REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 9 NÚM. 1 (2020) • PÁGS. 207-225 • DOI 10.5354/0719-2584.2020.56843
RECIBIDO: 16/3/2020 • APROBADO: 23/4/2020 • PUBLICADO: 30/6/2020

INFORMES

Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: El caso SyRI

Algorithmic valoration before human rights and the European Convention on Human Rights and the General Data Protection Regulation: The SyRI case

Guillermo Lazcoz Moratinos y José Antonio Castillo Parrilla
Universidad del País Vasco, España

RESUMEN La Corte de Distrito de La Haya dictó el 5 de febrero de 2020 una sentencia sobre el Sistema de Indicación de Riesgos (SyRI), por la que considera que: i) es lícito utilizar instrumentos de este tipo siempre que exista un interés público que lo justifique y se tomen las medidas adecuadas para garantizar la mínima injerencia necesaria en el derecho a la privacidad; y ii) que la implementación de SyRI no ofrece garantías suficientes como para considerar que este sistema en concreto respeta el necesario juicio de proporcionalidad que debe superar toda injerencia en la privacidad de acuerdo con el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH). A lo largo de este trabajo reflexionaremos en detalle sobre las consideraciones de la Corte en esta sentencia en relación con el respeto a la privacidad, la obtención masiva de datos y la opacidad con que funcionan los algoritmos de análisis de datos masivos.

PALABRAS CLAVE SyRI, vigilancia masiva, algoritmos, inteligencia artificial, derecho a la privacidad, CEDH.

ABSTRACT Last 5TH of February 2020, the District Court of The Hague published a pronouncement on the System of Risk Indicators (SyRI) by which it considers: (1) that it is lawful to use such an instrument whenever a public interest is involved and appropriate measures are taken to guarantee the minimum interference in the right of privacy; and (2) that, since the specific implementation of SyRI does not offer those appropriate guarantees, SyRI legislation does not respect the proportionality judgment between interference and the right of privacy according to article 8 of the European Convention on Human Rights (ECHR). Through this essay we reflect in detail on the considerations of the Court on the right of privacy, the massive collection of data and the opacity of algorithms for the analysis of big data.

KEYWORDS SyRI, massive surveillance, algorithms, artificial intelligence, right to privacy, ECHR.

Introducción

La sentencia[1] dictada el 5 de febrero de 2020 por la Corte de Distrito de La Haya sobre el Sistema de Indicación de Riesgos (SyRI) ha causado un justificado revuelo entre juristas de todo el mundo, ocupados de analizar el funcionamiento y los riesgos de la popularización y mejora de sistemas de gestión pública basados en algoritmos, así como de especialistas en derecho digital, protección de datos, inteligencia artificial y de la ciudadanía en general.

Hasta el momento, el algoritmo utilizado por un poder del Estado que más atención ha suscitado en la literatura jurídica es COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), una herramienta utilizada por los tribunales de algunas jurisdicciones de Estados Unidos[2] para evaluar el riesgo de reincidencia de los delincuentes, la cual podríamos categorizar como una inteligencia artificial judicial de valoración del riesgo (IAJVR) (Miró Llinares, 2018). Dicho algoritmo adquirió gran relevancia a partir del caso *Loomis*,[3] en el que el Tribunal Supremo de Wisconsin entendió que su utilización respetaba el derecho al debido proceso y a la igualdad de los acusados. El algoritmo COMPAS fue ampliamente cuestionado por el informe de ProPublica, en el que se denunciaban los sesgos raciales que reproducía,[4] e incluso se ha llegado a señalar que esta herramienta no es más precisa ni justa que las predicciones hechas por personas con poca o ninguna experiencia en justicia penal (Dressel y Farid, 2018; Lin y otros, 2020).

Este caso ilustra que la normativa relacionada con algoritmos y, en general, sistemas de inteligencia artificial, es tardía e insuficiente (Boix, 2020: 258), tanto en lo que se refiere a la situación de los propios algoritmos —expresamente excluidos en la normativa tanto de propiedad intelectual e industrial—, como en cuanto a las consecuencias que su uso tiene en los sectores público y privado. Todo ello confiere mayor importancia a este fallo, pues marca ciertos límites a una legislación —aquella sobre el uso de sistemas de inteligencia artificial basados en procesamiento de datos en masa— que aún está en un proceso muy embrionario de desarrollo. Muestra de ello

1. Sentencia del 5 de febrero de 2020 de la Corte de Distrito de la Haya (Rechtbank Den Haag). Referencia: ECLI:NL:RBDHA:2020:865. Disponible en https://bit.ly/2SpN2O4.

2. Broward County, Florida, y los estados de Nueva York, Wisconsin y California, entre otros (Kirkpatrick, 2017).

3. Sentencia del caso *Wisconsin con Loomis*, 881, N.W.2d 749, 7532 (Wis, 2016), 13 de julio de 2016. Se recomiendan los análisis sobre dicho caso de Romeo Casabona (2018) y De Miguel Beriain (2018).

4. Julia Angwin, Jeff Larson, Surya Mattu y Lauren Kirchner, «Machine bias», *ProPublica*, 23 de mayo de 2016, disponible en https://bit.ly/2YrjDqu.

es que la Unión Europea ha publicado recientemente dos importantes documentos que, sin embargo, no pasan de ser un libro blanco sobre inteligencia artificial[5] y una estrategia de política normativa para los próximos cinco años.[6]

La sentencia ha sido celebrada por el relator especial sobre la extrema pobreza y los derechos humanos de Naciones Unidas, Philip Alson, ya que la considera una clara victoria y un contundente precedente para otros tribunales,[7] lo que coincide con la preocupación mostrada en un informe presentado ante la Asamblea General de Naciones Unidas[8] por las graves amenazas que el estado de bienestar digital representa para los derechos humanos.

En estas páginas, a partir de dicho fallo, pretendemos no solo dar cuenta del funcionamiento de SyRI y su encaje en aquellas normas que en Europa se encargan de proteger el derecho a la privacidad y la protección de datos. Buscamos también reflexionar sobre algunas de las implicaciones que tienen este tipo de sistemas en relación con nuestra privacidad, así como con ciertas instituciones fundamentales de todo ordenamiento como son, entre otros, los principios de seguridad jurídica e interdicción de la arbitrariedad. Aunque el caso se circunscribe al contexto normativo europeo, entendemos que su relevancia trasciende dicho ámbito geográfico. Por primera vez, un tribunal ha acotado la utilización gubernamental de una herramienta como SyRI para combatir el fraude fiscal, sobre la base del derecho a la privacidad y a la protección de datos en el contexto de la utilización de datos masivos por parte de sistemas de inteligencia artificial.

Más allá de la falta de precedentes en la materia, el estudio de esta sentencia podría ser de particular interés en Chile, cuyo ordenamiento jurídico sobre protección de datos está siendo objeto de importantes modificaciones en los últimos años, tanto a nivel constitucional como legislativo. Además de la consagración del derecho a la protección de datos a través de la Ley 21.096, del 16 de junio de 2018, que modificó el artículo 19 de la Constitución, en 2017 se inició un proyecto de ley[9] para modificar la

5. «Libro blanco sobre la inteligencia artificial: Un enfoque europeo orientado a la excelencia y la confianza», Comisión Europea, Bruselas, 19 de febrero de 2020, COM (2020) 65 final, disponible en https://bit.ly/3feCQSs.

6. «Una estrategia europea de datos», Comisión Europea, Bruselas, 19 de febrero de 2020, COM (2020) 66 final, disponible en https://bit.ly/3fb3DyV.

7. «Landmark ruling by Dutch court stops government attempts to spy on the poor – UN expert», Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 5 de febrero de 2020, disponible en https://bit.ly/3dcResD.

8. Informe anual A/74/493, 11 de octubre de 2019, del relator especial sobre la extrema pobreza y los derechos humanos, sobre el estado de bienestar digital y los derechos humanos. Disponible en https://bit.ly/3aSdXbD.

9. Boletín 11092-07. Puede consultarse el histórico y el estado de tramitación del proyecto de ley en https://bit.ly/35pUjTc.

regulación actual del tratamiento de datos personales.[10] El objetivo general del proyecto es adecuar la Ley 19.628 a los estándares internacionales de la Unión Europea, la APEC y la OCDE,[11] y entre otros fundamentos, el preámbulo de dicho proyecto de ley reconoce el Reglamento General de Protección de Datos (RGPD) de la Unión Europea como el estándar más alto por el que optar. A la luz de este particular contexto, creemos que el acercamiento a esta sentencia puede resultar prolífico para la doctrina chilena, tanto para identificar posibles vacíos en la literatura nacional, como para desarrollar posteriores análisis en la materia.[12]

SyRI vista por la Corte de Distrito de La Haya

El Sistema de Indicadores de Riesgo es un instrumento desarrollado por el Gobierno neerlandés con el objetivo de prevenir y combatir el fraude a la seguridad social. El sistema se sirve de una infraestructura técnica y procedimientos asociados a través de los cuales se relacionan y analizan datos anonimizados en un entorno seguro orientados a producir informes de riesgo (párrafo 3.1 de la sentencia).

En otras palabras, SyRI se sirve de un algoritmo de procesado de datos en masa: estos datos son anonimizados y luego analizados y relacionados entre sí en un entorno seguro. El resultado del procesado de datos es informes de riesgo sobre la probabilidad de defraudar a la seguridad social, por ejemplo, a través de un uso inapropiado de fondos o del incumplimiento de la normativa correspondiente. Un informe de riesgo, por tanto, identifica a una persona natural o jurídica probable infractor o defraudador, y por ello aconseja que se le investigue (párrafo 3.2). Se trata, pues, de un instrumento de ayuda para las autoridades públicas encargadas de la investigación del fraude a la seguridad social. Éstas podrán servirse de las inferencias de SyRI[13]

10. Su normativa básica actual es la Ley 19.628, del 28 de agosto de 1999. Puede consultarse el texto vigente en https://bit.ly/3aWN9qT.

11. «Resumen de las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales», OCDE, 2002, disponible en https://bit.ly/3bY7Tj7. Sobre esta necesidad llamó la atención Viollier (2017: 47) antes de que se iniciara su tramitación el proyecto de modificación de la Ley 19.628: «Es necesario, por otra parte, introducir los principios reconocidos por la OCDE, tales como el de proporcionalidad, calidad de los datos, especificación del propósito o finalidad, limitación de uso, seguridad de los datos, acceso y oposición de su titular, y transparencia, entre otros».

12. Como ejemplo de ello, el excelente análisis a partir de fuentes europeas llevado a cabo por Contreras Vásquez y Trigo Kramcsák (2019), acerca del concepto de interés legítimo.

13. Podemos considerar que SyRI es una técnica de vigilancia que hace «perfiles preventivos» (*preemptive profiling*) en los términos descritos por van Brakel y de Hert: «El propósito principal es, por tanto, agrupar los datos de tal manera que permitan inferir información y proponer predicciones o expectativas. Los perfiles obtenidos son patrones que son, a su vez, el resultado de un procesamiento probabilístico de los datos. No describen la realidad, sino que son detectados en las bases de datos mediante agregación, extracción y depuración de los datos» (van Brakel y De Hert, 2011: 176; la traducción es nuestra).

(concretados en informes de riesgo sobre personas concretas) para hacer investigaciones singularizadas y, en caso de detectar incumplimientos o fraudes, sancionar.

El funcionamiento de SyRI se basa en la agregación (previa anonimización), triangulación y posterior análisis de grandes cantidades de datos (detallados en el párrafo 4.17 de la sentencia y de los que daremos cuenta más adelante) en poder de diversas administraciones públicas, que forman un acuerdo de colaboración por el cual intercambian datos a través de SyRI. La agregación, comparación y análisis de los datos compartidos permite identificar perfiles de riesgo de fraude a la seguridad social (párrafo 3.3).

La práctica que acabamos de describir ya existía antes de que Países Bajos desarrollara una normativa específica que la contemplase (párrafo 3.5), que es la que la Corte de Distrito de La Haya examina en este caso a la luz del artículo 8 del Convenio Europeo de Derechos Humanos.

En 2014 entró en vigor la normativa que resulta específicamente aplicable a SyRI: los artículos 64 y 65 de la Ley SUWI[14] y el capítulo 5.a del Decreto SUWI[15]. A continuación, explicaremos de manera breve el funcionamiento del algoritmo de acuerdo con la normativa SyRI. En este punto debemos agradecer la claridad del trabajo van Dalen y otros (2016), que sintetiza con gran claridad información que se encuentra diseminada y confusa a lo largo de la sentencia.[16]

Cada año, el Ministerio de Seguridad Social y Empleo de Países Bajos establece temas y prioridades de investigación. Basándose en estas prioridades, instituciones públicas pueden iniciar proyectos de intervención utilizando SyRI. El sistema debe ponerse en funcionamiento a través de un acuerdo de cooperación entre diversas autoridades públicas presidido por el Ministerio. El propósito del acuerdo de cooperación es, como hemos dicho, lograr una colaboración pública integral en relación con la prevención y el combate del fraude a la seguridad social (párrafo 4.4). Las autoridades públicas que deseen utilizar SyRI deberán enviar una solicitud al Ministerio a este efecto y constituir un acuerdo de colaboración, en el que se especifiquen objetivos concretos, aspectos de organización, fecha de inicio y duración del proyecto, datos a recabar y metodología de trabajo (van Dalen y otros, 2016: 12). El Ministerio será responsable del tratamiento[17] de acuerdo con el artículo 4.7 del RGPD. Se pretende evitar abusos estableciendo una serie de requisitos administrativos para formar parte

14. Los artículos referidos de la Ley SUWI pueden consultarse en https://bit.ly/2KQ5XNZ.

15. El capítulo sobre SyRI del Decreto SUWI puede consultarse en https://bit.ly/35rSftT.

16. La explicación contenida en los párrafos siguientes combina los párrafos de la sentencia (citados convenientemente) con la explicación de van Dalen y otros (2016: 12-13).

17. El RGPD considera responsable del tratamiento (artículo 4.7) a «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento».

del acuerdo de colaboración, como la obligación para las autoridades participantes de aceptar de manera pública el proyecto y justificar su necesidad y proporcionalidad (párrafo 4.9).

Por otro lado, si bien la Fiscalía y la Policía son partes en los acuerdos de cooperación para equipos de intervención y están representadas en el Comité Directivo Nacional para Equipos de Intervención (LSI, por sus siglas en neerlandés), no son un «cuerpo designado», de acuerdo con el artículo 64 de la Ley SUWI, y por lo tanto no podrán formar parte de acuerdos de colaboración según lo establecido en el citado artículo 64 de la Ley SUWI y en el Decreto de desarrollo. Tampoco podrán requerir la aplicación de SyRI ni enviar datos con tal propósito al Ministerio. Sí podrán solicitar informes de riesgo en la medida en que sean necesarios para el cumplimiento de sus obligaciones estatutarias (párrafo 4.10). Si el Ministerio aprueba el proyecto, las instituciones participantes deben proporcionar los paquetes de datos a la Oficina de Información (IB, por sus siglas en neerlandés). La IB seudonimiza los datos, y los compara con otros paquetes de datos para obtener perfiles que son evaluados de acuerdo con el modelo de riesgo, lo que da lugar a «perfiles de riesgo». Sólo respecto de estos últimos la IB desanonimiza los datos y envía este perfil de riesgo al Ministerio a un segundo análisis, para luego destruir el resto de los datos en el plazo de cuatro semanas.[18]

Respecto de los «perfiles de riesgo», el Ministerio envía una notificación al Registro de Notificaciones de Riesgo y a la Administración correspondiente, que iniciará

18. Puede ser conveniente aclarar la terminología para distinguir tres operaciones con datos importantes: *anonimizar*, *seudonimizar* y *desanonimizar*. Estas tres operaciones tienen lugar con datos que en algún momento de su procesado o tratamiento son personales. Los datos personales que son sometidos a un proceso por el cual quedan completamente disociados del sujeto al que se refieren (es decir, pasan a ser anónimos) han sido anonimizados. Los datos personales que son sometidos a un proceso de disociación respecto del sujeto al que se refieren, pero que es reversible, han sido seudonimizados. El considerando 26.º se refiere a los datos seudonimizados del siguiente modo: «Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que en forma razonable pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos». Si consideramos las explicaciones que acabamos de dar, sólo es posible revertir el proceso de seudonimización, no el de anonimización. Por tanto, cuando hablamos de *desanonimizar* los datos, hacemos referencia al proceso de reversión de la seudonimización de datos. Este proceso es posible en el caso de SyRI porque la IB sólo seudonimiza los datos, somete los datos seudonimizados a tratamiento, y revierte el proceso respecto de aquellas personas que han sido detectadas como perfiles de riesgo por el sistema.

las investigaciones pertinentes. En el plazo de veinte meses desde el inicio del proyecto, las instituciones implicadas deberán remitir informes sobre las investigaciones a efectos de evaluar los modelos de riesgo, trámite con el que concluye cada proyecto. Por último, los informes de riesgo no serán conservados durante más tiempo del necesario de acuerdo con el propósito para el que son elaborados y nunca más de dos años (párrafo 4.14). El Registro de Notificaciones de Riesgo puede retener la información que considere relevante a efectos de notificaciones durante un período de dos años. Los titulares de datos que son potenciales sujetos investigados (en la práctica, toda la población) podrán preguntar en este registro si han sido objeto de investigación.

El fallo de la Corte de Distrito de La Haya

Como hemos adelantado, la Corte de Distrito de La Haya evaluó este cuerpo normativo en relación con el artículo 8 del CEDH, que recoge el derecho al respeto a la vida privada y familiar en los siguientes términos:

> 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

La Corte de Distrito de La Haya declaró que la normativa SyRI (en concreto, el artículo 65 de la Ley SUWI y el capítulo 5.a del Decreto SUWI) es incompatible con el artículo 8.2 del CEDH en la medida en que la injerencia que supone SyRI en el derecho a la privacidad por parte del Gobierno neerlandés no cumple con las garantías exigidas por los juicios de necesidad y proporcionalidad contenidos en dicho artículo.

Para acercarse a la cuestión central del caso, es decir, si la normativa SyRI infringe o no el derecho a la privacidad, la Corte establece cuál es la base jurídica del derecho. Según los artículos 93 y 94 de la Constitución neerlandesa, la Corte entiende que ante esta normativa debe aplicarse el derecho humano al respeto a la vida privada y familiar contenido en el artículo 8 del CEDH (párrafo 6.20), a partir de la interpretación que del mismo ha hecho el Tribunal Europeo de Derechos Humanos (TEDH) y, en este sentido, determina que este derecho está íntimamente relacionado con el

derecho a la protección de los datos personales (párrafos 6.23 y ss.).[19] Del mismo modo, examina la legislación vigente de la Unión Europea, cuya Carta de los Derechos Fundamentales recoge en sus artículos 7 y 8 los derechos al respeto a la vida privada y familiar y a la protección de datos de carácter personal, y determina que el RGPD es directamente aplicable (párrafo 6.28). A partir de este punto, examina la relación entre el CEDH y el derecho de la Unión Europea y establece un aspecto clave para la interpretación de la violación o no del artículo 8.2 del CEDH: no hay razones para pensar que la protección mínima del derecho al respeto de la vida privada, que incluye la protección de los datos personales, en virtud del CEDH tenga un alcance menor que la protección de datos prevista en la Carta y en el RGPD sobre la base de los principios generales establecidos en ella (párrafo 6.41). Por ende, la Corte interpretará el artículo 8.2 del CEDH sobre la base de los principios generales contenidos en el artículo 5 del RGPD, en particular, el principio de transparencia, el principio de limitación de la finalidad y el principio de minimización de datos (párrafo 6.40).

A partir de estas precisiones, la Corte valora la extensión y severidad de la injerencia que supone SyRI en el derecho a la privacidad. La llamativa conclusión a la que llega es que no puede evaluar con exactitud qué es SyRI, dado que el Gobierno no ha hecho pública —ni ha aportado al procedimiento— información objetiva y verificable sobre el modelo de riesgo en el que se basa SyRI (párrafo 6.49). Considera que la normativa ofrece margen para el desarrollo de técnicas como *deep learning*, *data mining* y la elaboración de perfiles de riesgo,[20] y aunque no pueda determinar

19. Esta vinculación que la Corte recoge de la jurisprudencia del TEDH puede resumirse de la siguiente forma: dicha jurisprudencia viene consolidando que la noción de vida privada del artículo 8 no se limita a un «círculo interior» en el que el individuo puede vivir su vida personal como él elija excluyendo el mundo exterior. El artículo 8 protege el desarrollo de la autonomía personal en relación con el mundo exterior y con las relaciones que el individuo desea establecer en él, de modo que ha construido el «derecho a la autodeterminación» (*self-determination*), a la «autonomía personal» (*personal autonomy*) y al «desarrollo personal» (*personal development*) (párrafo 6.23). En relación con esta noción de privacidad, la jurisprudencia del TEDH ha reconocido el derecho a la identidad personal como un subaspecto del derecho al respeto por la vida privada del artículo 8 (párrafo 6.24), íntimamente ligado a la protección de los datos personales. En la doctrina en lengua castellana, estaríamos en el ámbito de la «autodeterminación informativa», definido como el control que ostentan las personas sobre el uso por terceros de información sobre ellas mismas (Murillo de la Cueva, 2009: 11). Por tanto, afirma la Corte, al no ser la protección de datos un derecho independiente en el marco del Convenio, es de fundamental importancia para el respeto a la vida privada del artículo 8 (párrafo 6.25).

20. Según el RGPD, la elaboración de perfiles es «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física» (artículo 4.4). Dicho tratamiento automatizado de datos, entre otras posibilidades, podría consistir en aplicar minería de datos (*data mining*) o de aprendizaje pro-

con exactitud qué clase de tratamiento desarrolla la herramienta SyRI, da por hecho que elabora perfiles de riesgo basados en datos históricos, personales o de otra clase (párrafo 6.53), lo cual queda avalado por el extenso elenco de categorías de datos que SyRI recoge en el Decreto SUWI y de los que la propia sentencia se hace eco en el párrafo 4.17. Además, indica que la normativa no prevé ninguna obligación de informar a aquellas personas cuyos datos son procesados con este propósito o de que se les ha aplicado un informe de riesgo, sino tan solo de publicar de manera oficial que una de las autoridades públicas involucradas va a iniciar un proyecto de investigación según la normativa SyRI y, en su caso, de dar acceso a los perfiles de riesgo a aquellas personas que lo soliciten de manera expresa (párrafo 6.54).[21]

La (i)legitimidad de la injerencia en el derecho a la privacidad

Del mismo modo que el Tribunal Europeo de Derechos Humanos, la Corte de Distrito de La Haya, después de afirmar la aplicabilidad del Convenio y la existencia de una injerencia, analizó en una segunda fase si dicha injerencia constatada puede considerarse justificada de acuerdo con el CEDH, determinando que la injerencia esté prevista por la ley; y luego, que sea necesaria en una sociedad democrática, lo cual implica valorar la necesidad de la medida en sí, además de la proporcionalidad entre los medios empleados y los fines perseguidos.

Acerca de la previsión por ley, en un sentido formal implica tener fundamento jurídico en el derecho nacional, si bien el TEDH ha entendido que debe añadirse un fundamento material, o de «calidad de la ley», lo que implica que la injerencia ha de ser accesible y previsible para la ciudadanía, de modo que los individuos puedan disponer de información suficiente sobre la norma jurídica aplicable, se les permita regular su conducta a partir de ella y prever en un grado razonable las consecuencias que una acción determinada puede acarrear (EPRS, 2018: 38). La Corte de Distrito de La Haya reconoció que, para el cumplimiento de los requisitos de accesibilidad y

fundo (*deep learning*). La Corte se refiere a estas técnicas en particular puesto que la parte demandante refiere en su argumentación que el Estado las utiliza (párrafos 6.45 y ss.).

21. En este punto la Corte desarrolla una interesante, aunque no aplicable al caso, interpretación relativa al artículo 22 del RGPD, que regula la toma de decisiones individuales automatizadas. Argumenta la Corte que un informe de riesgo genera por sí un efecto que afecta de manera significativa al interesado, aunque dicho informe no necesariamente conlleve una investigación o sanción, ya que puede almacenarse durante dos años y puede ser utilizado durante veinte meses por las autoridades participantes del proyecto de SyRI pertinente y, además, puede hacerse llegar a la Fiscalía o a la Policía, a petición de ellas (párrafo 6.59), lo cual implica que el propio informe de riesgo, dados sus efectos, puede considerarse de acuerdo con esta interpretación como una decisión individual automatizada en los términos del artículo 22. En la segunda parte de este trabajo analizaremos más en profundidad las reflexiones que suscita SyRI en relación con el RGPD.

previsibilidad, la normativa SyRI debe cumplir con el principio de interdicción de la arbitrariedad. Para ello, la Corte acude al caso *S. y Marper con Reino Unido*[22] para dejar abierto —sin resolver, más bien— si la interferencia cuenta o no con previsión por ley, puesto que, en realidad, la cuestión de si la norma provee suficientes garantías contra el riesgo de abuso y arbitrariedad está directamente relacionada con la consideración de si la interferencia es necesaria en una sociedad democrática.

De este modo, la Corte procede a entregar dicho juicio de necesidad de la interferencia, partiendo de que la normativa SyRI responde a un interés legítimo del Estado: el de prevenir y combatir el fraude en interés del bienestar económico (párrafo 6.4). A la hora de evaluar si una interferencia es necesaria en una sociedad democrática, el TEDH otorga un margen de apreciación nacional,[23] esto es, los Estados cuentan con cierta discrecionalidad a la hora de establecer restricciones de derechos fundamentales reconocidos por el Convenio en materias en las que no existe un amplio consenso europeo sobre el objeto del caso. La Corte de Distrito de la Haya hace suya la aplicación de este principio a la hora de determinar si la normativa SyRI contraviene el artículo 8.2 del CEDH (párrafo 6.73).

En su argumentación, la Corte cuantifica a cuánto asciende el fraude a la seguridad social y a la asistencia social en los Países Bajos, hasta definir el daño directo e indirecto que causa este fenómeno, y justifica —a partir de la aplicación del margen de apreciación— que el legislador vea una necesidad social imperiosa de adoptar medidas en interés del bienestar económico de los Países Bajos (párrafo 6.76). Dicho de otra manera, la normativa SyRI, por sí, no contraviene según la Corte el artículo 8.2 del CEDH en términos generales: entiende que crear una base jurídica para cooperación en el procesamiento masivo de datos entre distintas autoridades del Estado, bajo los objetivos establecidos en el artículo 64 de la Ley SUWI, responde a un interés legítimo.[24] Este argumento no solo tiene una repercusión directa en el fallo (ya que la Corte entiende que el artículo 64 de la Ley SUWI no contraviene el CEDH), sino

22. Sentencia del caso *S. y Marper con Reino Unido*, Tribunal Europeo de Derechos Humanos, disponible en https://bit.ly/2VWkM7L. En dicha sentencia se valoraba la ley de protección de datos del Reino Unido (1998), por la que se aplica la Directiva 95/45 y las directivas basadas en ella para el uso de la computadora nacional de la Policía en relación con el almacenamiento de huellas dactilares, material celular y perfiles de ADN.

23. El margen de apreciación nacional es una técnica de creación jurisprudencial que ha logrado mantener un punto de equilibrio entre dos necesidades: por un lado, el reconocimiento a nivel europeo de un mínimo común de protección de los derechos reconocidos en el Convenio, desde una interpretación evolutiva del propio tribunal favorecedora en la protección de los derechos y libertades; y, por otro, el mantenimiento de la soberanía nacional de los Estados parte, derivado del carácter subsidiario del propio Convenio (Sánchez-Molina, 2015: 226).

24. Además, consideró que el artículo 64 de la Ley SUWI respeta el principio de limitación de finalidad del RGPD, al entender que dicha norma es también proporcional según el artículo 8.2 del CEDH.

que es una de sus consecuencias más relevantes, como expondremos más adelante.

La Corte de Distrito de La Haya llega aquí al punto crucial de la sentencia, la determinación de si la normativa SyRI es una interferencia necesaria en una sociedad democrática (véanse los párrafos 6.73 y 6.43), no ya desde una consideración genérica, sino desde el juicio de proporcionalidad y subsidiariedad contenido en el artículo 8.2 del CEDH; en definitiva (en los términos que recoge también del caso *S. y Marper con Reino Unido*), si la interferencia logra un equilibrio justo entre los intereses públicos y privados en pugna.

Como habíamos adelantado, la normativa SyRI es analizada a estos efectos bajo los principios generales contenidos en el RGPD de transparencia, limitación de la finalidad y de minimización de datos. La conclusión, también ya adelantada, es que las salvaguardas que contiene la normativa SyRI para proteger el derecho a la privacidad son insuficientes, dado que la normativa no es lo bastante clara y verificable como para concluir que la injerencia que el uso del algoritmo SyRI supone en el derecho al respeto de la vida privada es necesaria, proporcional y conveniente a los fines legítimos a los que sirve la legislación.

Sin duda, la Corte otorga el mayor peso de su argumentación al principio de transparencia. Entiende, en primer lugar, que la normativa no ofrece ninguna clase de información sobre cómo determinados datos o circunstancias pueden derivar en el incremento del riesgo (párrafo 6.87). A su vez, tampoco ofrece información alguna sobre el modelo algorítmico utilizado por la herramienta,[25] con lo cual es imposible comprobar cómo se forma un perfil de riesgo, o cómo resulta el tratamiento de datos de aquellas personas que no derivan en perfiles de riesgo —la Corte entiende que el hecho de que aquellos datos que no derivan en perfiles de riesgo se destruyan antes de cuatro semanas no afecta a la transparencia requerida para su tratamiento (párrafo 6.90)—. El Estado argumentó que el Registro de Notificaciones de Riesgo validaba el modelo algorítmico y verificaba los indicadores de riesgo; sin embargo, la Corte indicó que la normativa no ofrece ningún tipo de información sobre esos procesos de validación y verificación, a los que ni siquiera ha tenido acceso el mismo órgano jurisdiccional en el procedimiento. El Estado (párrafo 6.49) argumentó que el funcionamiento del algoritmo debe ser oscuro, pues de lo contrario no se obtendrían datos masivos sobre el comportamiento de los ciudadanos de la suficiente calidad.[26]

25. Ya hemos señalado que ni siquiera la Corte puede determinar con exactitud en el procedimiento qué clase de tratamiento hace la herramienta SyRI, aunque da por hecho que elabora perfiles de riesgo basados en datos históricos, personales o de otra clase.

26. Resulta llamativo, cuando no sonrojante, que se defienda desde el propio Estado el análisis de *big data* comportamental a través de algoritmos deliberadamente opacos, apostillando, por si no quedase claro, que si los ciudadanos conociesen los criterios y parámetros del algoritmo, podrían acomodar su comportamiento a dichos criterios y parámetros; tanto más si es posible que el algoritmo trabaje con ciertos sesgos de origen o no evite que otros se produzcan.

El relator especial sobre la extrema pobreza y los derechos humanos de Naciones Unidas señaló en un informe aportado al procedimiento[27] que el desarrollo de SyRI tiene un efecto discriminatorio y estigmatizador.[28] La Corte de Distrito de La Haya reconoce que, hasta el momento, SyRI tan solo había sido empleado en barrios que eran considerados «problemáticos» (párrafo 6.92). Por un lado, entiende que esto por sí solo no implica una desproporción en términos del artículo 8.2 del CEDH; por otro lado, la clase de tratamiento utilizada para su desarrollo —esto es, procesamiento de grandes cantidades de datos, lo que incluye datos de especial protección— sí constituye un riesgo de que la utilización de SyRI se base en sesgos con fundamento en el bajo nivel socioeconómico o el origen migrante (párrafo 6.93). La Corte enlazó esta consideración con la falta de transparencia sobre el modelo algorítmico y los indicadores de riesgo, así como la ausencia de salvaguardas para paliar dicha opacidad, concluyendo que dicha interferencia en el derecho al respeto por la vida privada no es proporcional en los términos requeridos por el Convenio (párrafo 6.95).

A continuación, se ponen en consideración los principios de limitación del tratamiento y de minimización de datos, respecto de dos aspectos en particular. Primero, la gran cantidad de datos que resultan elegibles según el artículo 65 de la Ley SUWI y el capítulo 5.a del Decreto SUWI para el desarrollo de SyRI, puesto que la Corte dice que la lista de categorías elegibles es tan exhaustiva,[29] que prácticamente no hay datos personales que no puedan ser objeto de tratamiento por SyRI (párrafo 6.98). En segundo lugar, se refiere a que las propias autoridades participantes llevan a cabo la valoración de qué datos son necesarios para cada proyecto, es decir, la normativa no exige ninguna clase de auditoría por terceros. Aquí, la Corte vincula la opacidad con el modelo algorítmico y los indicadores de riesgo, puesto que son importantes para evaluar si es necesario determinado suministro de datos y en qué medida (párrafo 6.100), y, por lo tanto, también para evaluar el efecto general en la vida privada de esa correlación de diferentes conjuntos (masivos) de datos que tiene lugar en SyRI.[30]

27. Philip Alston, «Brief by the United Nations Special Rapporteur on extreme poverty and human rights as *amicus curiae* before the District Court of the Hague on the case of *NJCM c.s./De Staat der Nederlanden (SyRI)*, case No. C/09/550982/ HA ZA 18/388», 2019, disponible en https://bit.ly/35tyTEJ.

28. Este efecto, debe añadirse, correría el riesgo de quedar cristalizado debido a la autoridad que se confiere a los algoritmos (Beer, 2017: 9).

29. El Decreto SUWI contiene en su artículo 5.a.1 todas las categorías de datos que son elegibles para un proyecto SyRI, entre los que se incluyen, sin ánimo de ser exhaustivos: datos personales (nombre, dirección, lugar de residencia, dirección postal, fecha de nacimiento, género), datos fiscales, datos sobre la vida laboral, datos sobre financiación recibida en la etapa escolar, datos sobre pensiones percibidas, datos sobre deudas con las distintas administraciones, etcétera.

30. El Estado alegaba a su favor la elaboración previa de una evaluación de impacto relativa a la protección de datos (DPIA) y que no era necesario llevar a cabo una evaluación por cada proyecto de SyRI, según el artículo 35.10 del RGPD. Sin embargo, la Corte entiende que dicha evaluación había sido

A partir de este juicio de proporcionalidad, como habíamos adelantado, la Corte de Distrito de La Haya declaró la incompatibilidad del respeto al derecho a la vida privada (artículo 8.2 del CEDH) con el artículo 65 de la Ley SUWI y el capítulo 5.a del Decreto SUWI.

A continuación, señalaremos brevemente algunos de los aspectos que, a nuestro juicio, merecen mayor atención a partir de los argumentos del tribunal en esta sentencia sin precedentes y, creemos, serán de interés para el desarrollo de literatura jurídica. La sentencia que comentamos no puede observarse al margen del contexto en el que nos encontramos inmersos: la llamada Revolución Digital.[31] La Revolución Digital, en tanto que revolución tecnológica, conlleva la irrupción en un lapso breve de un conjunto de tecnologías, productos, industrias y dinámicas nuevas, capaces de sacudir los cimientos de la economía y de impulsar una oleada de desarrollo a largo plazo que, además, es capaz de difundir sus efectos allende las fronteras de las industrias y sectores económicos donde se desarrolló (Pérez, 2004: 32). En el marco general de la Revolución Digital surgen otras no menos importantes que redundan en la idea que acabamos de expresar. Nos referimos al auge del valor económico de los datos (economía de datos),[32] unido al de la importancia y reconocimiento social de los algoritmos, principalmente aquellos que se encargan del procesado de datos. Muestra de ello son los tres documentos que publicó la Comisión Europea el 19 de febrero de 2020.[33]

Las reflexiones con las que cerramos este comentario pretenden ser una invitación al debate sobre un futuro jurídico aún por desarrollar, a partir de aspectos tratados por la sentencia. Algunas de las preguntas que surgen, y que desarrollamos brevemente, son: ¿qué importancia tiene el principio de minimización de datos del artículo 5.c del RGPD en el caso que tratamos?, ¿cómo influye en los ordenamientos jurídicos la actual opacidad de los algoritmos?, ¿corremos el riesgo de aceptar cierto tipo de sesgos por virtud de sugerencias o decisiones basadas en algoritmos? y ¿deben los perfiles personales cumplir con la normativa del RGPD?

---

llevada a cabo antes de la entrada en vigor del RGPD, lo que impediría evaluar si dicho DPIA se ha llevado a cabo según los requerimientos del Reglamento. Además, dada la extensión y gravedad de la interferencia en el derecho a la vida privada que implica cada tratamiento bajo cada proyecto de SyRI, tampoco comparte que no sea necesaria la elaboración de un DPIA por cada proyecto.

31. Para un análisis en detalle de la irrupción y consecuencias de la Revolución Digital en tanto que revolución tecnológica, véase Castillo Parrilla (2018: 23-42).

32. Puede consultarse información actualizada sobre la evolución de la economía y el mercado de datos en The European Data Market Monitoring Tool, disponible en https://bit.ly/3bZA817.

33. Añadimos al libro blanco sobre inteligencia artificial y a la estrategia europea sobre datos la comunicación de la Comisión Europea «Configurar el futuro digital de Europa», Bruselas, 19 de febrero de 2020, COM (2020) 67 final, disponible en https://bit.ly/2L7jaSN.

Consideraciones relativas al RGPD a trabajar por la literatura jurídica a partir del caso SyRI

El caso SyRI debería ser examinado no solo desde la óptica del CEDH, sino también desde la del RGPD.[34] En este sentido, merece la pena apuntar de forma sucinta algunas reflexiones que consideramos pertinentes y que trabajaremos de cara a futuras aportaciones que profundicen en las cuestiones abiertas a partir de este fallo.

En primer lugar, SyRI lleva a cabo una recogida masiva de datos que no cumple con el principio de minimización de datos. El párrafo 4.17 de la sentencia se hace eco de todos los tipos de datos que pueden ser objeto de análisis por el sistema gracias a su normativa y, como la propia sentencia reconoce, la práctica totalidad de la información relativa a una persona queda reflejada en dichas categorías. Esto incumple el principio de minimización de datos del artículo 5.c del RGPD, según el cual el tratamiento de datos personales debe ser adecuado, pertinente y limitado a lo necesario en función de los fines que se persiguen. Dicho principio, de acuerdo con el considerando 39.º del RGPD, también implica que los datos personales «solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios». Es necesario ampliar el análisis sobre la aplicación de este principio jurídico en relación con modelos algorítmicos que, por sí, requieren de grandes cantidades de datos para resultar funcionales.[35]

En segundo lugar, la opacidad de los algoritmos es un riesgo para el ordenamiento jurídico. Como se reconoce en la sentencia (también por parte del Estado), el funcionamiento de SyRI es opaco. La opacidad es un término polisémico, por lo que según parece aquí estamos ante una clase de opacidad deliberada (Burrell, 2016), más que ante un modelo algorítmico no interpretable.[36] El Estado se niega a facilitar esta información alegando que para luchar contra el fraude es fundamental obtener «datos de calidad», entendidos como aquellos que vigilan el comportamiento de los ciudadanos sin que éstos lo sepan o sin que sepan en qué se fijan.[37] En otras palabras, datos

34. Bien es cierto que, como hace la Corte, el contenido del derecho al respeto a la privacidad encuentra también su fundamento en los principios generales contenidos en el RGPD. Sin embargo, lo que planteamos ahora es su examen particular a partir del propio Reglamento como instrumento jurídico autónomo.

35. Por ejemplo, los modelos de aprendizaje profundo o *deep learning* han sido definidos como modelos «hambrientos de datos»: «Ante problemas en los que los datos son limitados, el aprendizaje profundo no es, a menudo, una solución ideal» (Marcus, 2018: 7; la traducción es nuestra).

36. De hecho, el tribunal parece dar a entender que ni siquiera le resulta relevante si estamos ante un modelo de *deep learning* o no, en cuyo caso sí estaríamos ante un modelo algorítmico opaco en el sentido de no interpretable.

37. Como se refleja en el párrafo 6.49, el Estado decide no dar cierta información sobre el funcionamiento de SyRI argumentando que los ciudadanos podrían en tal caso ajustar su comportamiento a los parámetros del algoritmo. Dicho de otro modo, si los ciudadanos conocen los datos en que SyRI se

de espionaje masivo. Estas consideraciones parecen incompatibles con el derecho a la información —ampliamente abordado por la literatura (véase Veale y Edwards, 2018)— contenido en los artículos 13.2 f), 14.2 g) y 15.1 h) del RGPD, que incluye, al menos, el derecho a conocer la elaboración de un perfil y a conocer información significativa sobre la lógica aplicada por el algoritmo, en términos comprensibles conforme al principio de transparencia y suficientemente exhaustiva al mismo tiempo, sin necesidad de incluir información sobre los algoritmos utilizados o la revelación de todo el algoritmo (GT29, 2018: 28). De otro modo, difícilmente puede discutirse la sugerencia (o decisión) tomada por el algoritmo. Cuando los algoritmos se utilizan en el sector público, como es el caso de SyRI, la opacidad resulta aún más incomprensible, dado que actúan funcionalmente como normas (Boix, 2020). Si actúan en la práctica como normas, no se comprende el frontal incumplimiento de un principio tan básico como el de publicidad normativa.

En tercer lugar, si bien el RGPD no trata de manera directa aspectos sobre discriminación, conviene tener presente que la actividad que desarrolla SyRI puede provocar, como señala el relator de Naciones Unidas, situaciones discriminatorias. Sin embargo, el Grupo «Protección de Datos» del artículo 29 sí ha hecho referencia a la importancia de la evaluación de impacto de protección de datos o DPIA (artículo 35 del RGPD) como instrumento a la hora de paliar los efectos discriminatorios.[38] Debe considerarse que en el ámbito de la toma de decisiones automatizada del artículo 22 del RGPD, de forma previa a la implementación de estos algoritmos, es obligatoria la elaboración de una DPIA (Malgieri, 2019: 18). Como hemos analizado, en el presente caso sí se había hecho una evaluación de impacto de la normativa previa a su implementación, si bien la Corte consideraba que esta evaluación había de hacerse en forma obligatoria por cada proyecto SyRI que se desarrollase (párrafo 6.105). A la luz del libro blanco de la Comisión Europea, SyRI podría tratarse de una inteligencia artificial calificada de alto riesgo por el sector al que pertenece (aplicación de sector público) y los potenciales efectos que su utilización conlleva (efectos legales o de similar efecto para los derechos de individuos);[39] conviene abordar si la elaboración de una DPIA constituye un marco regulatorio suficiente para evitar riesgos discriminatorios.

---

fija y ajustan su comportamiento, el conocimiento obtenido de vigilarlos no sería igualmente útil en la medida en que la información obtenida (*raw data*) no sería de la misma calidad.

38. Así se recoge literalmente en las directrices: «Toma de decisiones automatizada con efecto jurídico significativo o similar: tratamiento destinado a tomar decisiones sobre los interesados que produce "efectos jurídicos para las personas físicas" o que les afectan "significativamente de modo similar" [artículo 35, apartado 3, letra a)]. Por ejemplo, el tratamiento puede causar exclusión o discriminación contra las personas. El tratamiento con poco o ningún efecto sobre las personas no coincide con este criterio específico. Las futuras directrices sobre elaboración de perfiles del GT29 contendrán más explicaciones sobre estas nociones» (GT29, 2017: 10).

39. Comisión Europea, «Libro blanco…», p. 17.

Por último, es importante reflexionar sobre la actividad fundamental que desarrolla SyRI en relación con el RGPD: el perfilado personal. ¿Un perfil personal es un dato personal? De la lectura del RGDP no está suficientemente claro que los perfiles personales deban considerarse datos personales, ya que podría considerarse que se trata de meras inferencias cuya exactitud no es segura. Por ello, consideramos relevante en este punto dejar claro que, desde nuestro punto de vista, los perfiles personales sí deben considerarse a todos los efectos como datos personales en el sentido del RGPD.[40] El artículo 4.1 del RGPD define los datos personales como «toda información sobre una persona física identificada o identificable». En ninguna parte establece como requisito que dicha información sea cierta, veraz u obtenida directamente del interesado (cosa distinta es la fiabilidad de la información o la calidad del dato). Por otro lado, el considerando 72.º del RGPD establece que «la elaboración de perfiles está sujeta a las normas del presente Reglamento».

Si se acepta este punto de partida, el examen de una normativa como la de SyRI a la luz del RGPD resulta de sumo interés, pues ello significa que no solo la información en bruto (*raw data*) debe acomodarse (en cuanto a su tratamiento) al RGPD, sino también el conocimiento que de ésta se obtenga, siempre que se trate de «información sobre una persona física identificada o identificable». No solo debería tenerse en cuenta la prohibición de ser objeto de decisiones basadas únicamente en el tratamiento automatizado de datos (artículo 22 del RGPD), sino que el sujeto al que se refiere un perfil personal podría, en tanto que titular de un dato personal, ejercer los derechos de acceso, rectificación, cancelación, oposición y demás recogidos tanto en el RGPD como en las respectivas normas nacionales de desarrollo. Todo esto adquiere una relevancia aún mayor cuando, debido a la crisis mundial que sufrimos como consecuencia del coronavirus, se está empezando a plantear la utilización de modelos matemáticos (algoritmos) para armar inferencias predictivas sobre la probabilidad de contraer el virus o estar infectado.[41] Desde luego, la situación en este último caso es diferente al tratarse de una cuestión de salud pública (artículo 9.2.i del RGPD). No obstante, tememos que pasada la crisis sanitaria el apego de los ciudadanos por su privacidad sea menor aún que el actual.

Conclusiones

Resulta difícil rebatir que la sentencia dictada el 5 de febrero de 2020 por la Corte de Distrito de La Haya sobre el Sistema de Indicación de Riesgos (SyRI) va a ser objeto de una profunda discusión en la doctrina. La pretensión de estas líneas es, por un

40. Esta tesis también la recogen Wachter y Mittelstadt (2019).

41. En esta revista, la utilización de esta clase de modelos algorítmicos en el campo de la medicina fue abordada por Perin (2019).

lado, hacer accesible un análisis a la argumentación jurídica sobre la que se sostiene la incompatibilidad de SyRI con el Convenio Europeo de Derechos Humanos; y, por otro, exponer ciertas consideraciones jurídicas relevantes a efectos del RGPD, ya que esta norma guarda una relación directa con el asunto enjuiciado y sirve de desarrollo del artículo 8 del CEDH en el ámbito de la Unión Europea.

A nuestro juicio, el resultado de la sentencia es positivo y sienta un precedente muy relevante; sin embargo, sus argumentos han de ser objeto de un análisis detallado. No debemos olvidar que la Corte no pone en cuestión el artículo 64 de la Ley SUWI, lo cual implica que está de acuerdo con que —bajo los fines de prevención y combate del fraude social— los poderes públicos compartan datos masivos y sean correlacionados por avanzados modelos algorítmicos, siempre y cuando se haga con las salvaguardas necesarias. Por ende, se comparta o no esta otra consecuencia del fallo, aquellas salvaguardas jurídicas que rodean a la implementación de algoritmos como SyRI merecen toda nuestra atención.

Reconocimientos

El texto ha sido elaborado gracias a la financiación del Departamento de Educación del Gobierno vasco para apoyar las actividades de Grupos de Investigación del Sistema Universitario Vasco (IT 1066-16), y se ha desarrollado en el marco del proyecto europeo de investigación «Participatory approaches to a new ethical and legal framework for ICT (PANELFIT)» (EC Grant Agreement 788039).

El autor José Antonio Castillo Parrilla, incorporado recientemente a la cátedra de Derecho y Genoma Humano (Contrato para la especialización de personal investigador doctor en la UPV/EHU-2019), desea agradecer a la cátedra y todo su equipo la cálida acogida, de la que este trabajo (en equipo) es el primero de ojalá muchos.

Referencias

Beer, David (2017). «The social power of algorithms». *Information Communication and Society,* 20 (1): 1-13. DOI: 10.1080/1369118X.2016.1216147.

Boix, Andrés (2020). «Los algoritmos son reglamentos: La necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones». *Revista de Derecho Público: Teoría y Método,* 1: 223-270. DOI: 10.37417/RPD/vol_1_2020_33.

Burrell, Jenna (2016). «How the machine "thinks": Understanding opacity in machine learning algorithms». *Big Data & Society,* 3 (1): 1-12. DOI: 10.1177/2053951715622512.

Castillo Parrilla, José Antonio (2018). *Bienes digitales: Una necesidad europea.* Madrid: Dykinson.

Contreras Vásquez, Pablo y Pablo Trigo Kramcsák (2019). «Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile». *Revista Chilena de Derecho y Tecnología,* 8 (1): 69-106. DOI: 10.5354/0719-2584.2019.52915.

De Miguel Beriain, Íñigo (2018). «Does the use of risk assessments in sentences respect the right to due process? A critical analysis of the *Wisconsin v. Loomis* Ruling». *Law, Probability and Risk,* 17 (1): 45-53. DOI: 10.1093/lpr/mgy001.

Dressel, Julia y Hany Farid (2018). «The accuracy, fairness, and limits of predicting recidivism». *Science Advances,* 4 (1). DOI: 10.1126/sciadv.aao5580.

EPRS, Servicio de Estudios del Parlamento Europeo (2018). *El derecho al respeto de la vida privada: Los retos digitales, una perspectiva de derecho comparado.* Disponible en https://bit.ly/2WqgSTK.

GT29, Grupo de Trabajo del Artículo 29 (2017). «Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679». Disponible en https://bit.ly/2WsdTui.

—. (2018). «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 a efectos del Reglamento (UE) 2016/679». Disponible en https://bit.ly/31Fz79C.

Kirkpatrick, Keith (2017). «It's not the algorithm, it's the data». *Communications of the ACM,* 60 (2): 21-23. DOI: 10.1145/3022181.

Lin, Zhiyuan, Jongbin Jung, Sharad Goel y Jennifer Skeem (2020). «The limits of human predictions of recidivism». *Science Advances,* 6 (7): eaaz0652. DOI: 10.1126/sciadv.aaz0652.

Malgieri, Gianclaudio (2019). «Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations». *Computer Law & Security Review,* 35 (5). DOI: 10.1016/j.clsr.2019.05.002.

Marcus, Gary (2018). «Deep learning: A critical appraisal». *ArXiv*. Disponible en https://arxiv.org/abs/1801.00631.

Miró Llinares, Fernando (2018). «Inteligencia artificial y justicia: Más allá de los resultados lesivos causados por robots». *Revista de Derecho Penal y Criminología,* 20: 87-130. DOI: 10.5944/rdpc.20.2018.26446.

Murillo de la Cueva, Pablo Lucas (2009). «La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad». En Pablo Lucas Murillo de la Cueva y José Luis Piñar Mañas, *El derecho a la autodeterminación informativa*. Madrid: Fundación Coloquio Jurídico Europeo.

Pérez, Carlota (2004). *Revoluciones tecnológicas y capital financiero: La dinámica de las grandes burbujas financieras y las épocas de bonanza*. Madrid: Siglo XXI.

Perin, Andrea (2019). «Estandarización y automatización en medicina: El deber de cuidado del profesional entre la legítima confianza y la debida prudencia». *Revista Chilena de Derecho y Tecnología,* 8 (1): 3-28. DOI: 10.5354/0719-2584.2019.52560.

Romeo Casabona, Carlos María (2018). «Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad». *Revista Penal,* 42: 165-179.

Sánchez-Molina, Pablo (2015). «Margen de apreciación nacional (en los sistemas de protección internacional de los derechos humanos)». *Eunomía: Revista en Cultura de la Legalidad,* 9: 224-231.

van Brakel, Rosamunde y Paul de Hert (2011). «Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies». *Journal of Police Studies,* 20: 163-192.

van Dalen, Steven, Alexander Gilder, Eric Hooydonk y Mark Ponsen (2016). «System risk indication: An assessment of the Dutch anti-fraud system in the context of data protection and profiling». Universidad de Utrech. Disponible en https://bit.ly/2L7Irw9.

Veale, Michael y Lilian Edwards (2018). «Clarity, surprises, and further questions in the article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling». *Computer Law & Security Review,* 34 (2): 398-404. DOI: 10.1016/j.clsr.2017.12.002.

Viollier, Pablo (2017). «El estado de la protección de datos personales en Chile». Derechos Digitales América Latina. Disponible en https://bit.ly/2APoeqk.

Wachter, Sandra y Brent Mittelstadt (2019). «A right to reasonable inferences: Rethinking Data Protection Law in the age of big data and AI». *Columbia Business Law Review,* 2019 (2): 1-130. Disponible en https://bit.ly/2z5at8J.

Sobre los autores

Guillermo Lazcoz Moratinos es licenciado en Derecho por la Universidad del País Vasco (UPV/EHU), España. Investigador FPU del Ministerio de Educación y Formación Profesional (Gobierno de España) en el GI Cátedra de Derecho y Genoma Humano, Universidad del País Vasco. Su correo electrónico es gullermo.lazcoz@ehu.eus. http://orcid.org/0000-0001-6567-045X.

José Antonio Castillo Parrilla es doctor europeo en Derecho Digital por la Universidad de Bolonia y doctor en Derecho Civil por la Universidad de Granada. Investigador posdoctoral en el GI Cátedra de Derecho y Genoma Humano, Universidad del País Vasco (UPV/EHU), España. Su correo electrónico es joseantonio.castillo@ehu.eus. http://orcid.org/0000-0002-8527-999X.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).