La importancia de los contextos. Datos personales y tratamiento[1]

Daniel Jove Villares

Doctor por la Universidade da Coruña

1. Algunas partes de este trabajo han sido presentadas en el XX Congreso de la Asociación de Constitucionalistas de España, celebrado en Cáceres los días 23 y 24 de marzo, puede consultarse el texto de la comunicación en: https://www.acoes.es/wp-content/uploads/2023/03/Comunicacion_Daniel-Jove_ACE.docx. Por otra parte, dada la naturaleza de esta publicación, se ha incidido más en el proceso de elaboración y en cuestiones metodológicas y menos en las reflexiones dogmáticas que conforman la tesis. Para conocer el fondo argumental de la tesis, vid. *La protección de lo sensible, o cuando la naturaleza del dato no lo es todo*, Tirant Lo Blanch (fecha de publicación: a lo largo del segundo semestre de 2023).

fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico

SUMARIO:

NOTA BIOGRÁFICA:

Daniel Jove Villares es graduado en Derecho por la Universidade da Coruña, con premio extraordinario. Máster en Derecho Constitucional (CEPC-UIMP) y, desde enero de 2022, doctor en Derecho por la Universidade da Coruña (*cum laude*, mención internacional y premio extraordinario). Durante la etapa predoctoral contó con un contrato de la Xunta de Galicia (2017) y, a partir de 2018, con un contrato FPU. Ha realizado estancias en la Università della Calabria, la Cátedra de Derecho y Genoma Humano de la Universidad del País Vasco y el Max Planck Institute for Comparative Public Law and International Law. Ha sido profesor interino de sustitución en la Universidade da Coruña hasta junio de 2023, momento en el que se incorporó a la Universidad Carlos III como profesor ayudante doctor.

I. BAGAJE Y ELECCIÓN DEL TEMA

¿Somos lo que los datos dicen (o no dicen) que somos? En la fría lógica algorítmica y en los sueños más lúbricos los apologetas de lo digital, el *doppelganger* virtual no deja de ser otra forma de representar a la persona real. Siempre se podrá aducir que las personas somos más que la mera agregación de nuestros datos, que hay intangibles que la computación no entiende, pero, poco a poco, la técnica va evolucionando para levantar esos velos y lograr la radiografía perfecta del ser (algunos usos de las neurotecnologías apuntan en esa dirección).

Hoy, los datos, personales o no, y sobre todo la inteligencia artificial que se alimenta de ellos, constituyen una de las grandes preocupaciones y temores de buena parte de los que nos dedicamos al Derecho (la explosión de *papers*, congresos, seminarios y jornadas sobre esta temática da buena cuenta de ello). La

capacidad de la IA para cambiar el tejido de la sociedad, y dar forma a un modelo de convivencia diferente, justifica el nivel de atención que se ha de prestar a su regulación. Frente al cambio de paradigma que estamos viviendo, es necesario activar todos los resortes del Derecho para tratar de gestionar los cambios que se producen, así como los que el futuro pueda deparar. La defensa (y pervivencia) de los derechos y libertades así lo exige.

Sin embargo, en 2016, cuando terminé el máster del Centro de Estudios Políticos y Constitucionales, no era la IA sino los datos personales y su regulación los que suscitaban la atención de los operadores jurídicos. La causa de ese renovado interés por la autodeterminación informativa fue la aprobación, en abril de 2016, del Reglamento General de Protección de Datos (RGPD). Esta norma, que se aplicaría a partir de 2018, es la vanguardia de la Estrategia digital europea[2], con la que la UE pretende lograr un doble objetivo: aprovechar las oportunidades que la tecnología y la economía basada en datos propicia y, a la vez, garantizar los derechos de la ciudadanía. El RGPD representa algo más que una mera actualización del marco regulatorio, es el reflejo de una política estratégica acerca de cómo habrá de ser la Europa de los próximos años, de cómo se han de afrontar los desafíos de un mundo cada vez más virtual. El cambio de modelo de protección, el paso de un enfoque esencialmente reactivo a uno proactivo, en el que la atención al riesgo y a las particularidades del tratamiento pasan a ser el eje central, apuntan en esa dirección.

Curiosamente, en mi caso, el interés por los datos personales y su regulación no llegó de la mano del RGPD, sino de un modo más indirecto. En efecto, al terminar el máster y comenzar el doctorado me planteé cuál debería ser el tema sobre el que habría de versar mi tesis doctoral. Debo reconocer que tuve la fortuna de tener libertad para escoger (no siempre es posible, a veces la posibilidad de acceder a un contrato predoctoral va anudada a una concreta línea de investigación), y si bien barajé la posibilidad de continuar con la temática del Trabajo Fin de Máster (la naturaleza y exigibilidad de los derechos reconocidos en los Estatutos de Autonomía), finalmente opté por comenzar de cero con algo nuevo y sustancialmente diferente. La inspiración para hacerlo, sin embargo, provino de una previsión estatutaria, concretamente el artículo 22 del Estatuto de Autonomía de Andalucía. En él, se reconoce el derecho de los pacientes andaluces a la "confidencialidad de los datos relativos a su salud y sus características genéticas". Datos de salud y datos genéticos fueron los términos que atrajeron mi atención y me suscitaron curiosidad, ¿cuál era su alcance? ¿Cómo se relacionaban y se gestionaban los supuestos fronterizos? ¿Cuándo un dato personal podía ser calificado como dato de salud? ¿Cómo se gestionaba el hecho de que un dato de salud fuese un dato personal y, a la vez, una información íntima? Las preguntas se agolpaban, así que resultaba evidente que esa era una temática que valía la pena explorar.

2. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_es

Fue el estudio de los datos genéticos y de los relativos a la salud el que me llevó al RGPD y al resto de normativa dedicada a disciplinar el tratamiento de la información personal. En el art. 9 del RGPD constaté que no todos los datos personales tienen la misma consideración jurídica, algunas tipologías están revestidas de una protección reforzada: las denominadas categorías especiales, entre las que se inscriben los datos genéticos y los relativos a la salud.

A las dudas iniciales se fueron adicionando otras, como, por ejemplo, ¿por qué establecer un conjunto tasado y cerrado de categorías especiales? ¿Por qué esas tipologías y no otras? ¿Son igual de sensibles todos los datos categorizados como especiales? ¿Cuándo pertenece un dato a una determinada tipología? ¿Es el contenido de la información lo que determina la condición especial? ¿Es la naturaleza de la información el único criterio a considerar para conferir a un dato la condición especial? ¿Qué ocurre con los datos de naturaleza "variable", esto es, con aquellos que pueden ser clasificados como pertenecientes a una determinada tipología en unos contextos, pero no en otros? En definitiva, ¿es el régimen de protección establecido por la normativa europea el más adecuado para proteger los derechos y libertades de la ciudadanía frente al tratamiento de la información personal?

Al constatar que las incógnitas que rodeaban a los datos genéticos y los relativos a la salud eran parangonables del conjunto de tipologías especiales, opté por hacer de ellas mi objeto de estudio. Comprender su razón de ser podría proporcionar las claves para dar respuesta a las preguntas que plantea su existencia y particular régimen de protección. El rumbo estaba fijado, tocaba comenzar a navegar.

II. LA IMPORTANCIA DE LOS CONTEXTOS

Dado el singular objeto de la tesis que pretendía elaborar (la pertinencia de un sistema de protección en el que se establece un conjunto tasado y cerrado de categorías especiales), conocer la realidad en la que se despliega la normativa de protección de datos constituía una variable fundamental a la hora de evaluar la adecuación de las medidas normativas implementadas. Consecuentemente, el contexto se erigió en uno de los ejes centrales del trabajo, un hilo conductor que contribuyó sustancialmente a dar coherencia al conjunto. Su transversalidad silente no obsta para que, al menos en tres momentos, se manifieste su impronta de manera explícita: al abordar la era digital y sus desafíos; al fijar el marco normativo y territorial objeto de estudio y, finalmente, al valorar su adecuación como criterio identificativo de lo sensible. De los tres, este último tiene un impacto directo en los resultados de la tesis, por lo que se analizarán sus efectos en un momento posterior de este trabajo. En lo relativo a los otros dos, su capacidad condicionante es menos evidente, pero no por ello desdeñable.

El momento histórico en el que se aplica una determinada medida es un factor crucial. La era digital está rodeada de una serie de particularidades que la hacen

especialmente desafiante; su dinamismo, la capacidad evolutiva de las tecnologías y, consecuentemente, de los riesgos que los usos de estas deparan, convierten en perentoria la adopción de respuestas normativas capaces de responder tanto a los desafíos presentes como a los retos que el futuro inmediato pueda deparar. Esa particular condición hace que el legislador deba trabajar sabiendo que el principal problema a solventar no es el presente, sino aquel que está por venir. Los profundos cambios que el desarrollo técnico está provocando en el modo de vivir y relacionarse en sociedad exigen repensar la manera de legislar. Frente a las múltiples amenazas de la hidra digital, ante su capacidad para generar nuevos peligros cuando se cercenan los existentes, son necesarios instrumentos jurídicos que combinen flexibilidad (en las medidas a adoptar) y precisión (en las respuestas a ejecutar). Si no se es consciente de la singular realidad en la que estamos inmersos, si no se evalúan los riesgos futuros, las normas están condenadas a la obsolescencia antes de comenzar siquiera a producir efectos.

La segunda variable contextual a considerar es la relativa al marco territorial y cultural en el que se despliega la regulación objeto de estudio. En este caso, optar por el ecosistema europeo del dato no fue una decisión casual. Con el RGPD se produce una traslación del centro de normación del derecho a la protección de datos. A partir de él, los elementos básicos, el contenido esencial del derecho fundamental, pasan a venir definidos por la normativa de la UE. Es cierto que el RGPD deja margen a los Estados miembros para la concreción de medidas específicas, como también lo es que, a la hora de evaluar si el sistema de protección de los datos sensibles es el adecuado, debemos estar a lo previsto en la regulación europea, pues es la que fija las condiciones básicas de actuación.

Además, la UE, en lo relativo al tratamiento de la información personal, ha abanderado la apuesta por un modelo en el que, junto a la libre circulación de los datos y a su aprovechamiento económico, se asegure el respeto por los derechos y libertades, fijando unos mínimos ineludibles que, de no atenderse, harán del tratamiento una opción jurídicamente inaceptable (quizá el reflejo más elocuente sean las dificultades para establecer un acuerdo que garantice un flujo de datos seguro, y respetuoso con los derechos, entre Europa y Estados Unidos).

En definitiva, al acotar el marco de actuación se opta por una forma concreta y específica de entender el derecho a la protección de datos, por una cultura jurídica específica. Comprender la idiosincrasia del sistema de protección es decisivo. El éxito o fracaso de cualquier medida que se proponga no depende, en exclusiva, de su eficacia o calidad técnica, sino de su capacidad para inserirse con naturalidad en la práctica jurídica. La coherencia, razonabilidad y predictibilidad del conjunto es fundamental, pues permite a los operadores de datos y a la ciudadanía entender la lógica inherente al modelo y acomodar mejor sus actuaciones a los parámetros normativamente fijados.

En la tesis, la cognición de la idiosincrasia del sistema europeo de tratamiento de datos de carácter personal ocupa un espacio destacado (quizá excesivo, pero creo

que necesario). En él se analizan los rasgos definitorios del RGPD, constatando la apuesta del legislador europeo por un modelo de protección eminentemente proactivo, en el que la atención al riesgo y la adecuación a las particularidades de cada tratamiento concreto son la regla general (en contraposición con la lógica reactiva que había venido imperando en las regulaciones precedentes). Sin embargo, cuando el análisis se centra en la regulación de las categorías especiales, parece que esa apuesta se diluye, pues se observan rasgos propios de modelos clásicos de protección, como son: la definición en abstracto del régimen a aplicar o el establecimiento de un conjunto tasado y cerrado de informaciones a las que se reserva, en exclusiva, la condición de dato especial.

Ante esa tesitura, además de considerar la coherencia intranormativa, se optó por examinar las dinámicas legislativas, esto es, hacia dónde apuntan los desarrollos normativos de la UE en este ámbito. De este modo, se analizó la idiosincrasia de las regulaciones (las aprobadas y las que están aún en fase de tramitación, como la propuesta de Reglamento de inteligencia artificial) que dan/darán forma al espacio europeo del dato. De su estudio se desprende que la estrategia legislativa europea considera que la proactividad, la atención al riesgo y la personalización en las respuestas constituyen el modo más adecuado para afrontar los desafíos que el dinamismo de la era digital plantea. De este modo, las dos variables contextuales (la temporal y la territorial-normativa) terminaron confluyendo.

III. LA COMPLEJIDAD DE ESTRUCTURAR EL RELATO

Una vez establecido el objeto (la adecuación del modelo de protección establecido para las categorías especiales) y fijado el contexto (tanto el normativo/cultural como el temporal), el siguiente paso era estructurar el trabajo, fijar qué elementos debía abordar y construir un armazón argumental que permitiese alcanzar una conclusión jurídicamente sólida. No fue una tarea sencilla. El relato es fundamental en cualquier trabajo, pero, en este, por sus características, había apartados que me iban a obligar a transitar por sendas muy concurridas y, por lo tanto, en las que el interés de quienes tuviesen a bien leer la tesis podría decaer.

Con carácter general, se plantearon dos posibles vías para alcanzar el resultado (al hacer la monografía posterior descubrí que había una tercera (y seguramente haya más), por lo que parece razonable no obcecarse con una hoja de ruta, y centrarse en saber a dónde se quiere llegar). La primera consistía en partir de la exégesis de las categorías especiales para, a partir de su conocimiento, plantear las propuestas de mejora de su marco regulatorio y concluir validando la viabilidad de dichas propuestas. Sin embargo, esta opción resultaba poco satisfactoria, el conjunto de elementos a considerar en la comprobación de la propuesta de mejora llevaba, ineludiblemente, a incurrir en más reiteraciones de las deseables. Además, al convertir las propuestas en el hilo conductor del proceso de verificación, se diluía su impacto e importancia. Por si no fueran

razones suficientes, ese modo de afrontar el problema comportaba el riesgo de incurrir en una acomodación inconsciente de los criterios de control, para hacerlos compatibles con los contenidos de las propuestas realizadas.

Descartada esta posibilidad, se apostó por una aproximación holística y gradual al modelo europeo de protección de datos, yendo de lo general a lo particular, a la vez que se iban reseñando aquellos factores que pudieran tener impacto en su regulación futura. Esta opción metodológica tuvo como resultado un trabajo estructurado en cinco capítulos. De ellos, los cuatro primeros, están dedicados a las variables que, de algún modo, inciden en el régimen jurídico de la protección de los datos personales y, especialmente, en la regulación de las categorías especiales, a saber: la era digital, la conformación y consolidación del derecho a la protección de datos, el ecosistema normativo europeo del dato y la naturaleza del derecho fundamental a la protección de datos.

Así, en el Capítulo primero, se describe, de manera sucinta, aunque no por ello carente de crítica, el contexto tecnológico actual y su impacto en el modo en que vivimos en sociedad. No cabe duda de que el constante desarrollo de ingenios tecnológicos capaces de afectar al modo en que se desarrolla nuestra personalidad y nos percibimos a nosotros mismos y nuestro entorno plantea retos jurídicos de primer orden. Si bien el derecho a la protección de datos no se circunscribe al entorno virtual, es evidente que es en la esfera digital donde se despliega en toda su magnitud. Por lo tanto, no pueden desconocerse los efectos que sobre este derecho pueda tener el particular ambiente en el que se ejercita.

Si el Capítulo primero realiza una panorámica general de la era digital, escrutando el presente y tratando de advertir los desafíos que el futuro pueda deparar, el Capítulo segundo echa la vista atrás, para tratar de encontrar, en el proceso de construcción doctrinal, jurisprudencial y normativa del derecho a la protección de datos aquellos elementos que permitan comprender mejor su regulación actual. Una vez fijado el marco espacio-temporal en que se despliega el derecho a la protección de datos, se aborda, en el Capítulo tercero, el ecosistema europeo del dato. El análisis de las diversas normativas que, de algún modo, inciden en el tratamiento de la información personal sirve para poner de manifiesto la complejidad y completitud del modelo europeo de tratamiento de la información. Ciertamente, el Reglamento General de Protección de Datos es la piedra angular del sistema, y en él se establecen sus elementos básicos. Pero existe todo un entramado normativo, en constante expansión, que vale la pena considerar; pues facilita la cognición de la idiosincrasia del modelo europeo y, consecuentemente, permite que, a la hora de elaborar cualquier propuesta alternativa, esta pueda ir en consonancia con la cultura jurídica europea. Evitando, con ello, las disonancias e ineficiencias que pudiera deparar una proposición ajena a nuestra realidad jurídica.

Con todo, el elemento determinante a la hora de valorar la viabilidad de cualquier propuesta que suponga una modificación del marco normativo, es que esta sea

respetuosa y compatible con los contenidos del derecho fundamental a la protección de datos. Por consiguiente, el Capítulo cuarto tiene como cometido analizar la naturaleza de este derecho en su configuración europea. Pudiera plantearse aquí si no habría sido mejor analizar primero el derecho fundamental y luego el ecosistema normativo creado a su amparo, sin embargo, la necesidad de explicar el proceso de europeización del derecho, unido al carácter general con que se estudia el marco regulatorio europeo, del que, sobre todo, interesaba conocer sus características básicas y su idiosincrasia, hacían más coherente abordar primero las características de las normativas que inciden en el tratamiento de la información personal, para, en un segundo momento, analizar con detalle la naturaleza del derecho fundamental. Como puede comprobarse, cada uno de los 4 capítulos proporciona ciertas claves que resultan imprescindibles para poder evaluar el sistema europeo de protección de los datos sensibles, y determinar su margen de mejora.

Finalmente, el Capítulo quinto, está dedicado a las categorías especiales, tanto a su razón de ser como a la proposición de alternativas regulatorias que permitan alcanzar, de un modo más eficiente, las finalidades que subyacen a su existencia. A su vez, se elucubra con la posibilidad de adoptar un concepto de dato personal más amplio, en el que el riesgo, la finalidad y los efectos del tratamiento tengan una relevancia mayor.

Definir, en los cuatro primeros capítulos, el marco de lo jurídicamente posible, permitía articular las propuestas con las que se cierra el trabajo desde la certeza de su compatibilidad con la configuración europea del derecho a la protección de datos. De este modo, se logró evitar ciertas reiteraciones explicativas y posibilitó un desarrollo coherente de la argumentación. En este sentido, debe señalarse que, los Capítulos iniciales, están pensados para ser algo más que una parte del conjunto. Todos tienen cierto carácter autoconclusivo, sin perjuicio de que sus aportaciones singulares terminan coadyuvando a la determinación de las posibilidades de regulación y desarrollo del derecho a la protección de datos, al delimitar los modos en que pueden configurarse las categorías especiales.

IV. LAS DUALIDADES DETECTADAS EN LAS CONCLUSIONES PARCIALES

Del conjunto de conclusiones parciales obtenidas en los primeros cuatro capítulos quisiera destacar tres que resultan especialmente relevantes, tanto por su relevancia intrínseca, como por el impacto en la consideración de las categorías especiales. Además, las tres comparten un rasgo común, en ellas existe algún tipo de dualidad que es necesario conjugar. En efecto, tanto el análisis del marco normativo europeo, como la naturaleza del derecho fundamental y, por supuesto, el binomio dato-tratamiento, son el reflejo de, al menos, dos elementos en busca de equilibrio y adecuación.

Comencemos por la más evidente, la referida a la relación entre dato personal y tratamiento. El dato personal es el centro de imputación del derecho a la protección de datos. Es el elemento material sobre el que se despliega el derecho fundamental. La existencia del vínculo dato-persona es el detonante primario para la activación de los mecanismos de protección normativamente previstos. Que esto sea así resulta perfectamente razonable, en la medida en que el dato identifica o revela información sobre un determinado sujeto, es lógico que éste se convierta en el pilar en torno al que se construye la protección normativa de los bienes jurídicos de la persona.

Ahora bien, si se observa la evolución del concepto dato personal, se constata cómo se ha ido ampliando el alcance del nexo dato-persona, transitando desde una conexión muy evidente, representada por la afirmación: dato personal es cualquier información referida a una persona identificada, hasta conexiones menos evidentes, como las que se refieren a la identificabilidad o la posibilidad de singularización, sin exigir una identificación precisa. Sin embargo, tal y como pusieron de manifiesto, el Grupo de Trabajo del Artículo 29 primero[3] y el Tribunal de Justicia de la Unión Europea después en el asunto Nowak[4], cabe un modo diferente de identificar la existencia del vínculo dato-persona. Es posible calificar como dato personal a aquellas informaciones que, por contenido, finalidad o efectos conecten con una persona determinada. La inclusión de la finalidad y los efectos supone una ampliación sustancial de las informaciones que pueden ser calificadas como dato personal. De adoptase como criterio general, se estaría produciendo una extensión del ámbito de aplicación de la normativa relativa al tratamiento de datos personales y, consecuentemente, de su régimen protector.

Aunque el concepto de dato personal sea el centro de imputación del derecho fundamental, no puede obviarse la existencia de un segundo detonante, también indispensable, para la activación de las medidas de protección: el tratamiento. Efectivamente, solo se puede aplicar la normativa de protección de datos si la información personal se ve incursa en algún tipo de operación. En caso contrario, al no existir riesgo para los bienes jurídicos de las personas, no hace falta acudir a remedio jurídico alguno. El tratamiento es, por tanto, una pieza esencial del derecho a la protección de datos.

Más allá de esa función de detonante aplicativo, debe destacarse que el tratamiento ha ganado en relevancia desde la aprobación del Reglamento General de Protección de Datos. La realidad del tratamiento, los riesgos que entraña, las medidas de seguridad que se han de implementar en cada caso concreto,

3. Dictamen 4/2007, sobre el concepto de datos personales, de 20 de junio de 2007. Puede consultarse en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf.

4. STJUE asunto C-434/16, Peter Nowak c. Data Protection Commissioner, de 20 de diciembre de 2017

son factores cruciales para la determinación de las exigencias jurídicas que los operadores de datos han de asumir. A pesar de esta relevancia, lo cierto es que aún tiene cierto margen de expansión. Sin ir más lejos, en caso de consolidarse la utilización de la finalidad y los efectos como criterios identificativos de la existencia de un dato personal, el tratamiento se convertiría en lo verdaderamente relevante. Sería su realidad la que permitiría valorar la finalidad y los efectos del uso de una determinada información y, de ser el caso, calificarla como dato personal.

La segunda de las dualidades anida en las normativas relativas al tratamiento de la información personal y, singularmente, en el Reglamento General de Protección de Datos. Del estudio de las normativas en vigor, así como de las propuestas en las que la Unión Europea está trabajando, se desprende la existencia de una apuesta, cada vez más evidente, por modelos de protección basados en la proactividad, la prevención de riesgos y la flexibilidad en las respuestas jurídicas, de manera que sea posible adaptarlas a los diferentes escenarios y situaciones que el dinamismo de la era digital exige. No obstante, esa tendencia legislativa no está plenamente consolidada, pues perviven en el RGPD ciertos elementos propios un modelo más rígido de protección en abstracto, v. gr. la regulación de las categorías especiales.

Esta dualidad dota a la regulación sobre tratamiento de datos de un carácter híbrido. En el que, si bien la proactividad y la atención al riesgo son los factores clave, no por ello se quiere dejar de aprovechar la mayor seguridad jurídica y certeza aplicativa que, en teoría, proporciona la predeterminación normativa de determinados supuestos. Este tipo de regulaciones híbridas puede resultar muy adecuadas para transicionar de un modelo de protección a otro; sin embargo, no dejan de entrañar un cierto riesgo. La pervivencia de elementos propios del modelo que se busca superar puede debilitar el cambio que se pretende implementar. En el caso de la normativa europea de protección de datos, conservar medidas de protección en abstracto puede llevar a aplicaciones mecanizadas que prescindan de la adecuación a la realidad del tratamiento, debilitando con ello la apuesta por la proactividad, la protección de datos desde el diseño y por defecto y la atención al riesgo.

La última de las dualidades que quisiera destacar está referida a la naturaleza del derecho fundamental a la protección de datos. Si se analiza este derecho desde una perspectiva teleológica, se observa que, desde sus orígenes, existe una doble finalidad que condiciona su morfología. Prueba de ello es que, las primeras regulaciones sobre la materia se focalizaban en proteger los derechos y libertades de la ciudadanía frente a las consecuencias que el uso de la información pudiera deparar. Solo posteriormente surgió la vertiente sustantiva y autónoma del derecho, caracterizada por la atribución de un poder de control y disposición sobre los datos a uno referidos, reflejo de la autonomía personal, la dignidad y el libre desarrollo de la personalidad.

Esas dos variables, protección de los derechos y poder de control y disposición, se han fusionado en el derecho fundamental, y permean a su regulación, como demuestra, de modo genuino, el artículo 1.2 del Reglamento General de Protección de Datos, al señalar que su cometido es proteger "los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales". El singular cometido de este derecho fundamental, su condición de instituto de garantía de otros derechos, su vinculación originaria con el derecho a la vida privada y su importancia para la economía y las relaciones entre particulares, han propiciado interpretaciones de todo tipo acerca de su naturaleza jurídica, incluidas algunas negadoras de su carácter iusfundamental, como la de Ralf Poscher[5].

En la tesis se valoran las diferentes opciones hermenéuticas para, finalmente, concluir que el derecho a la protección de datos, en su configuración europea, es un derecho fundamental autónomo, de configuración legal, pues exige que se regulen las condiciones que hagan jurídicamente aceptable el tratamiento de la información personal y, como aportación más significativa, se describe al derecho fundamental a la protección de datos como un simbionte con dos almas: El derecho a la protección de datos en sentido amplio, que se correspondería con la función instrumental de salvaguarda de los derechos y libertades. Y el derecho a la protección de datos en sentido estricto, que se compadece con las manifestaciones más vinculadas al ejercicio del poder de disposición y control sobre los datos personales (como sería el caso de las facultades de actuación o de las obligaciones de información del responsable). Solo combinando ambas facetas resulta posible la cognición de este derecho fundamental en toda su extensión.

V. LAS CATEGORÍAS ESPECIALES. ENTRE LA SEGURIDAD APLICATIVA Y LA EFICACIA EN LA PROTECCIÓN

Conforme al art. 9 del Reglamento General de Protección de Datos, son datos especiales las informaciones que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los datos genéticos, datos biométricos, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. Este listado de tipologías es una fuente constante de interrogantes.

¿Es igual la información fulanito tiene una gripe que el dato fulanito tiene una enfermedad degenerativa? ¿A una persona que busca empleo, qué dato le puede generar más problemas: su edad, su género o si está afiliada a un sindicato? ¿qué hacemos con las inferencias? Esto es, cómo afrontamos la posibilidad de poder

5. Poscher, Ralf. (2017). The Right to Data Protection. A No-Right Thesis. En Russell A. Miller (Ed.), Privacy and power: a transatlantic dialogue in the shadow of the NSA-affair (pp. 129-141). Cambridge: Cambridge University Press.

obtener información calificada como especial a partir de otra que no lo es. Por poner algunos ejemplos, el código postal es una variable que permite determinar la esperanza de vida de las personas y, sin embargo, en principio, no encaja en lo que se consideraría un dato relativo a la salud. Otro ejemplo, la ubicación, que no es un dato especial, permitió, en Corea del Sur, mediante las aplicaciones de rastreo que se usaron en la pandemia, conocer la orientación y preferencias sexuales de muchas personas. Un último ejemplo, uno que no requiere de tecnología alguna, el nombre de una persona, combinado con el nombre de su pareja, permite identificar su orientación sexual, es decir, obtener un dato especial. Como puede intuirse, si es posible hacer inferencias y deducciones básicas de información sensible a partir de otras que no lo son, qué no podrá hacerse mediante sistemas de *big data* e inteligencia artificial cuya característica principal es, precisamente, establecer correlaciones.

Para poder determinar si el modelo de protección diseñado por la normativa europea de protección de datos es el más adecuado, así como para poder plantear, en caso de que no lo fuese, alguna propuesta alternativa, el primer paso debiera ser, siempre que sea posible, comprender la naturaleza de aquello que pretende cuestionar. En este sentido, lo primero era identificar la razón de ser de las categorías especiales. En principio, dato es personal es aquel que ofrece información sobre algún aspecto de una persona identificada o identificable, sin embargo, hay algunos datos a los que, en atención a su naturaleza y capacidad para poner en riesgo los derechos y libertades, se les confiere una protección reforzada (Considerando 51 RGPD). Por lo tanto, su existencia se funda en una doble convicción: ni todos los datos son igual de valiosos, ni su uso entraña el mismo nivel de riesgo.

En el modelo europeo de protección de datos, esa condición especial está vinculada a la naturaleza del dato. De este modo, el mayor riesgo de discriminación y la capacidad más acuciada para revelar los aspectos más sensibles de la persona quedan inexorablemente unidos al contenido de la información. Sin embargo, si la razón de su existencia es la mayor probabilidad de discriminación de una determinada información, o tener una capacidad más acuciada para revelar los aspectos más sensibles de la persona; uno no puede dejar de preguntarse por qué no se utilizan estos criterios para determinar las medidas de protección, en lugar de establecer normativamente un conjunto tasado y cerrado de tipologías especiales.

Con esas premisas como referencia, el legislador europeo identificó el conjunto de tipologías que consideró merecedoras de especial consideración. Y no es una selección carente de lógica. En ella están presentes las clásicas categorías sospechosas del derecho antidiscriminatorio (el origen racial, la orientación sexual o las convicciones religiosas) y también datos, como pueden ser los relativos a la salud o los genéticos, que revelan los aspectos más íntimos de la persona. Sin embargo, adolece de ciertas carencias. De una parte, no se prevé una cláusula de apertura que permita extender los supuestos afectados a otras tipologías

potencialmente discriminatorias (género, edad o capacidad económica, por poner algunos ejemplos). De otra, ciertas categorías (los datos relativos a la salud, los datos genéticos y los datos biométricos (art. 4 RGPD)) incorporan definiciones que delimitan qué informaciones pueden pertenecer a esa tipología, lo que introduce una rigidez adicional a un ámbito ya de por sí poco flexible. En la era del dinamismo y la inteligencia artificial no parece una característica especialmente positiva, entonces, ¿por qué se implementó esta opción legislativa?

Probablemente porque tiene una fortaleza muy relevante, se trata de un modelo que proporciona a los operadores de datos una importante seguridad aplicativa. Si el dato personal en cuestión puede adscribirse a alguna de las tipologías previamente establecidas, automáticamente se puede saber cuáles son las medidas a implementar. A esta razón principal, y por sí sola suficiente, se le pueden adicionar otras, como podría ser el peso de las dinámicas históricas, pues estamos ante un mecanismo de protección por el que se ha apostado, de manera constante y desde hace décadas, para limitar los riesgos adicionales que el uso de ciertos datos entraña para los derechos y libertades. Quizás sea esa raigambre en la cultura jurídica europea la que haya hecho que, hasta cierto punto, la regulación de las categorías especiales no termine de encajar en el paradigma (anticipatorio y preventivo) que el RGPD pretende promover.

Con todo, el riesgo de obtener información sensible a partir de otra que no lo es mediante inferencias, sumada a la insatisfacción que me generaba la incapacidad del régimen de protección de las categorías especiales para cumplir, de manera completa y efectiva, con el objetivo que justifica su existencia (evitar situaciones discriminatorias o especialmente peligrosas para los derechos, derivadas del tratamiento de ciertos datos), justificaban la búsqueda de sistemas alternativos de garantía.

VI. LAS PROPUESTAS DE MEJORA EN LA PROTECCIÓN DE LO SENSIBLE

Frente a las incoherencias e ineficiencias del modelo previsto en el RGPD, se plantearon diversas soluciones. La más sencilla sería extender, por vía interpretativa, el alcance de las categorías especiales. Esta opción ya la había propuesto algún sector de la doctrina, por ejemplo, Romeo Casabona respecto de los datos relativos a la salud, y ha sido acogida por el TJUE, concretamente en el asunto C-184/20, OT y Vyriausioji tarnybinės etikos komisija, de 1 de agosto de 2022 (meses después de que hubiera defendido la tesis). Conforme a esta sentencia, también habrán de ser considerados como especiales aquellos datos que, "indirectamente", sean susceptibles de revelar información relativa a alguna de las categorías especiales.

Con ese pronunciamiento, el TJUE busca solventar el problema de las inferencias, pero, como apunté en la tesis antes de que hubiese sentencia y mantengo ahora que la hay, esta solución tiene un problema base, y es que no está libre

del pecado original, ello es así porque seguimos condicionados por el conjunto tasado y cerrado de categorías que el legislador ha identificado como especiales. Consecuentemente, sigue sin darse respuesta a situaciones en las que el riesgo de discriminación deriva, por ejemplo, y sin ánimo exhaustivo, de cuestiones económicas, de cuestiones relativas a la edad o al género de la persona. Por lo tanto, aunque es un avance, no es la panacea. Había que buscar otras posibilidades de acción que resulten más satisfactorias. Se me ocurrieron dos propuestas, una moderada y otra más rompedora, aunque ambas exigen la reforma del RGPD.

La solución moderada busca cambiar el foco, del dato al tratamiento, es decir, que en lugar de datos especiales se opere sobre la base de tratamientos especiales. De este modo, la atención al contexto y a las posibles inferencias serían un acto obligado, lo que permitiría dar encaje legal al criterio interpretativo establecido por el TJUE. El cambio en la literalidad del precepto no sería profundo, sin embargo, representaría toda una declaración de principios. Así, el artículo 9.1 del RGPD podría quedar redactado del siguiente modo:

Quedan prohibidos los tratamientos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los que estén dirigidos a identificar de manera unívoca a una persona física, los vinculados a conocer la información genética de una persona física, así como los relativos a su salud, su vida sexual u orientación sexual.

Es cierto que este cambio sigue adoleciendo del problema derivado de la existencia de un conjunto tasado de categorías especiales, no obstante, esto podría solventarse de un modo relativamente sencillo, por ejemplo, incorporando un aditamento en el que se indicase que también tendrá condición especial *cualquier otro tratamiento que pueda dar lugar a un supuesto discriminatorio.*

En lo que respecta a los criterios enervantes de la prohibición del tratamiento previstos en el apartado segundo del art. 9 RGPD, podrían conservarse o, si se quisiera realizar un cambio que proporcionase aún más flexibilidad al modelo, podrían incorporarse el nivel de riesgo y el potencial discriminatorio como baremos capaces de determinar si el tratamiento es jurídicamente admisible.

En lo relativo a la propuesta rupturista, que a mí personalmente me gusta más, consistiría en suprimir las categorías especiales de datos, sustituyéndolas por un modelo de protección de riesgos racionalizado. La lógica de esta opción es la siguiente, si cualquier dato es susceptible de ser considerado como especial en el contexto adecuado, entonces la predeterminación de lo sensible ya no funciona como mecanismo de protección. Consecuentemente, debe acudirse a las razones que subyacen a la existencia de las categorías especiales, es decir, el riesgo de afectación de los derechos o las posibilidades de discriminación que cada tratamiento comporte. Conforme a esta opción, si el tratamiento no ofrece garantías suficientes o comporta un riesgo inasumible no podrá llevarse a efecto, y esto con independencia de la naturaleza de los datos que se traten en él.

De este modo, serían los peligros concretos de cada tratamiento los que modularían las medidas de protección a adoptar, propiciando una protección más adecuada para cada caso concreto. Desde el punto de vista normativo, sería preciso fijar los umbrales a partir de los cuales el tratamiento dejaría de ser aceptable. En cuanto a la naturaleza de los datos tratados, esta se mantendría como uno de los criterios a considerar, pero no sería el único, ni condicionaría, apriorísticamente, las medidas a adoptar. En todo caso, si a efectos puramente orientativos se estableciese un listado de informaciones sensibles, este debería ser abierto y estar conectado con el resto de normativas de derecho antidiscriminatorio.

Esta propuesta, que *prima facie* puede parecer muy radical, no exigiría, desde el punto de normativo, reformas traumáticas. La proactividad, las evaluaciones de impacto, la protección de datos desde el diseño y por defecto, así como un conjunto sólido de derechos y principios, elementos necesarios para el éxito de esta medida, ya forman parte de la normativa de protección de datos, lo único que falta es creérselos y, sobre todo, aplicarlos. Si se hace, la reforma es viable y, en mi opinión, deseable.

VII. UNA CORRELACIÓN EXTRAÍDA POR ELEVACIÓN: LA RELACIÓN ENTRE DATO Y TRATAMIENTO

La existencia de categorías especiales de datos y la adecuación de su sistema de protección es el principal problema que se afronta en la tesis. Sin embargo, al analizar el modelo europeo de protección de datos, no pude dejar de notar que parte de los razonamientos y dudas que se suscitan en torno a los datos sensibles podrían trasladarse, con una intensidad diferente, a la relación dato personal-tratamiento, sobre todo si se toma en consideración que la anonimidad de la información no es una certeza atemporal. Los datos anónimos de hoy (excluidos del ámbito de aplicación de la normativa de protección de datos) podrían ser personales mañana.

Aunque la división dato personal-dato no personal no es tan nítida y absoluta como se pudiera pensar, pues cierta porosidad, lo cierto es que, el modelo europeo de protección de datos es tajante en cuanto a su ámbito de aplicación material. Si la información tratada es susceptible de ser calificada como un dato personal, se aplica la normativa de protección de datos, si es un dato anónimo, no. El dato personal es el condicionante aplicativo del sistema, en él se produce la conexión que dota de subjetividad al tratamiento y justifica que se activen los mecanismos de protección inherentes al derecho fundamental a la protección de datos. Consecuentemente, si se quiere ofrecer seguridad jurídica a quienes operan con información, es imperativo establecer qué se entiende por dato personal y fijar los criterios hermenéuticos que permiten identificar su existencia.

En este sentido, el RGPD establece una definición de dato personal bastante amplia, pues extiende esa calificación a “toda información sobre una persona

física identificada o identificable ("el interesado")" (art. 4). Con todo, perviven ciertos ámbitos de indeterminación. Así, en principio, se considera que cuando la capacidad, los costes o el tiempo requeridos para establecer el vínculo dato-persona sean desproporcionados, no se considerará dato personal. Sin embargo, la razonabilidad de los esfuerzos no deja de ser un criterio dotado de cierta subjetividad y, en todo caso, cambiante, pues la tecnología puede evolucionar y hacer que aquello que se consideraba seguro deje de serlo (v. gr. la computación cuántica puede hacer que contraseñas que hoy requieren siglos para quebrarse se puedan revelar en minutos). Del mismo modo, el desarrollo técnico hace que los mecanismos de anonimización de hoy puedan quedar obsoletos en un futuro no tan lejano. Por lo tanto, ni las barreras artificiales (anonimización), ni las naturales (tiempo y costes) parecen ser un criterio de exclusión que ofrezca certezas a largo plazo, aunque, evidentemente, constituyen una referencia válida a la hora de diseñar el tratamiento.

La advertencia del Tribunal Constitucional Federal Alemán en su sentencia de 1983 sobre la Ley del Censo se ha materializado con toda su fuerza. Hoy parece evidente que "ya no existe, bajo las condiciones del tratamiento automático de datos, ningún dato "sin interés"". El riesgo de reidentificación, las inferencias o los mecanismos de perfilado, combinados con el *big data* y el tratamiento algorítmico de la información, hacen de los modelos de protección una fortaleza necesitada de constante revisión. En este sentido, que el legislador europeo haya hecho de la proactividad el rasgo característico del sistema es todo un acierto, pues convierte en obligación jurídica lo que, inevitablemente, iba a ser una necesidad fáctica.

En la misma línea de adecuación a los retos de la era digital debe entenderse la jurisprudencia del TJUE que, con el asunto Nowak, parece remarcar la pertinencia de utilizar un concepto amplio de dato personal. Uno que incluya como criterios identificativos, además del contenido (reflejo de la realidad personal), la finalidad y los efectos. Esas dos variables adicionales amplían el abanico de situaciones a las que sería de aplicación la normativa de protección de datos. Ello es así, porque la conexión ya no se produciría, exclusivamente, debido al vínculo dato-persona, sino que también surgiría del tratamiento en que la información se utilizase. El contexto pasa a ser un criterio identificador más.

Sin embargo, el contexto, por su naturaleza adaptativa, permite, en una interpretación extensiva (acaso excesiva), justificar la aplicación de la normativa de protección de datos a cualquier tratamiento en el que se constate que esa operación tiene consecuencias para una persona determinada, con independencia de cómo se hubieran calificado a los datos utilizados (personales o no personales). De este modo, el carácter personal de la información ya no sería un *a priori* a constatar, sino una posibilidad a verificar en cada tratamiento concreto. Con todo, esta interpretación no deja de ser una mera elucubración, pues, a día de hoy, el RGPD excluye de su ámbito de aplicación los datos anónimos (Considerando 26), por lo que, el criterio interpretativo amplificado siempre tendría por límite a ese tipo de informaciones.

Ampliar las posibilidades de identificación dota de mayor flexibilidad al concepto dato personal y, sobre todo, permite ofrecer protección a un número más amplio de situaciones en las que el tratamiento de datos podría llegar a afectar a una persona. No obstante, esa extensión tiene como contrapartida un debilitamiento de la seguridad jurídica, pues la normativa a aplicar ya no vendrá determinada, en exclusiva, por criterios objetivos, sino que dependerá de la realidad específica en que operen las variables a considerar. Sin embargo, la pérdida de certeza parece un coste asumible, si con ello se cuenta con mejores instrumentos para afrontar un escenario tan complejo y cambiante como el actual.

Si aceptamos la idea de que todo dato es un dato personal, propuestas como la realizada por Purtova[6] cobran pleno sentido y deberían ser tomadas en consideración. Para esta autora, habría que abandonar el uso formal del concepto dato personal y articular un modelo de protección en el que las medidas se adoptasen en función de la finalidad del tratamiento y, sobre todo, en los efectos y riesgos que pudiera tener para las personas. Se trataría de un sistema escalable, en el que las consecuencias serían el elemento determinante a la hora de fijar las obligaciones y exigencias para los operadores de datos. La lógica es evidente, a mayor intensidad en la afectación o a mayor riesgo, medidas más restrictivas. En última instancia, se trataría de evaluar las características de la operación que se quiere efectuar. En ese escenario, la naturaleza de la información, esto es, el grado de conexión entre el individuo y la información, sería una variable a considerar, pero no la única, ni el criterio de inclusión/exclusión. Una propuesta de este cariz requiere dar una vuelta de tuerca más al modelo de protección, ya que implica cambiar el centro de imputación del derecho, para transitar del dato personal al tratamiento personal.

Aunque, con la regulación actual del RGPD, la propuesta de Purtova no es viable, considero que no está tan lejos el momento en que una conceptualización así deba ser asumida. La apuesta por la proactividad y la atención al riesgo que inspira el RGPD está generando el sustrato y cultura jurídica adecuados para que, cuando la fuerza de lo fáctico haga que sea prácticamente indiferente la naturaleza inicial de la información, estemos en condiciones de aceptar como natural el modelo que Purtova plantea como ideal.

VIII. UN FUTURO DESAFIANTE

Los ingenios tecnológicos que se han ido gestando en las últimas décadas no solo han afectado a sectores concretos, sino que han ido modulando a la sociedad. Estamos inmersos en una revolución, un auténtico cambio de era alimentado por un sinfín de innovaciones constantes. La velocidad con la que se producen

6. PURTOVA, N. N., "The law of everything. Broad concept of personal data and future of EU data protection law", Law, Innovation and Technology, vol. 10, nº 1, 2018, pp. 40-81.

las transformaciones, la imposibilidad de asimilarlas y, consecuentemente, de integrarlas en las lógicas y dinámicas preexistentes, hacen de estos unos tiempos inciertos. La forma de vivir y relacionarse en sociedad e, incluso, el modo en que se organiza y controla el poder está mutando ante nuestros ojos. El foro público es, cada vez más, un foro digital.

La profundidad del cambio social y político es una incógnita por despejar, se desconoce lo que aguarda en los abismos más profundos de la era digital, pero ya tenemos algunos atisbos, como el poder cuasi omnímodo de las compañías transnacionales, esenciales para hacer girar el mundo virtual, el decisionismo de la IA o la dilución de la idea de comunidad. Al alterarse la forma de relacionarnos, también lo hacen los pilares sobre los que se asientan las democracias liberales: los derechos, el pueblo como sujeto político o la separación e independencia de los poderes se tambalean.

Garantizar los derechos y libertades, evitar que la revolución técnica los arrase por completo, constituye uno de los grandes desafíos de nuestro tiempo. En este escenario, el derecho a la protección de datos es una pieza crucial, no solo por ser el instrumento mediante el que asegurar un uso jurídicamente aceptable de una materia prima esencial para el desarrollo digital, sino, sobre todo, por lo que puede aprenderse de su evolución histórica y constante perfeccionamiento y adaptación a las creaciones y metamorfosis que la tecnología genera. En efecto, aunque se trata de un derecho que se aplica a cualquier tratamiento de datos personales, es en los automatizados donde despliega todo su potencial. En este sentido, la principal lección que puede extraerse del proceso de decantación del derecho a la protección de datos es que lo fundamental es identificar la finalidad que justifica la existencia del derecho a proteger, así como el bien jurídico que efectivamente se pretende salvaguardar. Si las bases están claras, el modo de cumplirlas puede variar, siendo posible realizar ajustes en función del contexto sobre el que vaya a desplegarse.

Dado el dinamismo que caracteriza a la realidad actual, la legislación parece condenada a abrazar el cambio como algo natural, incluso necesario. No obstante, la seguridad jurídica demanda de cierto grado de predictibilidad y certeza, además, resulta técnicamente imposible estar modificando constantemente la normativa (y aunque lo fuese no sería deseable). Por consiguiente, parece razonable adoptar políticas legislativas capaces de responder a diferentes escenarios sin perder su esencia. Los principios generales deben tener un papel más protagónico, los mecanismos de respuesta han de ser flexibles y la anticipación y prevención de riesgos han de asumirse como una constante transversal a cualquier regulación del espacio virtual. Solo así se podrá evitar la obsolescencia cuasi-inmediata de los mecanismos destinados a salvaguardar los derechos y libertades.

En la medida en que el cambio es inherente a la condición humana, el Derecho debe valerse de aquellos instrumentos que le permitan adaptarse a la condición evolutiva de la sociedad. En caso contrario, será incapaz de llevar a efecto su

función racionalizadora de la convivencia en comunidad y, por paradójico que pueda resultar, el desarrollo técnico terminará comportando la involución de la persona como ser social, así como la pérdida de aquello que nos hace humanos. En el Derecho está el remedio para evitarlo, usémoslo con inteligencia (humana).