IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

ARTÍCULO

Límites y garantías constitucionales frente a la identificación biométrica

Pere Simón Castellano
Universidad Internacional de la Rioja

Xavi Dorado Ferrer
Escuela de Prevención y Seguridad Integral (Fundació Universitat Autònoma de Barcelona)

Fecha de presentación: septiembre de 2021
Fecha de aceptación: diciembre de 2021
Fecha de publicación: marzo de 2022

Resumen

El presente artículo examina los límites y garantías constitucionales frente al uso de técnicas de identificación biométrica a la luz del procedimiento sancionador PS/00120/2021 instruido por la AEPD y resuelto en la primavera de 2021. Los datos biométricos, siguiendo el RGPD, son aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características de una persona física, que permiten confirmar la identificación única o unívoca de esta, como patrones biométricos faciales en el supuesto que nos ocupa. Al respecto, existe mucha confusión, y la propia AEPD ha reconocido que se han extendido una serie de equívocos con relación a esta tecnología (huellas dactilares o mediciones faciales) para fines de identificación y autenticación. En este trabajo se analiza el concepto jurídico indeterminado de «interés público esencial», de acuerdo con la jurisprudencia, como excepción a la prohibición general de tratamiento de datos biométricos *ex* artículo 9.2.g) RGPD. De modo más específico, se aborda la problemática desde una triple perspectiva: desde el punto de vista del sujeto, especialmente en relación con el responsable del tratamiento (con mención especial al supuesto en el que este no sea un organismo público); desde el punto de vista formal, se examinan los límites relativos a la reserva de ley; y, por último, desde el punto de vista sustantivo, se estudian los límites materiales referentes al principio de proporcionalidad y al contenido mínimo del derecho fundamental a la protección de datos personales.

Palabras clave

datos biométricos; reconocimiento facial; RGPD; interés público; protección de datos personales

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Constitutional limits and guarantees with biometric identification

Abstract

This article examines the constitutional limits and guarantees with the use of biometric identification techniques in the light of sanction PS/00120/2021 instructed by the AEPD and passed in Spring 2021. Biometric data, according to the GDPR, are those personal data obtained via a specific technical treatment, relative to the characteristics of a physical person, which allow for the confirmation of the unique or unambiguous identification of said person, such as biometric facial patterns as the case may be. There is much confusion with regard to this, and the AEPD itself has acknowledged that there have been a series of errors in relation to this technology (fingerprints or facial recognition) for the purposes of identification and authentication. For this task, the indeterminate legal concept of "essential public interest" is analyzed in accordance with jurisprudence, as an exception to the general prohibition of the treatment of biometric data ex article 9.2.g) GDPR. More specifically, the problem is approached from a triple perspective: from the point of view of the subject, especially with relation to that responsible for treatment (with special mention of the event that this is not a public organization), from a formal point of view, the limits relating to legal discretion, and finally from a substantive point of view, the material limits pertaining to the principle of proportionality and the minimum content of the fundamental right to the protection of personal data are studied.

Keywords

biometric data; facial recognition; GDPR; public interest; personal data protection

1. Procedimiento sancionador por tratamiento de datos biométricos «de uno a varios»

1.1. Antecedentes, intervención previa de órganos judiciales e infracciones impuestas a Mercadona S. A.

El procedimiento sancionador PS/00120/2021, instruido por la Agencia Española de Protección de Datos (en adelante, AEPD), cuya resolución se publicó en la primavera de 2021, abordó la problemática en torno a la implementación de un sistema de reconocimiento facial en algunos de sus establecimientos, a modo de prueba piloto, con el objeto de impedir la entrada a aquellas personas que, previamente, habían sido condenadas en sede penal por hurto o robo en relación con hechos acaecidos en sus propios establecimientos.

Según hace constar la AEPD en la resolución, Mercadona puso en marcha esta prueba piloto sin realizar la consulta previa a la que hace referencia el artículo 36 del RGPD, puesto que solicitó la medida de seguridad en el proceso penal sin haber realizado la evaluación de impacto de protección de datos[1] (preceptiva en este supuesto según dispone el art. 35.1 del RGPD).

A su vez, cabe tener presente que la Audiencia Provincial de Barcelona, previamente y mediante auto,[2] había desestimado el recurso de apelación interpuesto por Mercadona contra el auto dictado por el juzgado *a quo* –más concretamente, el Juzgado de lo Penal n.º 24 de Barcelona–, por el que se denegó la autorización para la utilización de medios automatizados de captación de datos biométricos de los penados.

Sin embargo, la mercantil entendía, contra el criterio de los tribunales, que su actuación estaba amparada por el interés público, en la medida que el cumplimiento de las sentencias y las órdenes de alejamiento incursiona bajo el paraguas del artículo 118 de la CE, de acuerdo con el cual todos estamos obligados a prestar colaboración en la ejecución de las resoluciones judiciales. Sobre esta cuestión volveremos *infra*, en el epígrafe 2.2 del presente trabajo.

En todo caso, Mercadona S. A. es sancionada por varias infracciones contempladas en los artículos 83.4a, 83.5a y 83.5b del RGPD, que se concretan en la vulneración del principio de licitud del tratamiento; tratamiento de categorías especiales de datos personales sin concurrencia de circunstancias que levanten la prohibición; conculcación del derecho a la transparencia e información; vulneración del principio de minimización de datos; no aplicación del principio de protección de datos desde el diseño, y, por último, falta de aplicación de la evaluación de impacto relativa a la protección de datos y consulta previa.

Se trata de un conglomerado de razones e infracciones, si bien el presente artículo se centrará esencialmente en la falta de licitud, por improcedencia de invocar el interés público por una mercantil, en relación con los datos biométricos, así como el principio de proporcionalidad y la minimización de datos. Dejamos así fuera del análisis el resto de las infracciones, como las relativas a los derechos de los interesados en materia de transparencia e información, la evaluación de impacto o el principio de protección de datos por defecto.

Sea como fuere, antes de entrar en las cuestiones jurídicas de fondo, es preciso determinar algunos conceptos de orden técnico para una cabal comprensión del objeto de estudio que nos ocupa.

1.2. Datos biométricos «de uno a varios»

Entendemos por datos biométricos, siguiendo el artículo 4.14 del RGPD, aquellos 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».

En este sentido, los dispositivos de captura de imágenes, en concreto aquellos que permiten el reconocimiento facial utilizando técnicas algorítmicas para procesar una

1. Procedimiento sancionador PS/00120/2021, págs. 63-64.
2. Auto de la Audiencia Provincial de Barcelona de 11/02/2021, n.º de recurso 840/2020, y n.º de resolución 72/2021 (ECLI:ES:APB:2021:1448A).

serie de patrones captados por la cámara, contrastándolos con una base de datos, deben ser catalogados bajo el tratamiento específico al que hace referencia el RGPD en el artículo 9.1.

Además, como señala la propia AEPD,[3] debe distinguirse este tipo de técnicas de la videovigilancia en general, pues esta última, si bien también realiza un tratamiento de datos personales, no llega a procesar la información contra una base de datos previa que permita o confirme la identificación de personas, en los términos del precepto citado.

Adicionalmente, y siguiendo de nuevo a la AEPD,[4] cabe señalar que este proceso, denominado «de uno a varios» desde un punto de vista técnico, es de vital importancia en el sentido de que conlleva un tratamiento de datos de categoría especial, mientras que en aquellos procesos «uno a uno», esto es, en los que tienen como objeto la identificación del sujeto sin contrastarlo con una base de datos amplia (verificación o autentificación), no implicarían necesariamente supuestos de tratamiento de datos sensibles.

La cuestión no es trivial o baladí porque, precisamente, en ciencia de datos esta terminología «de uno a varios» se utiliza cuando se estudian las relaciones entre tablas en lenguaje estructurado, es decir, aquellos procesos para encadenar diferentes tablas o bases de datos y, por ende, lo que permite la identificación de la persona física en los términos del artículo 4.1 del RGPD.

Así pues, y en consonancia con el grupo del artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, tenemos tres escenarios diferentes que cabe distinguir: 1) técnicas de reconocimiento facial de uno a varios (identificación biométrica); 2) procesamiento de datos biométricos mediante reconocimiento facial de uno a uno (verificación-autenticación), 3) y videovigilancia sin cotejo con una base de datos adicional.

Otras clasificaciones de interés, siguiendo la doctrina (Romeo Casabona, 2021, pág. 711), serían aquellas que atienden al carácter estático o dinámico de la información, según revelen propiedades anatómicas con cierta permanencia en el tiempo, o bien aquellas relativas al comportamiento; o según su recurrencia u objetividad, considerando si son universales, individualizadoras, irrepetibles, etc.

En el caso analizado en el presente artículo, estaríamos ante datos biométricos estáticos, referentes a las propiedades fisionómicas y universales, considerando que se dan en todos los seres humanos, si bien el algoritmo opera buscando caracteres individualizados o irrepetibles, que son los que finalmente le llevan a la identificación de la persona física informada en la base de datos.

A este respecto, conviene tener presentes las alertas y los dilemas planteados en el informe de la AEPD intitulado «catorce equívocos con relación a la autentificación y a la autentificación biométrica», entre los que destaca el supuesto carácter infalible de estas técnicas que, al fin y al cabo, operan con plantillas, por lo que los patrones con los que trabaja no responden necesariamente al carácter irrepetible de estos. Este punto es de especial relevancia, ya que el algoritmo también puede equivocarse o errar, como de hecho ya ha ocurrido en Estado Unidos en supuestos de detenciones de sospechosos e investigados que en realidad eran inocentes (caso Robert Julian-Borchak Williams).[5]

Tampoco hay que perder de vista, como ha señalado la doctrina (Cotino Hueso, 2020), el hecho de que la aplicación de la IA respecto a humanos implica la entrada en juego del derecho a oponerse a las decisiones automati-

3. Procedimiento sancionador PS/00120/2021, pág. 28.
4. Ibíd., pág. 39.
5. En este caso, en el que se produjo una identificación errónea de un sospechoso por hurto, la doctrina (Rowe, 2020, pág. 18) ha señalado que la propia empresa desarrolladora del *software* (Data Works Plus) indicó que el programa no había sido suficientemente testeado. Sin embargo, sorprende que en el ámbito policial y penal se usen algoritmos diseñados por empresas privadas que, escudándose en la propiedad intelectual, no siempre se muestran colaboradoras para compartir el código fuente. En este sentido, y sobre los confines perimetrales del derecho a la tutela judicial efectiva y del derecho de defensa, véase la feroz crítica formulada por Simón Castellano (2021b, pág. 183 y 2021c). La doctrina nacional especializada se ha manifestado en la misma dirección cuando los algoritmos se aplican en el ámbito penitenciario (Martínez Garay, 2018 y 2019, págs. 149 y ss.).

zadas, tal como establece el artículo 22 del RGPD. Y si bien la norma prevé tres excepciones (relación contractual, habilitación legal y consentimiento), ninguna de estas se dio en el caso Mercadona.

El interesado, en este caso el identificado por el sistema biométrico, debería entonces poder impugnar la decisión, o, en términos de la doctrina administrativista, exigir el «derecho de audiencia o la garantía del principio de imparcialidad» (Cerrillo i Martínez, 2020, pág. 29); pero considerando que el uso estaba previsto para que se personaran las autoridades de orden público, ¿ante quién debería impugnarse la decisión?

El responsable del tratamiento es Mercadona, pero la «ejecución» de la identificación estaba reservada a la policía. Un ejemplo más de la inseguridad jurídica a las que puede conducir la «bienintencionada» colaboración del sector privado en las potestades de los poderes públicos, máxime cuando se trata de ámbitos materiales con regímenes jurídicos distintos o, como hemos señalado en otros foros respecto a la dificultad de aplicar normas en el campo de la IA, «un marco jurídico complejo atomizado en distintas directivas y reglamentos, más las normativas nacionales de referencia» (Simón Castellano, 2021c).

En síntesis, las técnicas de reconocimiento facial mediante cámaras como las que instaló Mercadona constituían técnicas de identificación biométrica, respecto al tratamiento vinculado a la base de datos que almacenaba información sobre las personas condenadas y con órdenes de alejamiento del establecimiento. La cuestión es si también caen bajo el concepto de tratamiento de datos personales la información del resto de los clientes que, simplemente, iban a hacer la compra.

1.3. El tratamiento de datos personales concurre en supuestos de procesos cortos en el tiempo

No acaba aquí la problemática en torno al tratamiento de datos mediante técnicas biométricas, pues los procesamientos cortos de menos de un segundo sobre personas que no correspondían con ninguno de esos registros también deben considerarse tratamiento de datos personales, pues, pese a que el circuito de identificación no llegara a encontrar un registro coincidente, técnicamente el proceso era el mismo (cotejo de uno a varios).

Este punto es relevante, pues, aunque no culminaba la cadena identificación, tomaba como objeto datos en masa de personas físicas ajenas a los procesos penales de los sujetos que constaban en la base de datos, incluyendo niños u otras personas que merecen especial tutela de acuerdo con el RGPD.

Por consiguiente, en la aplicación de este tipo de tecnologías de identificación biométrica de uno a varios, deben tenerse en cuenta los bienes jurídicos en juego no solo de los sujetos que constan en la base de datos, sino los de todas las personas físicas que se toman como muestra.

En este último escenario, además, puede darse el caso en que el responsable del tratamiento obvie este punto, por lo que ni siquiera se pregunte por la base habilitante en cuestión referida a la muestra, como de hecho ocurrió en el caso Mercadona. Por ello, si este tipo de tecnologías van a implementarse en el futuro con las garantías adecuadas que se desarrollarán a continuación, se ha de tener presente la base habilitante para el tratamiento de, al menos, dos categorías de interesados distintas: *a*) los sujetos cuya plantilla de datos biométricos se encuentra en la base de datos; *b*) la muestra general de personas físicas que arroja resultados no coincidentes. Dejamos fuera del objeto de este artículo, deliberadamente, un tercer sector involucrado, y que sí trata el procedimiento sancionador, como lo es el de los trabajadores de la empresa que constituyen una categoría de interesados por excelencia.

2. Límites y garantías constitucionales

En este apartado abordamos los límites y las garantías constitucionales desde la triple perspectiva del sujeto, el principio de reserva de ley y las garantías materiales como el principio de proporcionalidad y el contenido mínimo de los derechos.

2.1. Límites subjetivos. Responsable del tratamiento e interés público

En esta ocasión estamos ante un supuesto en el que, paradójicamente, el interés público se esgrime por parte de una mercantil para justificar el tratamiento masivo de datos personales y, en concreto, datos biométricos.

Se trata de una discusión que data de antiguo. De hecho, reaparece en escena la problemática en torno al concepto jurídico indeterminado de «interés público» como excepción a la prohibición genérica de tratamiento de datos sensibles prevista en el artículo 9.2.g) del RGPD.

No es, desde luego, la primera vez que este concepto irrumpe en el debate doctrinal y jurisprudencial, pues el máximo intérprete constitucional[6] ya reprochó en 2019 –en este caso, al legislador– la aplicación arbitraria de la noción de «interés público» como una suerte de comodín[7] que, al ser invocado, pudiera hacer decaer el derecho fundamental a la protección de datos en lo concerniente a la información referente a la ideología de los ciudadanos.

El interés público informativo[8] solo concurre cuando la información que se comunica es relevante para la comunidad, lo cual justifica la exigencia de que se asuman perturbaciones o molestias ocasionadas por la difusión de una determinada noticia. Se trata de un concepto jurídico indeterminado, cuya concurrencia pasa por determinar si nos encontramos ante unos hechos o circunstancias susceptibles de afectar al conjunto de los ciudadanos, que como bien señala López Calera (2010) debe ser «diferenciado de la idea metafísica e iusnaturalista de bien común, ha de ser ante todo un valor democrático, en cuanto a que su definición debe estar en manos de poderes democráticamente legitimados y su realización ha de implicar la protección y la realización de un mayor número de intereses particulares».[9] Con todo, nunca debe confundirse el interés público informativo con el interés del público, más cercano a la satisfacción de la curiosidad humana o ajena.

En esta línea, entendemos que la determinación de lo que deba ser «interés público» debe sustraerse de ciertas tesis esencialistas o rousseaunianas de la noción de opinión pública o «auténtica voluntad popular» defendidas por parte de la doctrina (García Sanz, 2019), ya que ello puede justificar la configuración de bases de datos ideológicas con el ánimo de descubrir una supuesta verdad oculta tras el ruido de la pluralidad manifestada en los entornos *online*.

En esta ocasión, y a diferencia de la STC 76/2019, comentada con anterioridad, el reproche no tiene como autor

6. Véase FJ 6 de la STC 76/2019, de 22 de mayo (ECLI:ES:TC:2019:76). En la fundamentación, se interpretó de forma tuitiva aceptando parcialmente las alegaciones del defensor del pueblo y la iniciativa de los profesionales Borja Adsuara, José Luis Piñar, Jorge García, Elena Gil, Víctor Domingo, Miguel Pérez Subías, Virginia Pérez Alonso y Rodolfo Tesone, cuyo trabajo incluía un conjunto de artículos en prensa y una campaña en redes sociales, y que posteriormente fueron premiados por la AEPD (Premios de Protección de Datos 2019). Parte de la doctrina (voces autorizadas en prensa como las de Artemi Rallo Lombarte y Ricard Martínez Martínez, que no necesitan presentación alguna ni referencia por haberlas realizado en la tribuna pública) empero no consideraba necesaria tal declaración de inconstitucionalidad, ante una eventual interpretación conforme tanto por parte de la jurisprudencia ordinaria como por parte de las todopoderosas autoridades de control en materia de protección de datos. A ojos de quienes suscriben estas líneas, sorprende la necesidad y la celeridad de la reacción frente a lo que preveía la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales en virtud de la cual se introducía el artículo 58 bis de la Ley Orgánica 5/1985, del 19 de junio, del régimen electoral general, cuando, por el contrario, la LOPD de 1999, que recogía la obligatoriedad del consentimiento como base de legitimación salvo contadas excepciones en el artículo 6 de la extinta ley, permitió durante prácticamente dos décadas la inusual y aberrante excepción que permitía cualquier tratamiento en caso de fuentes accesibles al público o en caso de interés público en un sentido amplísimo, incluyendo cualquier tratamiento de datos en el ejercicio de las funciones propias de las administraciones públicas, esto es, en el ámbito de sus competencias; también la autorización de las transferencias internacionales de datos en el artículo 34.h), y, finalmente, incluyendo un auténtico cajón de sastre en el artículo 24. Ante semejante despropósito, y ante las constantes llamadas de atención del TJUE por lo que se refiere a una adecuación no conforme de la Directiva europea de 1995, fruto de una mala transposición, por decirlo de alguna manera, ahora sorprende la rapidez para eliminar y expulsar del ordenamiento jurídico el mencionado artículo, al que se podía haber vaciado de efectos prácticos reales con una interpretación sistemática y coherente con el resto de los derechos fundamentales que recoge la carta magna, en general, y la normativa de protección de datos, en particular. Véase al respecto la sentencia del Tribunal Supremo (sala tercera, de lo Contencioso-Administrativo), de 8 de febrero de 2012 (ECLI:ES:TS:2012:429), que en sintonía con todo lo expuesto derogó el artículo 10.2.b) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobó el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD). Véase también la cuestión prejudicial resuelta por el Tribunal de Justicia de la Unión Europea en sentencia dictada en los asuntos C-468/10 y C-469/10.
7. Tampoco el interés legítimo, cuya tentación en este caso por parte de las empresas privadas es mucho mayor. Véase al respecto Gil González (2021).
8. El Tribunal Supremo ha justificado el ejercicio de la crítica a las resoluciones judiciales atendiendo al interés público que resulta siempre inherente al mero ejercicio de la función jurisdiccional. Véase por todas la reciente STS 92/2018, de 19 de febrero. Sobre la publicidad del proceso y los efectos que proyectan los debates en redes sociales, véanse Simón Castellano (2021a) y Guzmán Fluja (2018).
9. López Calera (2010, pág. 144).

el Tribunal Constitucional, sino la AEPD; y no tiene como destinatario el legislador, sino una mercantil. En concreto, el procedimiento sancionador analiza el caso en el que una entidad de derecho privado esgrime el concepto de interés público para justificar la base habilitante que operaría como excepción al tratamiento de datos personales sensibles, en concreto, a los datos biométricos de reconocimiento facial (art. 9.1 del RGPD).

Cierto es que el interés público ha sido interpretado expresamente por parte de la AEPD como la base de legitimación para fines de videovigilancia. Indica la autoridad competente[10] que, puesto que la finalidad de la videovigilancia consiste en garantizar la seguridad de personas, bienes e instalaciones, el interés público legitima dicho tratamiento. Asimismo, el considerando 45 del RGPD contempla que, si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público, este tratamiento debe tener una base en el derecho de la Unión o de los Estados miembros.

Por si la interpretación, como se argumentará más adelante, ya nos parece aberrante de entrada, la AEPD añade que existirá un interés público de los particulares en la captación de imágenes mediante cámaras de videovigilancia para garantizar la seguridad de personas o instalaciones en los espacios de su propiedad, como puede ser su domicilio o su plaza de garaje.

Resulta difícil e imposible de comprender por qué la AEPD insiste en recurrir a esta base de legitimación para los sistemas de videovigilancia cuyos responsables del tratamiento son empresas privadas, cuando es esta misma autoridad de control la que siempre ha vinculado el interés público a las administraciones públicas y organismos, descartando la posibilidad de que estos recurran al interés legítimo. Una contradicción interna insalvable que, en cambio, ha sorteado con brillantez la Information Commissioner's Office (en adelante, ICO) del Reino Unido, que siempre ha defendido que en ciertas instancias las autoridades deben ser capaces de emplear la base de legitimación del interés legítimo. Lo único que no tiene sentido, prosigue la ICO, es que se emplee el interés legítimo como base de legitimación si el tratamiento de datos está inextricablemente vinculado a tareas que desempeña en su función de autoridad.[11]

Es aberrante, como decíamos, sostener que un particular o una empresa está tratando datos personales con fines de videovigilancia sobre la base de un interés público cuando lo que hace es, en realidad, garantizar la seguridad de las personas o de los bienes e instalaciones de su propiedad. Es evidente que no existe un interés público en garantizar la seguridad de un parquin de una casa privada, como sostiene la AEPD. Tampoco existe interés público alguno en que un negocio dedicado a la comercialización y venta de teléfonos móviles controle mediante videovigilancia sus locales. Lo que hace, en realidad, esa persona o esa organización, no es otra cosa que cubrir un interés legítimo, el relativo a garantizar la seguridad de las personas, bienes e instalaciones que son de su propiedad y sobre las que recae una indubitada posición de garante, que les podría hacer responsables civiles y, también penales, sobre la base de la responsabilidad prevista expresamente en el Código Penal, ex artículo 120.3.

Una responsabilidad, también la penal, que nace en aquel viejo aforismo que nos recuerda que *qui sentit commodum, debet sentire incommodum*. El fundamento de la teoría del riesgo y la obligación de ser responsable también cuando aquello que proyecta el negocio (ámbito empresarial o privado) o la mera propiedad (ámbito particular o personal, en el que incluso podría explorarse de nuevo aquello de la exención doméstica, ahora previsto *ex* art. 2.2 del RGPD) no son precisamente ingresos o beneficios, sino problemas derivados de la comisión de un delito.

Hechas estas observaciones, cabe preguntarse por qué Mercadona no recurrió a la base habilitante del interés legítimo (art. 6.1.f del RGPD), saltando directamente al interés público, si bien el primero requiere que sobre los intereses del responsable del tratamiento no prevalezcan los intereses o los derechos y libertades fundamentales del interesado, lo que, a la luz del auto citado con anterio-

10. Véase la guía de la AEPD sobre el uso de videocámaras para seguridad y otras finalidades (2018).
11. La guía de la ICO es bastante completa sobre esta cuestión, y sigue un formato o modelo de pregunta y respuesta que, además, reúne una coherencia interna que es de agradecer [en línea] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/ [Fecha de consulta: 9 de septiembre de 2021].

ridad, debía descartarse igualmente. Con todo, parece un argumento mejor defendible que la invocación del interés público en el contexto del uso de datos biométricos en el ámbito de los intereses privados. Quizás, la razón de fondo para esa confusión por parte de la defensa jurídica de la mercantil Mercadona tiene su origen en la contradictoria e insostenible, cuando no aporética «doctrina»[12] de la AEPD, que insiste en vincular y constreñir los tratamientos basados en sistemas de videovigilancia al interés público como base de legitimación.

Sin embargo, sorprende que una entidad de derecho privado se arrogue la potestad de atribuirse esta misión, pues el RGPD, al referirse al interés público como base habilitante, lo hace en términos de poderes conferidos al responsable del tratamiento (art. 6.1e), por lo que debería existir una previsión legal específica en tanto al objeto (interés público) y sujeto (qué organismo tiene la potestad para actuar conforme a dicho interés).

No caben, pues, habilitaciones legales amparadas en el interés público, si el responsable del tratamiento no está específicamente habilitado por una norma de rango de ley, lo que nos lleva a la siguiente cuestión.

2.2. Límites formales. Interés público y reserva de ley

En lo concerniente al interés público desde un punto de vista formal, entendemos por uso público de bases de datos aquel que está destinado a un fin de interés general previsto en la ley. Por lo tanto, no cualquier utilización de la información merecerá este calificativo, sino aquella que obedece a una necesidad, utilidad, beneficio o provecho de la sociedad y, además, esté contemplado en una norma con rango de ley.

En este sentido, la reserva de ley está contemplada en el artículo 8 de la LOPDGDD, que entiende satisfecha esta condición cuando se dé cumplimiento a una misión de interés público y el uso de los datos derive de una competencia atribuida por una norma con rango de ley.

Así pues, uso público es aquel que responde al interés general, público o social que el legislador contempla en la ley. Estos conceptos aparecen en la Constitución de 1978 en varios preceptos: 76.1 y 124.1 (interés público), 33.3 y 124 (interés social), y 103.1 (intereses generales), en este último caso vinculado a la Administración pública.

Por su parte, la ley también hace un uso recurrente de este concepto, por ejemplo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas a lo largo de su articulado en numerosas ocasiones.

Además, el RGPD utiliza este concepto jurídico, por ejemplo, en el considerando 46 cuando indica que, en relación con el tratamiento de datos: «pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano».

El problema es que a menudo la ley o los operadores jurídicos utilizan este concepto como motivo habilitador para que la Administración –o, en este caso, una empresa privada– actúe en un procedimiento, sin especificar, como sí hace el reglamento citado, a qué hace referencia. De este modo, podríamos encontrarnos ante un concepto jurídico indeterminado.

Esto ocurriría cuando la ley invoca el interés público, pero no especifica su contenido. En este caso, estamos ante actuaciones que la justicia puede controlar en virtud del artículo 106.2 de la Constitución, que habilita el poder judicial para controlar la legalidad de la actuación de las administraciones públicas; o bien el propio Tribunal Constitucional cuando sea la propia ley la que no concretice el concepto de interés público.

Por ello, la vaguedad de la noción de interés público también puede ser motivo de control de constitucionalidad. El ejemplo de la indeterminación de este concepto nos lo da la ya citada STC 76/2019, de 22 de mayo. Esta sentencia analizaba la constitucionalidad del apartado 1 del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado a esta por la disposición final tercera, apartado dos, de la LOPDGDD de 2018.

12. De nuevo, nos referimos a la guía de la AEPD sobre el uso de videocámaras para la seguridad y otras finalidades (2018).

En concreto, se trataba de dilucidar si, en el contexto de campañas electorales, el tratamiento de datos sensibles referentes a la ideología de las personas podría ser amparado por el ordenamiento jurídico, invocando únicamente el concepto de interés público.

En este caso, el Alto Tribunal arguyó que la disposición legal impugnada no identificaba en ningún momento ese interés público esencial, presuponiendo su existencia sin que se llegara a especificarla.[13] Así pues, la sentencia concluye que la legitimidad constitucional de la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado interés público, «pues en otro caso el legislador habría trasladado a los partidos políticos –a quienes la disposición impugnada habilita para recopilar datos personales relativos a las opiniones políticas de las personas en el marco de sus actividades electorales– el desempeño de una función que solo a él compete en materia de derechos fundamentales en virtud de la reserva de ley del art. 53.1 CE, esto es, establecer claramente sus límites y su regulación».[14]

Así pues, cuando el artículo 9.2.g del RGPD dispone que el tratamiento de datos sensibles puede ser lícito cuando sea necesario por razones de un interés público, añadiendo que debe ser proporcional al objetivo perseguido, así como respetar el contenido mínimo esencial del derecho a la protección de datos, se entiende que el legislador debe determinar cuál es este interés público, así como el régimen jurídico de tratamiento de dichos datos, de modo que se respete el núcleo del derecho fundamental a la protección de datos al que se refiere el precepto y la jurisprudencia del máximo intérprete de la Constitución.

En el supuesto que trata el procedimiento sancionador de la AEPD, se observa que no existe la habilitación legal prevista en la ley, de tal manera que un responsable del tratamiento en el ámbito privado pueda arrogarse potestades relacionadas con un interés público que, además, tampoco se especifica. Por ello, la AEPD señala acertadamente que no concurre esta base habilitante en el procesamiento de datos de reconocimiento facial, por mucho que se invoque de forma generalizada el interés público en virtud del artículo 118 de la CE y el obligado cumplimiento de las resoluciones.

En este sentido, la propuesta de reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante, propuesta de reglamento IA) y se modifican determinados actos legislativos de la Unión,[15] persigue disminuir la inseguridad jurídica y la falta de previsión legal en el uso de las técnicas de identificación biométrica en tiempo real.

De acuerdo con el citado borrador, respecto al uso de técnicas de reconocimiento facial en tiempo real, el artículo 5.1d establece una regla general prohibitiva que solo podrá ser levantada en los siguientes supuestos: *a*) la búsqueda selectiva de víctimas, incluidos menores desaparecidos; *b*) la prevención de una amenaza inminente para la integridad de las personas o de un atentado terrorista; y *c*) la detección, localización, identificación o enjuiciamiento de personas que han cometido o se sospecha que han cometido alguno de los delitos de entrega automática mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo.

Entre estos, se encuentran los robos organizados o a mano armada cuya pena máxima sea, al menos, de tres años, por lo que entendemos que, desde un punto de vista material, podría en el caso Mercadona,[16] con las debidas garantías en términos de poderes públicos eventualmente habilitados legalmente.

13. FJ 7 de la STC 76/2019, de 22 de mayo (ECLI:ES:TC:2019:76).
14. Ibíd. FJ 7.
15. Disponible en:
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206&from=EN
16. Los condenados (véase auto citado en la nota siete en el que se cita la sentencia del juzgado de lo penal n.º 28 de Barcelona) lo fueron como autores de un delito de robo con violencia en las personas (pena máxima de 5 años *ex* art. 242 del CP).

Por último, cabe señalar que el RGPD se refiere a un interés público «esencial»,[17] por lo que no cualquier interés público puede superponerse a los derechos fundamentales de los interesados, sino solo aquel que cumpliendo el principio de proporcionalidad y respetando las medidas necesarias en una sociedad democrática, en la terminología del TEDH, merezca una tutela especial que justifique la limitación de la protección de datos y de los bienes jurídicos reales (intimidad, privacidad, honor, etc.) que con peculiar construcción jurisprudencial[18] se tutelan de forma indirecta o refleja mediante la normativa de protección de datos personales.

2.3. Límites materiales. Principio de proporcionalidad y contenido mínimo

Llegados a este punto, analizamos los límites materiales que deben traerse a colación cuando se pretendan implementar técnicas de identificación biométrica, considerando que se hayan superado los filtros subjetivos y formales estudiados anteriormente.

En este sentido, de acuerdo con el principio de proporcionalidad en la consolidada jurisprudencia del Tribunal Constitucional (FJ 4, STC 207/1996, de 16 de diciembre), para dilucidar si una medida supera el juicio de proporcionalidad, debe realizarse un triple juicio: idoneidad, necesidad y proporcionalidad estricta. La idoneidad es simplemente la eficacia de la medida para conseguir el objetivo en cuestión, lo que no se cuestiona en el caso de las tecnologías de identificación facial.

No obstante, es más difícil, si no imposible en algunos casos, justificar su necesidad, esto es, la inexistencia de otros medios menos gravosos para obtener el mismo fin. En el caso objeto del procedimiento sancionador que nos ocupa, el uso de estas tecnologías no superaba este juicio, pues se pueden pensar cauces menos perjudiciales para los bienes jurídicos en juego (recordemos: tanto de las personas condenadas como de las personas que forman parte de la muestra total). El interés privado en juego, disfrazado de interés público, no puede prosperar para justificar el tratamiento masivo de datos sensibles.

Además, el juicio de proporcionalidad, en caso de haber llegado incólume a esta fase, aún debe justificar que el sacrificio de los bienes jurídicos de relevancia constitucional conlleve más ventajas que renuncias, lo que tampoco prospera cuando colisionan derechos fundamentales contra intereses privados, descartado el interés público. En esta línea, la propuesta de reglamento IA prevé en su artículo 5.2b que el uso de identificación biométrica a tiempo real, cuando no esté prohibido, deberá prever «las consecuencias que [...] el sistema tendría para los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias».

Un ejemplo de ello lo encontramos en el informe de la AEPD en materia de reconocimiento facial aplicado a las universidades *online* (*e-proctoring*) que rechazó que esta técnica, aplicada a los exámenes, superara el test de necesidad, por existir medios o vías menos gravosas (no estaría de más saber cuáles son esas alternativas menos gravosas que permitían a los estudiantes examinarse en medio de una crisis sanitaria galopante), y de proporcionalidad estricta, por derivarse mayores sacrificios que beneficios respecto a los bienes jurídicos en juego.[19]

17. Cabe señalar que añadir un concepto jurídico indeterminado como «esencial» a lo que ya de por sí es un concepto jurídico indeterminado no ayuda, desde el punto de vista hermenéutico, a aclarar sus límites materiales. En este sentido, la extensión de lo que deba ser «esencial» corre los mismos peligros de incurrir en *ultra vires* y subjetividad en su aplicación por parte de los poderes públicos, si no se ofrece una definición más próxima a la taxatividad legal que a los conceptos abiertos de rango constitucional. Sin ir muy lejos, ya sabemos cómo han acabado sus homólogos «extraordinaria y urgente necesidad» a la luz del uso y abuso del Decreto Ley en los últimos años, hasta sumar dos tercios de la producción legislativa.
18. En este sentido, el máximo intérprete constitucional ha señalado: «De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal». STC 292/2000, de 30 de noviembre, FJ 6 (ECLI:ES:TC:2000:292):
19. Agencia Española de Protección de Datos. Informe sobre reconocimiento facial en los exámenes. N/REF: 0036/2020, pág. 16. Véase también la resolución de advertencia n.º: E/05454/2021 de la AEPD dirigida a la Universidad Internacional de La Rioja (UNIR), de acuerdo con la cual «existe una diferencia entre la mera identificación por cámara para acceder al examen, la cual es posible y legal, y la parametrización y control constante con perfilamiento biométrico, la cual no puede implementarse sin una ley que a día de hoy no existe» (pág.1).

En este orden de consideraciones, sorprende que una autoridad administrativa, pese a su independencia según dispone el artículo 44.1 de la LOPDGDD, entre de modo tan frecuente a aplicar el principio de proporcionalidad y a ponderar derechos fundamentales,[20] pues si nos ceñimos a sus potestades y funciones de acuerdo con el título VII de la LOPDGDD, la ponderación de derechos fundamentales desborda su régimen jurídico, máxime cuando están en juego procedimientos sancionadores, y se entra en un campo que debería estar reservado al poder judicial.

A la hora de utilizar dispositivos de identificación facial en espacios públicos o en recintos comerciales, debe tenerse presente que el bien jurídico protegido por el artículo 8 de la CEDH y el artículo 18.4 de la CE no ha desaparecido, por lo que la justificación de su intromisión debería resolverse con un escrupuloso juicio de proporcionalidad y previamente considerados los límites y las garantías constitucionales a los que hemos hecho referencia en el presente artículo.

Para finalizar, conviene tener presente que, como señala acertadamente el informe *Regulating facial Recognition in the EU* del Servicio de Estudios del Parlamento Europeo, la generalización de las técnicas de reconocimiento facial puede tener un impacto en derechos fundamentales, tales como la libertad de religión, opinión, expresión, reunión y asociación,[21] entre otros, puesto que si los espacios públicos devienen espacios hipercontrolados, la eficacia de tales derechos se verá mermada, por lo que la doctrina del TEDH que extiende la intimidad de los ciudadanos a los espacios públicos será de vital importancia en los años venideros.

Tal juicio se manifiesta desde el punto de vista del sujeto –el responsable del tratamiento debe estar investido expresamente de los poderes públicos en este ámbito–, desde la perspectiva formal –tanto estos poderes como el interés público invocado debe estar definido de forma taxativa en una norma con rango de ley– y desde un punto de vista del objeto o material, por lo que se somete dicho tratamiento a un juicio de proporcionalidad –idoneidad, necesidad y proporcionalidad estricta–, respetando el núcleo material del derecho fundamental en cuestión.

En todo caso, este tipo de juicios deben estar reservados al poder judicial. De un tiempo a esta parte, autoridades administrativas como la AEPD están asumiendo funciones de ponderación de derechos fundamentales que desbordan el ámbito de autoridad de control para el que fueron pensados. En ocasiones, los sancionados se sienten intimidados y prefieren finalizar el procedimiento por pago voluntario sin recabar la tutela jurisdiccional, que es donde deberían ventilarse los procesos en los que intervengan derechos fundamentales. Sin embargo, se trata de una arista que escapa al objeto de este trabajo por límites espaciales, por lo que deberá ser afrontada en futuros, a los que nos aventuramos a remitirnos y en los que nos referiremos a este paradigma bajo la voz de «los poderes salvajes de las autoridades de control».

Por último, cabría señalar que el interés legítimo es una base habilitante más adecuada que el interés público cuando el operador es un particular o empresa privada, pues la reserva de ley, de haberla, vinculará preferentemente este concepto a responsables del tratamiento investidos de poderes públicos.

Conclusiones

Los procesos de detección biométrica, en especial los de captación de imagen que operen con algoritmos de identificación de la identidad de personas físicas registradas en una base de datos, son tratamientos de datos personales de categoría especial, por lo que su uso en el futuro debe superar un exhaustivo juicio de constitucionalidad.

20. Véase pág. 48 y siguientes del procedimiento sancionador PS/00120/2021.
21. *Regulating facial Recognition in the EU*, 2021, pág. 8.

Referencias bibliográficas

AEPD (2021). Procedimiento Nº: PS/00120/2021.

AEPD (2020, junio). «Catorce equívocos con relación a la autentificación y a la autentificación biométrica».

AEPD (2020). «Informe sobre reconocimiento facial en los exámenes». N/REF: 0036/2020 [en línea]. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-informe-reconocimiento-facial-examenes

AEPD (2021). Advertencia Expediente Nº: E/05454/2021 de 27 de julio de 2021.

CERRILLO I MARTINEZ, A. (2020). «¿Son fiables las decisiones de las Administraciones públicas adoptadas por algoritmos?». En: *European review of digital administration & law*, vol. 1, núm. 1-2, págs. 18-36.

COTINO HUESO, L. (2020). «Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos». En: *IDP: Revista de Internet, Derecho y Política*. núm. 31 [en línea]. DOI: https://doi.org/10.7238/idp.v0i31.3244

DORADO FERRER, X. (2021). «Redes sociales, metadatos y derecho a la intimidad en los procedimientos tributarios». En: *Revista Quincena Fiscal*, núm. 12, págs. 91-103.

GARCIA SANZ, R. (2019). «Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público». En: *Revista de Estudios Políticos*, núm. 183, págs. 129-159 [en línea]. DOI: https://doi.org/10.18042/cepc/rep.183.05

GIL GONZÁLEZ, E. (2021). «El interés legítimo en el tratamiento de datos personales masivos». Tesis doctoral. Director: José Luis Piñar Mañas. Universidad San Pablo-CEU [en línea]. Disponible en: http://hdl.handle.net/10637/13021.

GUZMÁN FLUJA, V. C. (2018). «Juicios paralelos en las redes sociales y proceso penal». En: *IDP: Revista de Internet, Derecho y Política*, núm. 27, págs. 52-66 [en línea]. DOI: https://doi.org/10.7238/idp.v0i27.3148

LÓPEZ CALERA, N. (2010). «El interés público: entre la ideología y el Derecho». En: *Anales de la Cátedra Francisco Suárez*, núm. 44, págs. 123-148.

MARTÍNEZ GARAY, L. (2018). «Peligrosidad, algoritmos y due process: El caso State vs. Loomis». En: *Revista de Derecho Penal y Criminología*, núm. 20, págs. 485-502 [en línea]. DOI: https://doi.org/10.5944/rdpc.20.2018.26484

MARTÍNEZ GARAY, L. (2019). «La relación entre culpabilidad y peligrosidad». En: MARAVER GÓMEZ, M. y POZUELO ARQUIMBAU, L. (Coords.). *La culpabilidad*, págs. 115-200. Montevideo: B de F.

ROMEO CASABONA, C. (2021). «Datos biométricos (comentario al art. 4.14 RGPD)». En: TRONCOSO REIGADA, A. (Dir.). *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales*, págs. 709-712. Cizur Menor: Editorial Civitas (Thomson Reuters-Aranzadi).

ROWE, ELISABETH A. (2020). «Regulating Facial Recognition Technology in Private Sector». En: *Stanford Technology Law Review*, vol. 24, núm. 1, págs. 1-54.

SIMON CASTELLANO, P. (2021a). «Internet, redes sociales y juicios paralelos: un viejo conocido en un nuevo escenario». En: *Revista de Derecho Político*, núm. 1(110), págs. 185-228 [en línea]. DOI: https://doi.org/10.5944/rdp.110.2021.30332

SIMON CASTELLANO, P. (2021b). *Justicia Cautelar e Inteligencia Artificial: La Alternativa a Los Atávicos Heurísticos Judiciales*, 1.ª ed. [en línea]. Barcelona: J.M. Bosch. DOI: https://doi.org/10.2307/j.ctv1tqcxbh

SIMON CASTELLANO, P. (2021c). «Inteligencia artificial y administración de justicia: ¿Quo Vadis, justitia?». En: *IDP: Revista de Internet, Derecho y Política*, núm.33 [en línea]. DOI: https://doi.org/10.7238/idp.v0i33.373817

Cita recomendada

SIMÓN CASTELLANO, Pere; DORADO FERRER, Xavi (2022). «Límites y garantías constitucionales frente a la identificación biométrica». *IDP. Revista de Internet, Derecho y Política*, núm. 35. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i35.392324

Sobre los autores

Pere Simón Castellano
Universidad Internacional de la Rioja
pere.simon@unir.net

Profesor Titular (acreditación ANECA desde 2015) de Derecho Constitucional en en la Universidad Internacional de La Rioja UNIR. Docente en asignaturas de grado y posgrado en diferentes universidades (UNIR, Universidad de Girona, UOC O ESERP Business School, adscrita a la Universidad de Vic - Central de Cataluña). Secretario de la Junta de la Sección de Derecho de las TIC del Ilustre Colegio de Abogados de Barcelona. Premio de la Agencia Española de Protección de Datos (2011) y de la Agencia Vasca de Protección de Datos (2015). Investigador del grupo de investigación PENALCRIM de UNIR.

Xavi Dorado Ferrer
Escuela de Prevención y Seguridad Integral (Fundació Universitat Autònoma de Barcelona)
xavier.dorado@fuabformacio.cat

Coordinador de grado y formación continuada en la Escuela de Prevención y Seguridad Integral (Fundación Universidad Autónoma de Barcelona). Tutor del máster de Fiscalidad (Universitat Oberta de Catalunya). Miembro del grupo de investigación consolidado TaxBusiness- Fiscalidad, relaciones laborales y empresa. Premio Extraordinario de Licenciatura en Filosofía (Universidad Autónoma de Barcelona).