VIGURI CORDERO, Jorge Agustín, *Seguridad y Protección de Datos en el Sistema Europeo Común de Asilo*, Tirant lo Blanch, Valencia, 2021, 447 pp., ISBN 978-84-1378-17-09.

http://dx.doi.org/10.18543/ed-69(2)-2021pp353-365

Que cada persona está continuamente vigilada, perfilada y catalogada por el Estado (tanto en su sentido clásico como moderno) es una premisa que dejó hace muchos años de pertenecer únicamente a la ciencia ficción y ha pasado a ser una realidad insoslayable de nuestro tiempo, aunque evidentemente se ha visto acentuada en los últimos años. En efecto, vivimos en una era en la que existen no sólo los clásicos Estado-Nación, sino también los Estados digitales; de ahí denominaciones como *Facebook Nation*: si bien sus fronteras son difícilmente delimitables, con sus casi mil setecientos millones, hace de esta 'nación', el pueblo más grande del mundo y, si bien no tiene plena soberanía, tiene su propio sistema financiero, moneda, sistemas de resolución de conflictos, lo que queda plasmado en su 'constitución' auto-otorgada, a través de sus términos legales (*Términos y Condiciones de uso*), y como una suerte de primera potencia mundial, ha influido considerablemente en las percepciones, y en las decisiones personales, sociales, económicas y políticas a escala planetaria (Newton 2014).

En una época en la que la verdad es todo (y casi única y exclusivamente) aquello que existe en el mundo virtual (en la Red o en las bases de datos de las que muchas veces se nutre), somos testigos de las nuevas reglas del juego por las cuales estamos sentenciados (si queremos participar en la vida social, económica, política y cultural); es decir, a quedar invadidos, sometidos y manipulados, en función de los datos que recogen y exponen sobre nosotros, incluso «de manera invisible», por «mecanismos ingeniosos y máquinas pensantes» (Rodotà 2014, 289) construidas y operadas bajo premisas legítimas pero con sesgos sistémicos, intenciones encubiertas y riesgos impredecibles. Resulta especialmente preocupante el uso de la Inteligencia Artificial aplicada a la investigación policial y judicial o al funcionamiento diario de las administraciones públicas (por sus potencialmente perjudiciales consecuencias jurídico-sociales). Como constitucionalista me surgen numerosos interrogantes ¿Cómo aseguramos que no se producirán actuaciones discriminatorias? ¿Bajo qué condiciones entendemos legítimo el uso de estas herramientas digitales? ¿Cuáles son las condiciones de garantía

para los derechos fundamentales en jaque?

De una parte, la información (sobre todo la información de carácter personal) se ha convertido en poder; así, los sistemas basados en los datos han devenido en herramienta clave para sistemas opresivos de los que ya nos advirtieron, entre otros, Orwell, Zamyatin y Huxley y que, de alguna manera u otra, también se han visto reflejados en momentos de nuestra historia contemporánea, con cada nueva etapa de revolución tecnodigital. Sin entrar en cuestiones sobre las nuevas facetas de la vigilancia electrónica, tanto pública como privada, sí que cabe, al menos, citar al nuevo fenómeno de la *dataveillence* en la era post-Snowden. Con dataveillence me refiero a una suerte de recogida y agregación panóptica en la que los datos reunidos a través de las prácticas de vigilancia del ciudadano ordinario da paso a mecanismos de vigilancia del Estado, a través de las corporaciones que poseen esos datos (Bakir 2015, 12-25; y, Sancho López 2018, 39-47). Precisamente la creciente preocupación por la privacidad (y los demás derechos y libertades individuales) ha venido de la mano de las revelaciones vinculadas a los sistemas de vigilancia y tratamientos masivos de información que concierne a las personas, creados y utilizados bajo la justificación de proteger la seguridad nacional.

De otra parte, la visión y premisas que fundamentan el llamado Espacio de Libertad, Seguridad y Justicia (ELSJ) han estado presentes en el ordenamiento jurídico europeo desde antes del cambio de siglo (inicialmente con el Tratado de Maastricht, pero, sobre todo, con las modificaciones del Tratado de Ámsterdam). El ELSJ es, a fin de cuentas, una nomenclatura simplificada del conjunto de políticas y actuaciones de la UE, a fin de crear y garantizar un área de cooperación y coordinación a nivel comunitario que facilite la seguridad interior, que asegure una justicia eficaz y que garantice una protección efectiva de los derechos y libertades en el conjunto del territorio europeo. Es más, con la reforma del Tratado de Lisboa, que reconfiguró a la UE y modificó los tratados constitutivos[1], dejó de ser una visión político-jurídico y se incorporó

[1] Por lo que nos interesa para esta recensión, el Tratado de Lisboa también trajo otros dos cambios significativos. Por un lado, incorporó el art. 16 Tratado de la Funcionamiento de la UE mediante el cual se le reconoce a la UE una nueva competencia para legislar en materia de protección de datos. Este precepto establece el derecho a que los datos personales se protejan y concreta que la UE tiene competencias legislativas específicas sobre la protección de las personas respecto al tratamiento de sus datos personales. Por otro lado, incorporó la Carta de Derechos Fundamentales de la UE (CDFUE), reconociéndole fuerza jurídica y elevándola como parte del derecho originario (otorgándole el mismo valor que los demás tratados constitutivos). Esta, a su vez, consagra de manera explícita un derecho fundamental y autónomo a la protección de datos de carácter personal (art. 8 CDFUE) y un derecho de asilo (art. 18 CDFUE) y protección en caso de devolución o expulsión (art. 19 CDFUE). Esta incorporación se ha considerado un hito, no sólo por crear una «Declaración de Derechos Europea», con el reforzamiento de los derechos clásicos y la consagración de muchos nuevos no expresamente reconocidos en el Convenio Europeo de Derechos Humanos (como podría argumentarse es el caso de estos tres derechos), sino también por insertarla en su estructura dogmática

expresamente, como uno de los principales objetivos 'constitucionales', el ofrecer a los ciudadanos europeos un espacio de libertad, seguridad y justicia sin fronteras interiores (art. 3.2 Tratado de la UE).

Sin lugar a dudas, el ELSJ se ha convertido en uno de los ámbitos más relevantes y polémicos de la UE, sobre todo debido a los desafíos de los últimos tiempos relacionados con el terrorismo, la delincuencia transnacional, la crisis migratoria y de refugiados, así como el papel de los avances tecnológicos y su potencial amenaza para la protección efectiva de los derechos y libertades fundamentales en estos ámbitos. Concretamente, las implicaciones de las Nuevas Tecnologías de la Información y la Comunicación (NTIC) en el ámbito del ELSJ han sido (y seguirán siendo) diversas y trascendentales; entre ellas, son especialmente preocupantes las amenazas a la privacidad y a la protección de datos en una era que destaca ya no sólo por la libre y globalizada circulación de capitales, de personas (incluidos colectivos vulnerables y delincuentes), de bienes y de servicios, sino también (y cada vez más) por la libre circulación e intercambio de información y de datos de carácter personal.

Es más, esta época también se caracteriza por la cooptación del sector privado en la lucha contra el crimen y en la salvaguarda de la seguridad y orden público (sirva el ejemplo de la censura de contenidos considerados nocivos en redes sociales y plataformas virtuales como muestra de ello). En el caso concreto del ELSJ, la recopilación y análisis de la información se crea y se pone a disposición por empresas que gestionan actividades ordinarias de la vida diaria (desde transacciones financieras y desplazamientos aéreos, hasta el uso de la telefonía móvil y un largo etcétera) lo que demuestra que nos movemos en asociaciones multinivel, con múltiples actores que abarcan tanto el sector público como el privado. La limitación de determinados derechos y libertades bajo la justificación del paraguas de la seguridad u orden público es un tema recurrente. Esto se ve reflejado en actuaciones y políticas diversas dentro del ELSJ, entre ellas, las bases de datos paneuropeas en asuntos de interior (principalmente en *border management* y *law enforcement*): el registro de nombres de los pasajeros (PNR, por sus siglas en inglés), el Sistema de Información de Visados (VIS, por sus siglas en inglés), la base de datos europea de huellas dactilares (EURODAC, por su acrónimo inglés), el Sistema de Información de Schengen (SIS II, por sus siglas en inglés), a los que hay que sumarle los novedosos sistemas de entrada/salida (EES, por sus siglas en inglés), el sistema europeo de información y autorización de viajes (ETIAS, por sus siglas en inglés) entre otros. Gracias a la evolución tecnológica, impulsada por consideraciones de seguridad en el mundo posterior al 11-S (lamentablemente continuado por el 11-M, 13-N, 22-M, 14-J y el 17-A, entre otros numerónimos) el legislador de la UE ha creado milhojas de sistemas de tratamiento de información relativa a personas identificadas o identificables.

fundacional, haciendo la naturaleza de la Unión Europea mucho más constitucional.

* * *

La 'frontera entre la privacidad y la seguridad nacional es difusa y de ella nace una búsqueda compleja por encontrar el mejor encaje entre bienes jurídicamente protegidos aparentemente contrapuestos. No obstante, hay una falsa percepción de que sólo se puede proteger un bien/valor jurídico en el marco del ELSJ a expensas del otro. Si bien hay un delicado equilibrio entre la privacidad y la seguridad, se trata sin duda de un equilibrio posible y necesario. Como afirma Rodotà, se ha allanado un camino para *«aprovechar las oportunidades ofrecidas por este nuevo mundo, sin tener que sufrir las tiranías y los riesgos, tratando de dejar bajo el control del derecho y de los ciudadanos unos procesos que de otra manera podrían arrastrar, de una sola tacada, a las personas y a la democracia»* (Rodotà 2014, 289).

Pues bien, en este contexto, tiene pleno sentido (y resulta particularmente valioso) el trabajo del Prof. Dr. Jorge Viguri Cordero titulado *Seguridad y Protección de Datos en el Sistema Europeo Común de Asilo*, publicado en la editorial de excelencia Tirant lo Blanch a principios de este año. Se habla mucho, en la dicotomía Derecho-Tecnología, de una temática que ya es clásica: los mandatos del tráfico económico para favorecer las clásicas libertades económicas, como límite a derechos fundamentales. En otras palabras, el permanente conflicto (y la difícil conciliación) entre las libertades económicas y la protección de datos personales, como se ha analizado en otras ocasiones (Martínez López-Sáez 2017, 139-176). En esta ocasión, el autor se adentra en otra temática y conflicto jurídico igualmente clásico pero indudablemente más complejo, y por ello doblemente encomiable: el permanente conflicto (y la difícil conciliación) entre la seguridad y la protección de datos. A la *tensión dialéctica* entre libertad y seguridad, se le suma el dilema permanente entre la privacidad y la seguridad (pág. 392). Seguramente no en vano el autor haya elegido emparejar estas palabras clave en el título de su trabajo.

Nos encontramos ante un trabajo de gran extensión (que supera las cuatrocientas páginas) y, pese a todo, se presenta con un formato agradable de leer y con una redacción muy cuidada. El trabajo está bien estructurado, con una introducción a modo de contextualización, con tres partes centrales que se completan conforme se va avanzando en la lectura: primero cuestiones jurídicas relativas al asilo y a la protección internacional, incluyendo unas consideraciones preliminares sobre la inminente aprobación del paquete de reformas (Capítulo I) para luego incidir en la creación y desarrollo del Sistema Europeo Común de Asilo (Capítulos II y III), especialmente en lo que concierne la excepción justificada por excelencia, a saber, el mantenimiento del orden público y la protección de la seguridad nacional (sirviéndose de la jurisprudencia del TJUE y, en clave de complementariedad y sinergia, del TEDH) para finalmente examinar el régimen de la protección de datos, en general, y en relación con los sistemas informáticos previamente analizados (Capítulos IV y V). Como colofón a

su estudio añade un apartado de conclusiones finales sobre los retos más destacados a los que se enfrenta el SECA, las propuestas de reforma y las contrapropuestas regulatorias que él mismo presenta para paliar las graves injerencias en el derecho de asilo y el derecho a la protección de datos de los solicitantes de protección internacional. Por último, los anexos referentes a las fuentes utilizadas (doctrinales, normativas, jurisprudenciales y documentales) se formulan también de manera cuidadosa y denotan la excelencia investigadora del autor.

Viguri Cordero nos ofrece un inestimable trabajo monográfico. En palabras de su directora de tesis doctoral y prologuista, nos hallamos ante un estudio que «se aborda de forma absolutamente novedosa» y que resulta ser «pionero» en nuestro ordenamiento (págs. 19-20). En efecto, la sistematización simultánea del régimen jurídico de la protección de los datos de carácter personal y del Sistema Europeo Común de Asilo, así como el análisis de sus fortalezas y propuestas regulatorias para paliar sus deficiencias, en el ordenamiento jurídico comunitario (y, a la luz de la globalización, del constitucionalismo europeo y del sistema multinivel de derechos, también en el ordenamiento español) ofrecen al lector un punto de partida considerablemente valioso para el perfeccionamiento de ambos regímenes normativos, y, en última instancia, para garantizar la efectividad de los derechos fundamentales en juego, sobre todo para aquellas personas tan desamparadas que necesitan seguridad jurídica y protección. El autor, a lo largo del trabajo, aprecia ese dilema permanente entre la seguridad y la privacidad pues reconoce la necesidad de la justicia preventiva y la salvaguarda de la seguridad pública, a la vez que cuestiona que, so pretexto de la seguridad, se hayan extendido los canales de monitoreo de la movilidad de las personas, produciendo situaciones de vigilancia preventiva. Aquí destacamos la doble faceta del autor en tanto que constitucionalista español, especializado en el derecho a la protección de datos y en el derecho de asilo, pero con perspectiva europea, en su sentido más amplio. En efecto, analiza lo que él llama *«el conflicto de derechos fundamentales de primer orden entre el derecho a la protección internacional y el derecho a la protección de los datos personales»* (pág. 31) a la vez que examina su difícil conciliación con la salvaguarda de la seguridad nacional y de los objetivos y políticas en el marco de una competencia compartida y especialmente delicada y compleja[2] entre la UE y los EEMM.

* * *

Ya que es Viguri Cordero el verdadero experto en el derecho de asilo y el SECA, y en tanto en cuanto compartimos intereses de investigación más bien en lo que al régimen paneuropeo de protección de datos y a la protección de personas en situación de

[2] Pues, en realidad, la todavía embrionaria «Unión de Seguridad» a la luz de la *Estrategia Global para la Política Exterior y de Seguridad de la UE (2020-2025)*, es un esfuerzo polivalente e intersectorial en el que es sumamente difícil difuminar las fronteras entre migración, seguridad, delincuencia y política exterior.

vulnerabilidad se refiere, me centraré en los aspectos más destacables, a mi juicio, de su monografía, es decir, la tercera parte (Capítulos IV y V). Pese a ello, esto no es óbice para que aluda a las advertencias del autor en cuanto a los derechos vinculados al SECA en sentido más amplio: Primeramente, en lo que se refiere a las causas y consecuencias de la llamada *lotería del asilo*, el autor insiste que debido a la generalización y flexibilización de las causas de exclusión y a la *inoperatividad práctica* de las distinciones en la clasificación de los dos estatutos de protección internacional (pág. 157); y, seguidamente, en lo que se refiere a las revisiones del sistema que podrían propiciar una peligrosa *noción de temporalidad* del derecho a la protección internacional como consecuencia de un constante flujo de intercambio de información, lo que iría en detrimento de dicho derecho (págs. 157 y 390). Con respecto a la faceta *iusdigital*, el autor examina *la incidencia del procesamiento y gestión de la información de los solicitantes de protección internacional en el Sistema de Dublín, como en sus propuestas de reforma con objeto de concretar y actualizar el difuso régimen jurídico de protección de datos e información personal, esencialmente, a la luz del Reglamento General de Protección de Datos (2016/679), de la Directiva de protección de datos en el ámbito penal (2016/680)* [lo que yo llamaré Directiva Policial]*, así como del novedoso Reglamento relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración (818/2019)* [lo que yo llamaré Reglamento Institucional de Protección de Datos o RIPD]. Adelanto que coincido plenamente con la práctica totalidad de las observaciones jurídicas que hace Viguri Cordero, aunque también expondré algunas reflexiones complementarias a su análisis.

En primer lugar, la temática deviene relevante en tanto en cuanto estamos hablando no sólo de datos personales (datos que identifican o hacen identificable a una persona) sino de datos especialmente sensibles como los datos biométricos, incorporación novedosa del marco paneuropeo de protección de datos[3], en tanto que *«datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que* ***permitan o confirmen la identificación única*** *de dicha persona, como imágenes faciales o datos dactiloscópicos»* (énfasis mío) (art. 4(14) RGPD). Es decir, que hablamos de datos que identifican de manera inequívoca y absoluta a una persona, los cuales, por ello mismo, requieren de especial protección debido a que su tratamiento afecta más intensamente a los derechos y libertades por sus potenciales usos con fines o consecuencias discriminatorias.

En segundo lugar, los supracitados sistemas indudablemente aseguran una

[3] También se ha incluido en la modernización del Convenio 108 del Consejo de Europa, el conocido como Convenio 108+: se ha ampliado la definición de dato personal, incorporando los datos genéticos, biométricos y aquellos relacionados con la afiliación sindical y el origen étnico. *Vid*. art. 6 del Convenio 108+.

mejor protección de las fronteras, una mejor gestión de los flujos migratorios y contribuyen a reforzar la seguridad interior de los EEMM, y, en consecuencia, de la Unión. No se discute que la UE necesita un ecosistema de seguridad (basado en los datos) robusto ante las nuevas amenazas (transfronterizas y transversales) para la seguridad de los Estados y de sus ciudadanos, lo que inevitablemente implica un mayor intercambio de información e interoperabilidad de los sistemas y una cooperación más estrecha de todos los actores implicados. Sin embargo, en tanto en cuanto los datos de carácter personal (entendidos como cualquier información que identifica o hace identificable a una persona física), muchos de ellos especialmente sensibles al ser datos biométricos o reveladores del origen racial/étnico (las llamadas categorías especiales de datos)[4], son el elemento básico y eje central de estos sistemas, las implicaciones en materia de privacidad y protección de datos son incuestionables y serias: por ejemplo, decisiones individuales automatizadas, basadas en sistemas de inteligencia artificial alimentada por el tratamiento (sesgado) de determinados datos personales u otros efectos nocivos de la llamada «dictadura del algoritmo» (Rodotà 2014, 361). Y por todo ello, ante las amenazas que se ciernen sobre la privacidad y la dignidad, debemos avanzar con suma precaución. En palabras de Viguri Cordero, si bien la operatividad funcional podrá solventar o reducir diferentes lagunas jurídicas, también podrían generar situaciones sumamente desventajosas como la aplicación indiscriminada y generalizada de las cláusulas de exclusión (pág. 160), y, por ende, producir situaciones susceptibles de menoscabar el ejercicio de uno o varios derechos como consecuencia de esa aplicación, lo que, a su vez, *limita o veda el acceso efectivo al procedimiento de protección internacional* (pág. 389). La ONG *Privacy International* ha resumido muy bien los graves riesgos que tiene la *data-driven approach* de estos sistemas informáticos y políticas de inmigración[5]. En análoga línea se pronuncia el autor de esta obra: *«su funcionamiento prioriza las dimensiones de seguridad, eficiencia y eficacia, y, lejos*

[4] Art. 9 RGPD, arts. 10 tanto de la Directiva 2016/680/UE (Directiva policial) como del Reglamento 2018/1725 (RIPD): *«datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física».*

[5] *«pretende utilizar datos digitales invasivos y potencialmente defectuosos sobre las personas para tomar decisiones que cambien su vida, al tiempo que amplía los controles de estado a las interacciones cotidianas en la sociedad […] Estas políticas de inmigración basadas en datos no sólo conducen a un trato discriminatorio de las personas y socavan la dignidad de las mismas, sino que los fallos tecnológicos dan lugar a una toma de decisiones injusta, especialmente cuando se automatizan [esos procesos bajo el prisma de la interoperabilidad]»* (traducción propia). «Protecting migrants at borders and beyond», Privacy International. Acceso el 28 de agosto de 2020, https://privacyinternational.org/protecting-migrants-borders-and-beyond

de complementar la protección de los derechos de los refugiados, interfiere negativamente en el derecho a la protección de sus datos personales» (pág. 34), en tanto que la información solicitada y procesada «resulta frecuentemente sensible» y está al alcance de una amalgama muy diversa y amplia de organismos internacionales, europeos y nacionales que intervienen, de alguna manera u otra, sin formación adecuada (el autor ha insistido bastante en la escasa formación de las autoridades competentes sobre la legislación general y sectorial de protección de datos) y sin pautas uniformes sobre el tratamiento de información de carácter personal.

En esta línea, y en tercer lugar, el autor insiste en que parte del problema (al menos en cuanto a la falta de uniformidad y la inseguridad jurídica de la que adolece el régimen examinado) deriva del amplio margen de apreciación que la normativa europea permite a los EEMM en este ámbito competencial en el que hay culturas y ordenamientos jurídicos y posturas políticas tan dispares en lo que concierne al ámbito de los asuntos de interior (págs. 28 y 139). Igual sucede en materia de protección de datos; lo que se ha venido llamando las «clausulas abiertas», permitiendo a los EEMM, entre otras cosas, limitar las protecciones vertidas sobre el derecho a la protección de datos (bien a través de restricciones o bien a través de la especificación de excepciones) para garantizar objetivos o bienes de interés público, entre los que, indudablemente se encuentra salvaguardar la seguridad nacional o el orden público (Considerando 73 y el art. 23 RGPD). De hecho, EDRI, la mayor red europea de defensa de los derechos y las libertades en línea, publicó un informe interesante sobre los abusos y la manera en la que algunas autoridades públicas y organismos competentes a nivel nacional esquivan tener que aplicar estándares más elevados en materia de protección de datos, bajo justificaciones de seguridad, comportamientos sospechosos y situaciones de urgencia, que, como sabemos, son justificaciones genéricas que conducen a terrenos jurídicamente escudados pero hartamente resbaladizos desde el punto de vista de los derechos humanos[6]. Así, el concepto impreciso e indeterminado de 'seguridad', priorizado constantemente (págs. 33, 76 y 152) a expensas de otros derechos y valores, puede servir para socavar las distinciones clave y los límites del alcance del Estado en la vida de las personas.

En cuarto lugar, el autor hace alusión a las exclusiones previstas en el RGPD en materia de persecución de los delitos entre otras materias, que, no obstante, se regulan por otras normas de la UE, como la Directiva Policial o en el caso del correcto funcionamiento de las instituciones o agencias europeas, el RIPD. Además, recuerda que se extendió la protección de los datos a todo interesado en el tratamiento (persona física) que se encuentre en la UE, debiendo, a su juicio, quedar amparados también los solicitantes de protección internacional (pág. 284 y ss.). Es verdad que la Directiva Policial tiene una protección

[6] Acceso el 28 de agosto de 2020, https://edri.org/wp-content/uploads/2021/07/EDRI_RISE_REPORT.pdf

más reducida en comparación con el RGPD o el RIPD en cuanto a los principios de tratamiento de datos y los derechos de los interesados. Por ejemplo, se limita el principio de transparencia (dadas las cuestiones de prevención de las fuerzas de seguridad y las prácticas de vigilancia encubierta), se reducen los principios de limitación de la finalidad y minimización de los datos (la ley no pide que el tratamiento sea adecuado, pertinente o limitado, solo exige que no sea excesivo, dando más margen de apreciación a las autoridades competentes en detrimento de los derechos de los interesados), se establecen términos diferentes para los períodos de conservación/retención y despersonalización de los datos personales recogidos, se restringen al mínimo los derechos de información y acceso y ha dado pie a instrumentos de especialidad para cada actor implicado (como es el caso del reglamento de protección de datos de las instituciones europeas o el todavía más específico de la agencia EUROPOL). Con respecto a estas dos últimas cuestiones Viguri Cordero ha sido especialmente crítico en supuestos en los que se tratan datos personales de solicitantes de asilo.

Coincido plenamente en que existe un claro menoscabo de los derechos del interesado (especialmente el derecho de acceso/información, de supresión y de limitación) en el ámbito policial y penal: lo que él llama *un considerable retroceso en la protección efectiva del intercambio de información*. Ello, claramente, se ve justificado bajo la premisa de flexibilizar hasta el máximo exponente las funciones de cooperación e intercambio de información (y las obligaciones) de las distintas autoridades administrativas y policiales en sede nacional, pero, como bien apunta el autor, emplazando el derecho a la protección de datos del interesado del tratamiento a un plano subsidiario y agravando así, la desconfianza de los solicitantes en los procedimientos de protección internacional. Termina abogando no solo por dotar de la suficiente transparencia a estos procedimientos, sino por incrementar sustancialmente las deficitarias condiciones de acogida que han dispuesto, con carácter general, los EEMM situados en primera línea (España, Italia o Grecia, entre otros), especialmente, en los *hotspots* (págs. 255 y 287). Paralelamente, aunque coincido en que, en ocasiones, la multiplicidad de normas y el excesivo uso de la remisión normativa generan confusión y mayor inseguridad jurídica (pág. 381), sí que considero interesante, y quizás positivo para los afectados, que exista una *lex specialis* para cada tipo de organismo responsable del tratamiento, pues el tipo de tratamiento y la injerencia a los derechos en juego dependerá mucho de la finalidad del tratamiento (y esta, a su vez, dependerá de los objetivos que persigue o para los que se ha creado el responsable del tratamiento); lo anterior lo afirmo, eso sí, siempre y cuando los principios de limitación de la finalidad, minimización y exactitud queden respetados, en la medida que se efectúe un examen de proporcionalidad más estricto[7] en el análisis de las

[7] En línea con los parámetros que siguió el TJUE en los Asuntos acumulados C-293/12 y

medidas tomadas, y siempre que se disponga de un umbral/estándar mínimo de protección alto (o, al menos, adecuado al supuesto de hecho). Todo ello es aún más necesario en tanto en cuanto frecuentemente el tratamiento de los datos de carácter personal no se limita sólo a su procesamiento o almacenamiento, sino que exige, dados los elementos transfronterizos característicos del ELSJ, un intercambio y trasferencia transnacional de los mismos.

En este sentido, Viguri Cordero, además, insiste en que la propuesta de reforma del SECA adolece de una perspectiva basada en la protección de los datos. Según él, el sistema, y sus propuestas de reforma, reflejan una tendencia hacia una mayor recopilación de datos (sobre todo categorías especiales de datos). A su juicio, además, el sistema sufre de varios déficits: (1) la amplia flexibilidad en la toma de decisiones a la hora de intercambiar información (con criterios ambiguos de suficiencia, pertinencia y necesidad) y su supeditación a formalidades imperativas vinculadas al principio de confidencialidad y otros deberes relativos a la designación de puntos de contacto y canales de comunicación entre distintos organismos; (2) las excepciones por razones de seguridad nacional y orden público en lo que se refiere a las limitaciones vinculadas a la transferencia de datos a terceros países a efectos de retorno.

Concretamente, para el caso del sistema de información Eurodac, se muestra crítico respecto a la falta de consenso en la aprobación de su reglamento de reforma, que lleva más de cuatro años en el limbo legislativo europeo. Así, explica las novedades *de hondo calado* que, a su vez, también presentan dudas jurídicas en cuanto a su coherencia y adecuación con el régimen europeo de protección de datos aplicable, como es el caso de la ampliación del objeto y finalidad de ese sistema de información, la propia transferencia de información personal a terceros países (cuando son los de retorno), o, las que más me preocupan desde la perspectiva del riesgo y de la vulnerabilidad, la incorporación de las imágenes fáciles como nueva categoría de datos biométricos, la reducción de la edad para la recopilación de este tipo de dato especialmente sensible a los seis años y el acceso cuasi automático (bajo el amparo de una necesidad imperiosa de seguridad o por razones importantes de interés público) de las autoridades policiales y la Europol a los datos recabados, por citar algunos de los ejemplos más paradigmáticos (págs. 383 y ss.).

Concretamente, para el caso de la AAUE y la GEFC, también se muestra crítico en cuanto a su excesiva indeterminación y generalización en las amplias categorías de sujetos y finalidades (desde cuestiones relativas a la gestión de los flujos migratorios, las fronteras y la protección internacional, hasta cuestiones vinculadas a la delincuencia transfronteriza y el terrorismo), lo que, según él, *incidirá negativamente en las garantías de la protección de datos* (págs. 391-394).

* * *

En otro orden de cosas, también resulta especialmente interesante el

C-594/12, *Digital Rights Ireland Ltd v. Seitlinger y otros,* STJUE de 8 de abril de 2014

enfoque «pro personae» que adopta el autor para determinadas situaciones de vulnerabilidad. En lo que concierne específicamente a la protección de datos de los colectivos vulnerables, destacamos dos de las publicaciones de la Agencia de Derechos Fundamentales de la Unión Europea (FRA, por sus siglas en inglés) que versan sobre la protección de datos en el marco del ELSJ. Por un lado, el Informe relativo a la protección de datos especialmente sensibles, titulado *Under watchful eyes: biometrics, EU IT systems and fundamental rights*[8]; en el que se examina y se recomiendan medidas protectoras de protección de datos para personas en situación de especial vulnerabilidad, como son los refugiados e inmigrantes. Por otro lado, el Informe relativo a la interoperabilidad de los sistemas en la UE titulado *Fundamental rights and the interoperability of EU information systems: borders and security*[9] en el que, entre otras cosas, incide en la especial vulnerabilidad de (y concreciones técnicas de interoperabilidad para) los migrantes menores de edad, dada su situación de particular vulnerabilidad (doble o incluso múltiple). Además, el autor, con buen criterio, hace referencia al principio *favor libertatis*, abogando por una interpretación favorable del ejercicio de sus derechos, una interpretación restrictiva de las cláusulas limitadoras de los derechos y una apuesta por una protección efectiva de los derechos en juego. Suscribo íntegramente su opinión relativa a que las restricciones generalizadas criminalizan *de facto* a los solicitantes, produciendo efectos discriminatorios y desvirtuando la institución de la protección internacional y, por tanto, deberán efectuarse *de forma individual, sobre una solicitud en concreto y sin causar indefensión al interesado; máxime, habida cuenta de la posición de vulnerabilidad del solicitante y de la importancia que revisten sus datos personales en todo el proceso de determinación del estatuto de refugiado o protección subsidiaria* (pág. 225).

Por último, la moderada postura del autor, a pesar de su juicio crítico, sobre la escasez de disposiciones del nuevo sistema de garantías relativas a la protección de datos, es digna de especial encomio. El autor recuerda como la priorización de los derechos de los solicitantes comportaría una excesiva limitación para el Estado en la consecución de los objetivos encaminados a gestionar eficaz y eficientemente las solicitudes de protección internacional y a preservar los intereses y seguridad nacionales, pero que, paralelamente, las autoridades nacionales tampoco pueden limitar de forma

[8] FRA — European Union Agency For Fundamental Rights, «Under watchful eyes: biometrics, EU IT systems and fundamental rights», *Oficina de Publicaciones de la Unión Europea*, 28 de marzo de 2018. Acceso el 28 de agosto de 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf

[9] FRA — European Union Agency For Fundamental Rights, «Fundamental rights and the interoperability of EU information systems: borders and security», *Oficina de Publicaciones de la Unión Europea,* 07 de julio de 2017. Acceso el 28 de agosto de 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf

indiscriminada los derechos de los solicitantes bajo esas mismas premisas. En análoga línea, a pesar de mostrarse partidario de la interoperabilidad, reclama sumo cuidado para que ello no se convierta en una *interconexión automática de información sino que una nueva técnica que favorezca la sinergia de esfuerzos para dar solución a escenarios realmente complejos* (pág. 395). Así, aboga por un equilibrio continuo entre la seguridad nacional y jurídica en este ámbito y por evitar la criminalización y discriminación de este colectivo. Además insiste en la necesidad de configurar *marcos jurídicos proactivos*, lo que nos recuerda, tal y como pone de relieve en sus investigaciones más recientes, la importancia de la responsabilidad proactiva de aquellos que gestionan y procesan información vinculada a procedimientos de protección internacional o cuestiones más amplias ligadas a la seguridad. Esto inexorablemente implica asegurar que se configuran sistemas de privacidad por diseño y por defecto (de las propias herramientas digitales utilizadas en el tratamiento de los datos recopilados) como ya venía abogando en trabajos anteriores (Viguri Cordero 2021, 160-176; y Viguri Cordero 2021, 1-12).

Como decíamos al principio, en las últimas tres décadas hemos asistido a una profunda transformación en muchos ámbitos de las competencias compartidas entre la UE y los Estados miembros, especialmente en las relativas al conocido como Espacio de Seguridad, Libertad y Justicia. La evolución de las tecnologías digitales ha sido un componente indispensable de estos esfuerzos, incluyendo la toma de huellas dactilares, la elaboración de perfiles y la vigilancia de los viajes, supuestamente legitimados bajo preocupaciones de seguridad nacional y pública. La creación y el funcionamiento de las bases de datos de inmigración paneuropeas es un ejemplo destacado en este contexto. La obra que tenemos entre nuestras manos no sólo analiza, de manera exhaustiva y con crítica constructiva, muchos de los componentes principales de la SECA (Dublín y Eurodac), la GEFC y la propuesta de reforma de la AAUE, sino que también, y lo que es más importante, propone elementos y aspectos concretos susceptibles de mejora que no me atrevo a desvelarle al futuro lector, pero que se encuentran perfectamente resumidos al final de la obra (págs. 395-397).

La obra es muy recomendable para los estudiosos de los dos derechos fundamentales examinados y también para aquellos, como la que suscribe estas líneas, que buscan una obra que actúe como «la última palabra», hasta la fecha, sobre un nuevo ámbito condicionado por las NTIC y por amenazas cambiantes y en el que continuamente se multiplica el número de instrumentos normativos (sean vinculantes o programáticos) y publicaciones, todo lo cual dificulta el seguimiento. No sólo estamos ante una obra que revela solvencia estructural y rigor metodológico, otorgándole una notable solidez científica, sino que además estamos ante un académico que exige suma cautela y nítida certeza jurídica en un ámbito tan delicado y sensible no sólo para los Estados soberanos miembros de la UE sino también, y sobre todo, para las personas afectadas en procedimientos de protección internacional.

La garantía de los derechos de distintas categorías de personas migrantes de terceros países afectados por el procesamiento de sus datos es un tema central de este trabajo, no sólo desde el punto de vista de los derechos individuales, sino también desde el punto de vista de la conformación (y limitación) de la acción del Estado en una sociedad (y organización supranacional) democrática. Sin duda, sería sumamente ingenuo e ignorante de mi parte pensar que las NTIC y los flujos migratorios no generarán más desafíos que los que observamos y nos preocupan actualmente, o que estos se podrán resolver en un futuro a corto plazo. Ante las preguntas que surgen, en lo que se refiere a cuánto margen de libertad estamos dispuestos a sacrificar en un Estado democrático para obtener un grado suficiente de seguridad, como con casi todo en esta vida, en el término medio y la moderación está la virtud. Así, Viguri Cordero insiste (y a la luz de sus argumentos acaba probablemente convenciendo a aquellos lectores escépticos) en que si bien *a priori*, pudiera parecer que estamos ante intereses verdadera y perpetuamente contradictorios entre sí, *de facto* acaban por complementarse para la consecución de diversos objetivos, entre los que se encuentra la protección efectiva de las personas solicitantes de protección internacional, la gestión de las fronteras y la prevención de la delincuencia en su sentido más amplio (pág. 392).

Con anterioridad a la lectura de esta obra, encontraba difícil vislumbrar dónde se encontraba esa dosificación mesurada. Sin embargo, gracias a *Seguridad y Protección de Datos en el Sistema Europeo Común de Asilo,* estamos mejor preparados jurídicamente para afrontar las mejoras necesarias del sistema europeo de protección de los derechos (tanto de asilo como de protección de datos) y estamos más cerca de encontrar un mejor equilibrio entre los imperativos de seguridad de los últimos años y la protección efectiva de los clásicos y emergentes derechos de los más vulnerables.

Mónica Martínez López-Sáez
Centro de Estudios Políticos y Constitucionales

VIGURI CORDERO, Jorge Agustín, *Seguridad y Protección de Datos en el Sistema Europeo Común de Asilo*, Tirant lo Blanch, Valencia, 2021, 447 pp., ISBN 978-84-1378-17-09.

http://dx.doi.org/10.18543/ed-69(2)-2021pp353-365