentren en posición de demandantes y exista la posibilidad de que se guarde información de ellas, pueden ver afectada su presunción de inocencia[56]. El TEDH indicó que la retención de datos de huellas dactilares para quienes no han sido condenados a penas privativas de libertad sobre los veinticinco años es un despropósito, ya que en la práctica significa mantener la información indefinidamente. Es así que se recomienda que un periodo estándar es máximo un año[57].

Por otro lado, se han reconocido como prácticas no contrarias a la privacidad del artículo 8 de la Carta Europea, que se almacenen por 30 años datos de personas que han sido condenadas por delitos sexuales y se eliminen automáticamente luego de ese plazo[58].

Extrapolando estos casos a nuestros tribunales, la Corte Suprema también ha fijado plazos de razonabilidad. En 2019, indicó que no existiendo norma legal alguna que autorice la mantención indefinida de los datos de investigación que involucró a la recurrente y cuyo proceso terminó en sobreseimiento definitivo, no cabe duda que la mantención de los mismos después de haber transcurrido alrededor de cinco años desde la dictación del sobreseimiento definitivo, configura un acto ilegal y arbitrario que lesiona el derecho a la honra y a la privacidad[59].

---

54 European Court of Human Rights (2008), considerando 110.
55 European Court of Human Rights (2008), considerando 125.
56 European Court of Human Rights (2013), considerando 36.
57 European Court of Human Rights (2013), considerando 45.
58 European Court of Human Rights (2009), considerando 67.
59 Rol N° 25.763-2019, considerando séptimo.

Para la ministra Vivanco los registros tienen una consideración del tiempo en relación a la gravedad de los delitos que registran. Pone como ejemplo de excepción a los crímenes de lesa humanidad, por su imprescriptibilidad. Sin embargo, la eliminación de registros debe ser vista siempre con la finalidad de reinserción social[60]. Similar argumento es el esbozado por el profesor Leturia, quien justifica el derecho al olvido en materia judicial en la urgencia de reinserción social y rehabilitación[61].

Tal como indica la ministra Vivanco, también en base a la relevancia del tema, nos da cuenta de la necesidad de gozar del derecho a "disponer de nuestra propia historia" en aquellos casos en que no haya interés público genuino en seguir accediendo a ella libre y abiertamente[62]. Ahora, sabemos que el interés público de retener ciertos datos por parte de organismos estatales debe ser manifestado, en virtud del principio de juridicidad, por medio de habilitaciones legales directas.

Para ambos autores, la conservación de datos o su eliminación, debe ser considerada como una herramienta para resguardar la posibilidad de reinserción social. En ambos casos se solicita ponderar entre dos derechos para resguardar de mejor manera los intereses del individuo. Cabe hacer presente que ambos trabajos fueron previos a la modificación constitucional.

En el entendido que el derecho a la protección no es un derecho absoluto, la Corte Suprema ha rechazado, como indica Ortiz y Viollier[63], solicitudes de derecho al olvido en casos penales donde los delitos son relacionados con abuso sexual y obtención de servicios sexuales de personas menores de edad mediante dinero, en razón que serían ilícitos de interés colectivo o general, en cuanto es necesario para poder difundir a terceros delitos de esta gravedad.

7. EFECTOS PERSONALES DE PERTENECER A UNA BASE DE DATOS NO RECONOCIDA

Clasificar personas es propio de nuestra esencia. Los seres humanos estamos fabricados para reconocer patrones[64]. Imaginar y planificar cómo grupos de personas que comparten características comunes puedan tener resultados similares, parece ser una gran ambición de los gobiernos, lo que facilita la asig-

60 Vivanco Martínez (2017a) p. 372 y ss.
61 Leturia (2016) p. 100.
62 Vivanco Martínez (2017a) p. 379.
63 Ortiz y Viollier (2021) p. 103.
64 Snowden (2019) p. 79.

nación de recursos, esfuerzos y penas. Para la profesora Safiya Umoja Noble, la invención de la cultura de la imprenta aceleró la necesidad de clasificar. Esta cultura produjo históricamente clasificaciones que degeneraron en segregaciones permanentes a ciertos sectores de la población[65] y que actualmente son uno de los riesgos más comunes al pensar en protección de datos frente a la Administración del Estado.

Uno de los problemas que aparece al momento de entender las clasificaciones, es que estas tienden a permanecer indefinidamente. Los datos, una vez recogidos, son difíciles de olvidar. Los registros tienden a ser permanentes por defecto, lo que es antecedente de una sociedad enfocada en características negativas de sus ciudadanos[66]. Con la reducción de los costos de almacenamiento de información y con la automatización de la captura de datos[67], se facilitó la posibilidad de registrar y conservarlo todo. Protocolos de eliminación son difíciles de implementar y cuando los recursos son limitados, las justificaciones o excusas facilitan mantener la información de forma permanentemente, más aún, si las clasificaciones son llevadas por órganos públicos.

La obsolescencia documental es propia de los registros en papel, ya que ocupaban un espacio físico, su crecimiento requiere salas o bodegas y la búsqueda de información se complejiza. Si bien no podríamos argumentar que el derecho tenga como uno de sus fines el olvidar las acciones del pasado, sino más bien poder entregar una respuesta justa a los errores cometidos, tampoco podríamos apoyar la idea de la razonabilidad del registro permanente en aquellos casos en que se han cumplido las sanciones. Un registro eterno que tenga efectos en el individuo no parece justo en todos los posibles errores cometidos[68].

No parecen existir incentivos suficientes, en nuestro sistema, para que se eliminen datos. La clave de los registradores es la acumulación de datos, el volumen de información. Muchas de nuestras instituciones públicas sufren del "Síndrome de Diógenes Electrónico". Acumular todos los datos posibles, aun cuando no tengan un destino claro, ya que en algún momento podrían ser útiles.

El estar en una base de datos de registro de condenados e imputados y no serlo, es un problema serio y grave. Primero, no es evidente para el individuo el conocimiento sobre su clasificación dentro del registro. Segundo, el desconocimiento hace ineficaz los derechos de rectificación, cancelación u oposición. Como consecuencia de no tener conocimiento ni control sobre nuestra infor-

65 Noble (2018) p. 137.
66 Véliz (2021) p. 155.
67 Véliz (2021) p. 156.
68 Eubanks (2018) p. 187.

mación ni los efectos en asignación de derechos o discriminación que podría tener, perdemos nuestra autodeterminación informativa. El caso más extremo de pérdida de nuestras garantías fundamentales podríamos llamarlo adjudicación errónea de datos personales, esto es, la mera incorporación de un sujeto a dicha base le asigna un dato personal, no conocido ni tampoco controlado.

Independiente de lo que se pueda argumentar, que el dato está en calidad de sobreseído o en calidad de no formalizado, la mera existencia de un nombre propio en dichas bases podría producir sesgo por parte de las personas encargadas de tomar decisiones con esa información. Pertenecer a la base de datos SAF del Ministerio Público es un antecedente negativo y hace presumir que la persona ha participado en diferentes grados en conductas contrarias a la ley. El solo hecho de pertenecer a una base es un dato personal, ya que, responde a la definición básica de dato personal: se le asignan al titular características por estar ahí.

Los registros SAF evidentemente van a producir un efecto en el discernimiento de los fiscales. En estos casos existe una alta posibilidad de que tenga algún grado de responsabilidad. Crea un indicio para el fiscal de criminalidad por el estar en una base. Sería interesante conocer el razonamiento que realiza un fiscal en los casos en que la persona esté en el registro, pero que sea sobreseída definitivamente. En ese sentido se extrema el argumento cuando nos damos cuenta que se retiene información incluso de los denunciantes. Respecto a estos últimos, se conservan los datos personales de la misma forma que la de los condenados, constituyendo una evidente vulneración a sus derechos fundamentales, que como ha resuelto el TEDH, podría generar una estigmatización[69].

Olvidar es una virtud personal, pero también lo es para las sociedades. El olvido social permite dar segundas oportunidades a faltas menores, errores o insolvencias. Sociedades que no olvidan pierden su capacidad de perdonar[70]. La capacidad que tengan las sociedades de olvidar se traduce en beneficio para el individuo y también como un beneficio para toda la sociedad. Olvidar hechos pasados que no fueron probados o que han sido pagados es un antecedente para volver a empezar la vida con una segunda oportunidad[71]. No es únicamente en la autodeterminación informativa que encontramos la justificación legal de la eliminación de la información por aquellos órganos que no se relacionan con su función, sino que también es permitir que se

69 The European Court of Human Rights (2008), considerando 122.
70 Véliz (2021) p. 155.
71 Véliz (2021) p. 155.

pueda empezar de cero a quien no ha tenido razones suficientes para ser condenado o donde la misma ley le autorizó seguir adelante sin registrarse antecedentes de acciones ilegales.

8. LOS ARGUMENTOS FALTANTES EN LA CORTE

La discusión europea en materia de retención de datos por parte de autoridades es iluminadora en relación a los puntos clave de la dignidad de la persona humana. Dicha discusión nos sirve como antecedente comparativo para revisar los fundamentos utilizados por nuestros tribunales en discusiones similares y evidenciar de manera breve los razonamientos que no solo podrían, sino que deberían a lo menos sembrar discusión en los tribunales de nuestro país.

En primer lugar, aún falta que en la discusión local se ponga en el centro la finalidad del tratamiento y la retención razonable de datos. Se torna necesario pensar y limitar las facultades en relación a su mandato legal y determinar el límite de la protección a la dignidad frente al actuar del Estado.

En ese sentido, el registro de los delitos que pudieron ser las bases de datos de los "por si acaso" no parece justificarse en un Estado Democrático de Derecho. Ya hemos tenido pasados distópicos en regímenes socialistas que intentaron el control absoluto, de listas de sospechosos y de incentivos perversos a encontrar responsables aún en los grupos de inocentes. El más clásico ejemplo literario es el trabajo de Orwell en *1984*, que es un reflejo de los deseos de control social de la Alemania Nazi y de la Unión Soviética[72].

En segundo lugar, el Principio de Transparencia, que trae consigo las preguntas necesarias a hacerse en el caso concreto para resolver un asunto jurídicamente controvertido: ¿dónde están?, ¿cuánto duran?, ¿cuándo se borran?, etc. Tal principio no solo busca responder tales interrogantes, sino que apunta a permitir un acceso a los datos de cada uno de los titulares. Es posible que el principio de transparencia en el derecho nacional se asocie únicamente al artículo 8 de la Constitución Política de la República, que manda ser públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y procedimientos. No obstante, intrínsecamente podemos obtener de principios generales del derecho –que nadie niega que deben estar presentes-, el contenido del Principio de Transparencia en un sentido europeo. La buena fe y la igualdad de poder negociación, que permean el derecho privado y que el derecho público busca propender, permiten extraer que en nuestro ordenamiento jurídico no

[72] Richards (2022) p. 136.

es ajeno el tener que informar de forma transparente, inteligible y de manera clara, no buscando aprovecharse de aquel en desigualdad. En otras palabras, tal descripción es nada menos que el principio de transparencia con una lógica europea aplicada a la protección de datos personales.

En tercer punto, además debe añadirse en el razonamiento de los tribunales que los fines del tratamiento de los datos deben ser determinados, explícitos y legítimos. Estas condiciones del tratamiento no parecen ser tan claros en el caso de la Fiscalía, al ni siquiera contar con una regulación exhaustiva y al argumentar la existencia del registro SAF en disposiciones que no lo mencionan de manera explícita. Es relevante que, sin ir más allá de las fronteras chilenas, encontremos que el articulo 9 de la Ley N° 19.628 exige el principio de finalidad y como ya se expuso, esta norma, no hace excluyente al Ministerio Publico de ella. El elemento central que debería plantear la Corte Suprema desde la garantía fundamental de protección de datos es determinar si el Ministerio Público está cumpliendo el principio de finalidad.

Por último y en la línea expuesta, debemos cuestionarnos y analizar el período por el cual se utilizan los datos, este debe ser adecuado a los fines solicitados. Si no existe una función directa sobre la que es necesario mantener la información, su mantenimiento carecería de base de legitimidad. Es manifiesto a esta altura que la Corte Suprema ha optado por utilizar otras aristas en la resolución de los casos, a diferencia de la jurisprudencia comparada revisada, donde se evidencian criterios de "gravedad", "tiempo" e "interés en una sociedad democrática", entre otros.

9. IDEAS FINALES

El principio de objetividad de las actuaciones del Ministerio Público requiere parámetros claros, precisos e imparciales. Esos parámetros generalmente se enfocan en que las diligencias también busquen acreditar la inocencia del imputado[73]. Sin embargo, la objetividad se consigue de diferentes formas. Una de ellas es la eliminación de prejuicios por parte del investigador. Que la Fiscalía recuerde en los casos en que haya aparecido el nombre de una persona, más aún si esta no fue condenada, evidentemente viola la idea de juicio objetivo, ya que constituye una predeterminación del investigador frente a la posibilidad de que el sujeto tenga participación, es más probable que sea un "ahora sí lo atrapamos" a un "qué extraño, nuevamente este individuo está siendo acusado".

73 FN (2014) p. 14.

Efectivamente, podemos concluir que nuestro ordenamiento no ha determinado un tiempo de eliminación de registros, lo que dificulta la toma de decisión por parte del Ministerio Público. Si bien en el análisis no es razonable la existencia de registros indefinidos, más aún de casos en que no se ha acreditado la responsabilidad penal. La inexistencia de una norma de retención ha dificultado claramente la aplicación de un periodo razonable de eliminación de registros. En ese sentido, el Ministerio Público con justa razón podría replantear su normativa de eliminación de datos. Aquello explica por qué únicamente queda para los titulares requerir a tribunales la eliminación de su información, la que debería darse en los casos similares a este, y dejando en evidencia que se hace necesario –más que nunca– la actualización de la normativa que permita ajustarse a la correcta protección de las garantías fundamentales de la protección de los datos personales en una sociedad democrática y de Estado de Derecho, como la chilena que debería cuestionar los acercamientos totalitarios.

10. BIBLIOGRAFÍA

Álvarez Hernando, Javier (2019): "Protección de Datos Personales en el Proceso" XII Congreso Nacional de Abogacía, Consejo General Abogacía Española e Ilustre Colegio de Abogados de Valladolid. Disponible en: https://www.formacionabogacia.es/pluginfile.php/58511/mod_resource/content/1/Protección%20de%20datos%20personales%20en%20el%20proceso%20penal.pdf

Amnesty International (2015): "#Unfollowme: 5 Reasons We Should All Be Concerned About Government Surveillance.". Disponible en: https://www.amnestyusa.org/unfollowme-5-reasons-we-should-all-be-concerned-about-government-surveillance/

Clarke, Roger (2015): "Data retention as mass surveillance: the need for an evaluative framework", International Data Privacy Law, vol 5, N° 2, pp. 121-132.

EDPB – European Data Protection Board (2021): Recomendaciones 01/2021 relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal. Disponible en: https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_es.pdf

Eubanks, Virginia (2018): Automating Inequality (st. Martin's Press, New York).

Fabricant, Chris (2022): Junk Science and the American Criminal Justice System (New York, Akashic Books).

Fiscalía Nacional (2023): "Fiscalía de Chile comenzará a usar sistema de inteligencia artificial que detecta estructuras criminales", 22 de marzo. Disponible en: http://www.fiscaliadechile.cl/Fiscalia/fiscalias_nacional/noticias_det.do?id=21921

Heredero Higueras, Manuel (1983): "La Sentencia del Tribunal Constitucional de la República Federal Alemana Relativa a la Ley del Censo de Población de 1983", *Documentación Administrativa*, N° 198, pp. 139-158.

Horvitz Lennon, María Inés y López Masle, Julian (2006): Derecho Procesal Penal Chileno (Editorial Jurídica, Santiago, tomo II).

Lara, Carlos, Pincheira, Carolina y Vera, Francisco (2014): "La privacidad en el sistema legal chileno", Derechos Digitales, Policy Paper N° 08. 94 pp. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf

Leturia, Francisco (2016): "Fundamentos jurídicos del derecho al olvido. ¿un nuevo derecho de origen europeo o una respuesta típica ante colisiones entre ciertos derechos fundamentales?", Revista Chilena de Derecho, vol 43, N° 1, pp. 91-113.

Ministerio Público (2011): Oficio FN N° N° 028/2011. Disponible en: http://www.fiscaliadechile.cl/comisionjuridica/docu/inst/of_28.pdf

Ministerio Público (2014): "Instrucción General que imparte criterios de actuación aplicables a la Etapa de Investigación en el Proceso Penal" Oficio FN N° 133/2010. Disponible en: http://web.uchile.cl/archivos/derecho/CEDI/Normativa/Oficio%20Fiscal%20Nacional%20133%202010%20Parte%201.pdf

Ministerio Público (2022): Red Gestión Penal, Minuta del Proyecto, de 20 de junio. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj7k5CD-fz_AhVMppUCHZksD6IQFnoECAkQAQ&url=http%3A%2F%2Fwww.fiscaliadechile.cl%2Ftransparencia%2F2022%2Ftrimestre2%2FOficio_DEN_N_187_22_MP_InformaGlosa_Articulo_14_N_13_Ley_21395_Proyecto_subtitulo29.docx&usg=AOvVaw2zvmJRAbnG4Cf9YTj_D1t8&opi=89978449

Noble, Safiya Umoja (2018): Algorithms of Oppression (New York, New York University Press).

O'neil, Catherine (2016): Weapons of Math Destruction: How Big Data Increases Inequality and Threats Democracy (New York, Crown).

PDPC (2022): Guia Básica de Anonimización, emitida por la Personal Data Protection Commission Singapore (traducida por la Agencia Española de Protección de Datos). Disponible en: https://www.aepd.es/es/documento/guia-basica-anonimizacion.pdf.

Reusser Monsálvez, Carlos (2021): Derecho al Olvido: la protección de datos personales como límite a las libertades informativas (Santiago, Ediciones DER).

Richads, Neil (2022): Why Privacy Matters (United States, Oxford University Press).

Snowden, Edward (2014): "Edward Snowden interview - the edited transcript", The Guardian, entrevista hecha por Alan Rusbridger y Ewen MacAskill. Disponible en: https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript

Véliz, Carissa (2021): Privacy is Power (New York, Melville House Publishing).

Vivanco Martínez, Ángela (2017a) "El derecho al olvido y el eventual poder que tenemos sobre nuestra propia "historia", Sentencias Destacadas 2016, N 13, pp. 349-382.

Vivanco Martínez, Ángela (2017b) "Volviendo a discutir sobre privacidad: el retorno de "1984"", El Libero, 7 de septiembre. Disponible en: https://ellibero.cl/opinion/volviendo-a-discutir-sobre-privacidad-el-retorno-de-1984/

Normas e instrumentos citados

Reglamento sobre Procedimiento de Custodia, Almacenamiento y Eliminación de Registros, Documentos y Similares (26/10/2020), Resolución FN/MP N°1092/2020.

European Court of Human Rights (1978) Case of K. and Others v. Germany, considerando 50.

Declaración Universal de Derechos Humanos (1948).

European Court of Human Rights (2012) M.M. v. The United Kingdom, considerando 187.

Tribunal Constitucional (2011) rol 1894-2011, N° 30.

The European Court of Human Rights (2020) G. v. the United Kingdom.

The European Court of Human Rights (2013) M.K. v. France.

The European Court of Human Rights (2017) A. v. France.

European Court of Human Rights (2008) S. and Marper v. The United Kingdom.

European Court of Human Rights (2013) M.K. v. France.

European Court of Human Rights (2009) B.B v. France.

Constitución Política de la República de Chile (11/08/1980).

Ley Orgánica Constitucional del Ministerio Público (15/10/1999)

Ley 19.628 (28/10/1999).

Código Procesal Penal (12/10/2000)

Ley 20.931 (05/07/2006).