EL CRIMINALISTA DIGITAL
PAPELES DE CRIMINOLOGÍA - 2ª ÉPOCA

II Época, Número 9, 2021, pp. 20-37
ISSN 2340-6046

UTILIZACIÓN DEL SISTEMA DE RECONOCIMIENTO FACIAL PARA PRESERVAR LA SEGURIDAD CIUDADANA

Use of the facial recognition system to preserve public safety

Cristina Domingo Jaramillo*

Resumen

De un tiempo a esta parte, el uso de las nuevas tecnologías de la información y la comunicación ha irrumpido con fuerza y se ha extendido a cada vez más ámbitos de la sociedad. El de la seguridad, como no podía ser de otro modo, tampoco ha permanecido impasible ante tal expansión, pues cada vez son más los instrumentos utilizados para salvaguardar la seguridad pública. Entre los mismos, destacan aquellos que se basan en la biometría, al permitir la identificación de una persona a través de parámetros fisiológicos. Especialmente significativo es el reconocimiento facial, al ofrecer la posibilidad de detectar a una persona, incluso entre una gran multitud, a través de los parámetros del rostro. A pesar de que se ha puesto en práctica en algunos países, con el fin de detectar a delincuentes conocidos, mostrando ciertas garantías de éxito, lo cierto es que su implementación en nuestro país no está exenta de controversias. Los principales inconvenientes que plantea, se derivan de la eventual conculcación de los derechos y libertades fundamentales de la ciudadanía. Por este motivo, es necesario abordar el estudio de las implicaciones éticas y legales que la utilización del sistema de reconocimiento facial supondría en nuestro país, con el fin de determinar si se podría aplicar en todo caso o bajo ciertas condiciones establecidas específicamente en una Ley

Palabras clave

Biometría, reconocimiento facial, seguridad, derechos fundamentales.

Abstract

For some time now, the use of new information and communication technologies has erupted with force and has spread to more and more areas of society. Security has not remained impassive in the face of such expansion, since more and more instruments are used to safeguard public security. Among them, those that are based on biometrics stand out, by allowing the identification of a person through physiological parameters. Especially significant is facial recognition, offering the possibility of detecting a person, even in a large crowd, through the parameters of the face. Although it has been put into practice in some countries, in order to detect known criminals, showing certain guarantees of success, the truth is that its implementation in our country is not without controversy. The main inconveniences that it raises derive from the eventual infrigement of the fundamental rights and freedoms of citizens. For this reason, it is necessary to address the study of the ethical and legal implications that the use of the facial recognition system would entail in our country, in order to determine if it could be applied in any case or under certain conditions specifically established in a Law.

Keywords

Biometrics, facial recognition, safety, fundamental rights.

Información del artículo:

Fecha de recepción: 17/2/2021
Fecha de aceptación: 23/2/2021

Cómo citar este artículo:

Domingo Jaramillo, C. (2021). Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana, *El Criminalista Digital*, 9, 20-37. Recuperado de: http://revistaseug.ugr.es/index.php/cridi/article/view/20899 (fecha de consulta: 13 de enero de 2020).

* Contratada predoctoral FPU [ref. FPU 17/04799]. Departamento de Derecho Penal. Universidad de Granada.

Sumario: I. Introducción; II. Uso del reconocimiento facial para preservar la seguridad ciudadana en lugares públicos: *1. Cuestiones previas; 2. Vulneración de los derechos y libertades fundamentales:* 2.1. Discriminación; 2.2. Intimidad personal; 2.3. Protección de datos de carácter personal; *3. Discusión en torno a la limitación de los derechos fundamentales y preservación de la seguridad ciudadana;* III. Posible intervención del Derecho Penal: *1. Responsabilidad de los sujetos encargados del sistema de reconocimiento facial; 2. Excurso: violación del derecho a un proceso con todas las garantías;* IV. Conclusiones.

I. Introducción

Hoy día, las nuevas tecnologías de la información y la comunicación se están abriendo paso con fuerza y extendiendo su uso a cada vez más ámbitos de la sociedad. La seguridad pública no es ajena a esta expansión, pues aquellas se están implantando con el objetivo de garantizarla. Así, el reconocimiento facial se ha incorporado a los sistemas de videovigilancia por parte de las fuerzas del orden en algunos países. Éste es un método técnico de identificación de personas a través de una fotografía o imagen captada por una videocámara que lleva incorporado dicho sistema[1]. Para que la persona sea detectada, previamente debe haberse inscrito la imagen de su rostro en una base de datos informática[2]. Dicha imagen es la que posteriormente se comparará con los datos del rostro del sujeto detectados por el instrumento cuando aquel desee acceder a un lugar o sea localizado de forma encubierta en un espacio, ya sea público o privado[3]. Se considera que la imagen del rostro está compuesta por un número finito de elementos o características que varían en cada individuo y lo hacen único e identificable, por lo que el reconocimiento facial se muestra como un mecanismo de Inteligencia Artificial[4] de gran utilidad para preservar la seguridad pública[5], pues es capaz de identificar a personas a distancia, incluso entre una gran multitud.

[1] La imagen de una persona, en la medida en la que la identifique o la pueda identificar, es un dato de carácter personal que puede cumplir distintas finalidades. La más común es el uso de cámaras para garantizar la seguridad de personas, bienes e instalaciones, tal como recoge la Agencia Española de Protección de Datos (en adelante, AEPD) en la *Guía sobre el uso de videocámaras para seguridad y otras finalidades*, última modificación el 18 de junio de 2020, p. 4.

[2] La técnica analiza un número determinado de puntos alrededor de los ojos, la nariz y los pómulos. Estas medidas se toman usando un complejo algoritmo y posteriormente se someten a un proceso de codificación para insertarse en una plantilla: BREY, P. (2004). "Ethical Aspects of Facial Recognition Systems in Public Places". *Journal of Information, Communication and Ethics in Society*, 2, p. 99.

[3] COFFIN, J.S., e INGRAM, D. (1999). *Facial recognition system for security Access and identification*, Patente de Estados Unidos, nº 5.991.429, Washington DC: Oficina de Patentes y Marcas de los Estados Unidos, p. 1.

[4] Por Inteligencia Artificial se entiende la habilidad de una máquina para percibir y responder a su entorno de forma independiente y realizar tareas que normalmente requerirían de la inteligencia y de los procesos de toma de decisiones humanos, pero sin intervención directa de los mismos. En tal sentido, RIGANO, C. (2019). "Using Artificial Intelligence to address criminal justice needs". *National Institute of Justice*, 208, p. 1. El reconocimiento facial por desarrollar la labor de identificación y detección personal que normalmente llevan a cabo las personas, a través de un algoritmo automatizado, se incluye dentro de las técnicas de Inteligencia Artificial.

[5] Igualmente, se ha descubierto como un mecanismo útil a la hora de coadyuvar en el proceso judicial. Sobre ello, véanse, entre otros: *ibd.*, pp. 1-10; y DE MIGUEL BERIAIN, I., y PÉREZ ESTRADA, M.J. (2019). "La Inteligencia Artificial en el proceso penal español: un análisis a su admisibilidad sobre la base de los derechos fundamentales implicados". *Revista de Derecho. UNED*, 25, pp. 531 y ss. Los autores citados aluden específicamente al reconocimiento facial en la p. 534 como mecanismo capaz de apoyar al Tribunal en su percepción de si un testigo o el acusado levantan falso testimonio por la interpretación de sus movimientos corporales.

Por ser un método basado en el reconocimiento de personas a través de sus características fisiológicas[6], se constituye como una técnica biométrica[7] y, por dicho motivo, un tipo de información sensible[8]. En tal línea, el art. 9 del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (en adelante, RGPD) establece que los datos biométricos son una categoría de datos personales especiales y, en su apartado primero, prohíbe el tratamiento de los mismos, siempre y cuando vayan "dirigidos a identificar de manera unívoca a una persona física"[9]. Sin embargo, en su apartado segundo añade una excepción cuando concurran unas determinadas circunstancias, entre las que se encuentra la existencia de un "interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado". Por lo tanto, el uso de estos datos no está prohibido en todo caso, siempre y cuando exista un interés público esencial que legitime su utilización, como ocurre con la preservación de la seguridad ciudadana.

El uso de la biometría en general y, del reconocimiento facial en especial, plantea problemas en relación a la eventual conculcación de los derechos fundamentales recogidos en el art. 18 CE (específicamente a la intimidad personal y la protección de datos de carácter personal, recogidos en los apartados primero y cuarto, respectivamente)[10] y, con ello, la responsabilidad penal por los delitos tipificados en el Título X del Libro II del

[6] *Vid.*, Observatorio de la Seguridad de la Información. (2011). *Estudio sobre las tecnologías biométricas aplicadas a la seguridad*, Ministerio de Industria, Turismo y Comercio, p. 22; e Instituto Nacional de Ciberseguridad (INCIBE). (2016). *Tecnologías biométricas aplicadas a la ciberseguridad*. *Una guía de aproximación para el empresario*, p.4. La biometría no es una técnica novedosa, puesto que desde muy antiguo se ha recurrido al análisis de las características físicas de los individuos para identificarlos. Hasta que se desarrollaron métodos electrónicos de identificación, se hacía manualmente: COFFIN, J.S., e INGRAM, D. *Facial recognition system for security Access and identification…*, cit., p. 11; y DÍAZ RODRÍGUEZ, V. (2013). "Sistemas biométricos en materia criminal: un estudio comparado". *Revista del Instituto de Ciencias Jurídicas de Puebla*, 31, pp. 30-34. Concretamente, el uso de fotografías para la identificación de sospechosos es un antiguo elemento de la investigación policial. El reconocimiento facial actual (automatizado) es una extensión de los métodos tradicionales utilizados en los sistemas de justicia desde el siglo XIX. En este sentido, MANN, M., y SMITH, M. (2017). "Automated Facial Recognition technology: recent developments and approaches to oversight". *University of New South Wales Law Journal*, 40 (1), p. 122.

[7] Los datos biométricos son 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", tal y como viene recogido en el apartado 14 del art. 4 del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (en adelante, RGPD).

Para poder utilizar los sistemas biométricos, la identidad de los individuos debe ser registrada previamente mediante la captura de los parámetros que se pretenden analizar, ya sea el iris, la retina, la geometría de la mano, las huellas dactilares o, en nuestro caso, el rostro. Véase, Observatorio de la Seguridad de la Información, *Estudio sobre las tecnologías biométricas aplicadas a la seguridad*…, cit., pp. 31-37; INCIBE, *Tecnologías biométricas aplicadas a la ciberseguridad*…, cit., pp. 10-13. Las huellas dactilares en primer lugar y, el rostro en segundo, son los más utilizados, puesto que son únicos para cada persona. En este sentido, véase: COFFIN, J.S., e INGRAM, D. *Facial recognition system for security Access and identification*…, cit., p. 11; y YANG, W., WANG, S., HU, J., ZHENG, G., y VALLI, C. (2019). "Security and Accuracy of Fingerprint-Based Biometrics: A Review". *Symmetry*, 11 (141), p. 3.

Las funciones de la biometría para la identificación remota (que es la que utiliza el reconocimiento facial automatizado) son principalmente dos: identificación y autenticación. La primera permite reconocer a un individuo comparando sus datos con todos los que están almacenados en una plantilla y, la segunda, verificar la identidad cotejando los datos personales con otros almacenados previamente. Se comparan para determinar si la persona de las dos imágenes es la misma. Tal y como recoge la Comisión Europea en el *Libro Blanco sobre la Inteligencia Artificial: un enfoque europeo orientado a la excelencia y la confianza*, *de la Comisión Europea*, COM(2020) 65 final. El procedimiento de autenticación se utiliza por ejemplo, en los controles fronterizos de los aeropuertos.

[8] En este sentido, COTINO HUESO, L. (2017). "Big Data e Inteligencia Artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales". *Dilemata*, 24, p. 146, al afirmar que, cuando los macrodatos provenientes del Big Data y la Inteligencia Artificial no son de personas concretas identificadas o identificables, no se aplica la legislación de protección de datos. Por el contrario, el marco jurídico de protección para el uso del reconocimiento facial –por ir expresamente dirigido a identificar a una persona– es el RGPD y la *LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (a partir de ahora, LOPD) que deroga la anterior *LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* y traspone al Ordenamiento Jurídico lo recogido por el RGPD.

[9] A tenor de este precepto, se entiende que los datos biométricos considerados categoría especial son aquellos que, sometidos a tratamiento técnico específico, se dirijan a identificar a una persona. En caso de que no tengan dicha finalidad, no tendrán tal consideración. AEPD, *Informe 36/2020*, de 8 de mayo de 2020, sobre la utilización de técnicas de reconocimiento facial en la realización de pruebas de evaluación online, p. 18. Siguiendo el anterior, la Agencia se vuelve a pronunciar en idénticos términos en el *Informe 10308/2019*, de 28 de mayo de 2020, sobre el uso de sistemas de reconocimiento facial por parte de las empresas de seguridad privada, pp. 11 y 12.

[10] Sobre ello se ha pronunciado la Comisión Europea en el *Libro Blanco sobre Inteligencia Artificial*, p. 26, en el que se advierte sobre la afectación que en los mismos puede conllevar el reconocimiento facial.

Al ser la biometría una técnica relativamente novedosa, la jurisprudencia no es muy abundante al respecto, siendo inexistente para el reconocimiento facial. En este sentido, las resoluciones judiciales en la materia se refieren al uso de algunas técnicas en el sector privado para vigilar el cumplimiento por parte de los empleados de sus obligaciones contractuales. Así, el ATC (Sala Segunda) 57/2007 de 26 de febrero [RTC 2007/57] y, meses después, el Tribunal Supremo, en Sentencia de 2 de julio de 2007 [RJ/20017/6598] sostienen que la lectura biométrica de la mano para el control del horario es idónea, necesaria y proporcionada al fin perseguido, por no existir otros mecanismos menos intrusivos. Ambos entienden que no se infringe el derecho a la integridad física porque no produce lesión ni menoscabo corporal; tampoco se vulnera el derecho a la intimidad, ya que la mano no supone una parte

CP ("delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio") cuyo bien jurídico protegido se identifica con los derechos fundamentales señalados[11].

Sobre el funcionamiento y uso del reconocimiento facial –al igual que sucede con las nuevas tecnologías en general–, no existe normativa específica, dado que la legislación siempre va un paso por detrás de los avances técnicos, derivándose, en este caso, a lo establecido para la protección de datos de carácter personal. Por los problemas indicados anteriormente, se presenta como una técnica necesitada de regulación. Así, su estudio se muestra esencial, especialmente desde la ciencia penal[12], a fin de arrojar luz sobre la cuestión. Principalmente centraremos nuestro análisis en el uso que de aquella realizan las fuerzas y cuerpos de seguridad en lugares públicos con fines de preservación de la seguridad y de investigación y control de individuos, por ser un debate siempre latente la confrontación entre la seguridad ciudadana y la preservación de los derechos y libertades fundamentales.

II. USO DEL RECONOCIMIENTO FACIAL PARA PRESERVAR LA SEGURIDAD CIUDADANA EN LUGARES PÚBLICOS

1. Cuestiones previas

El reconocimiento facial se ha utilizado con múltiples fines, tanto en el sector privado[13] como en el público. En este último, algunas ciudades estadounidenses (como Tampa, San Francisco y Oakland) y de Reino Unido vienen aplicándolo desde hace tiempo, con el propósito principal de identificar a conocidos criminales o personas con una orden de arresto. Con dichos objetivos, la primera ciudad en implantarlo fue Londres en el

íntima del cuerpo. Por otro lado, la protección de datos queda garantizada, dado que la información únicamente se utiliza para verificar los parámetros recogidos previamente por la plantilla, no siendo la información convertida, idónea por sí misma para identificar a las personas. En idénticos términos pero referidas a la huella digital: la STS (Sala de lo Social) 96/2017 de 2 de febrero [RJ/2017/1628] y la STSJ de Murcia (Sala de lo Social, Sección 1ª) de 25 de enero [AS/2010/165], ya que este método no supone una intromisión ilegítima en el derecho a la intimidad, tanto por la parte del cuerpo utilizada, como por las condiciones en las que se lleva a cabo.

[11] En este sentido, *vid.*, GÓMEZ NAVAJAS, J. (2005). *La protección de los datos personales. Un análisis desde la perspectiva del Derecho Penal*. Navarra: Aranzadi, p. 83; y SÁINZ-CANTERO CAPARRÓS, J.E. (2020). "Capítulo 14. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I)", en Morillas Cueva, L., (Dir.), *Sistema de Derecho Penal. Parte Especial*. Madrid: Dykinson, pp. 338 y 339. El autor en cita continúa señalando que dicho Título, referido a la intimidad, es pluridimensional, pues afecta a la dignidad o integridad moral del individuo que puede convertirse en objeto de contemplación como una mera "cosa", si no tiene suficientemente garantizada la intimidad o un ámbito de privacidad en el que desarrollarse; a la libertad, ya que la intimidad es un ejercicio de voluntad por el que se fija un ámbito privado, personal… del que se excluyen a terceros; y, a la seguridad de todos los individuos frente a injerencias de otros.

[12] De esta opinión, MIRÓ LLINARES, F. (2018). "Inteligencia Artificial y justicia penal, más allá de los resultados lesivos causados por robots". *Revista de Derecho Penal y Criminología. UNED*, 3ª época, 20, p. 90. El autor no hace referencia exclusiva al reconocimiento facial, sino a los sistemas de Inteligencia Artificial, entre los que se encuentra aquel. Considera que estamos ante una problemática "a caballo" entre distintas ciencias relacionadas con la penal (sistema constitucional y sus derechos fundamentales, legislación procesal o administrativa, así como la Criminología que le da sentido a su uso policial). Así las cosas, se corre el riesgo de que su análisis y la determinación de las mejores condiciones de implementación quede en tierra de nadie. Por tanto, lo ideal es abordarlo de forma holística.

[13] El reconocimiento facial se utiliza como sistema de verificación de la identidad para acceder a *smartphones* y cuentas bancarias. En nuestro país, entidades bancarias como LA CAIXA han comenzado a implantarlo en sus cajeros automáticos. En un comunicado oficial, la entidad informa que la técnica garantiza una identificación completamente correcta, sin necesidad de utilizar el código PIN para acceder a la cuenta desde los cajeros automáticos. *Vid.*, CAIXA BANK, *CaixaBank inicia el despliegue de los cajeros con tecnología de reconocimiento facial por toda España*, 6 de junio de 2020, recurso electrónico obtenido a través de la Web: https://www.caixabank.com/comunicacion/noticia/caixabank-inicia-el-despliegue-de-los-cajeros-con-tecnologia-de-reconocimiento-facial-por-toda-espana_es.html?id=42302# , (consultado por última vez el día 6 de agosto de 2020). También se utiliza en el sector privado con fines de preservación de la seguridad. En esta línea, la cadena de supermercados Mercadona, lo ha implantado en 40 de sus tiendas para detectar a personas con una orden de alejamiento o medida judicial análoga –que les prohíbe acceder a sus establecimientos– contra la empresa o sus trabajadores. La AEPD ha iniciado una investigación de oficio por considerar que puede existir infracción legal, encontrándose el procedimiento en la fecha de redacción de estas líneas, en la fase de actuaciones previas de investigación, por lo que aún no se tienen detalles sobre el pronunciamiento. Véase RUBIO, I. (2020) "Protección de Datos abre una investigación sobre las cámaras de vigilancia facial de Mercadona". *El País*. 6 de julio, recurso electrónico obtenido a través de la Web: https://elpais.com/tecnologia/2020-07-06/proteccion-de-datos-abre-una-investigacion-sobre-las-camaras-de-vigilancia-facial-de-mercadona.html, (consultado por última vez el día 6 de agosto de 2020). Las tiendas que tienen implantada esta medida cuentan con un cartel informativo a la entrada, por lo que se presume que los usuarios están debidamente informados, cumpliendo así con el deber de información exigido en los artículos 12 RGPD y 22.4 de la LOPD. Específicamente en este último se señala que dicho deber de información queda cumplido mediante la colocación de un dispositivo informativo en un lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD. En el plano internacional, algunos artistas han usado este método en sus conciertos para controlar a sus acosadores, como es el caso de la estadounidense Taylor Swiftt: DEB, S., y SINGER, N. (2018). "Taylor Swift Said to Use Facial Recognition to Identify Stalkers". *The New York Times.* 13 de diciembre, recurso electrónico obtenido a través de la Web: https://www.nytimes.com/2018/12/13/arts/music/taylor-swift-facial-recognition.html, (consultado por última vez el día 24 de agosto de 2020).

año 1998, seguida posteriormente por Tampa (Florida) durante la final de la Superbowl XXXV en 2001[14]. A pesar de los ingentes beneficios en seguridad que aporta, esta técnica biométrica ha sido fuertemente criticada por los numerosos problemas que de la misma se derivan. Por este motivo, la ciudad de San Francisco, considerada el centro de la revolución tecnológica, ha prohibido la implementación del reconocimiento facial por parte de la policía y demás agencias de seguridad, con el fin de evitar la instauración de un estado policial de vigilancia masiva. Se critica que su uso se ha extendido más allá de los fines iniciales, ampliándose a la búsqueda de pequeños delincuentes. Además, el gobierno podría estar abusando de la tecnología, realizando una vigilancia opresiva[15].

En nuestro país, el reconocimiento facial se ha empezado a aplicar en distintos lugares con diversos propósitos[16] pero aún no se utiliza en espacios públicos con fines de preservación de la seguridad ciudadana y, antes de ponerlo en práctica, habría de valorarse si supone una injerencia intolerable en los derechos fundamentales. Es esencial que el uso de este tipo de sistemas sea respetuoso con los mismos, motivo por el que se requiere de una legislación sólida y consolidada en la materia puesto que, de lo contrario, nos abocamos hacia una sociedad orwelliana de la "tecnovigilancia"[17] o vigilancia masiva, en la que aquellos se ven gravemente afectados.

2. Vulneración de los derechos y libertades fundamentales

El reconocimiento facial –como venimos señalando– al igual que toda técnica basada en la biometría, presenta problemas en relación a los derechos y libertades fundamentales[18]. Aunque es menos invasiva que

[14] BREY, P. "Ethical Aspects of Facial Recognition Systems in Public Places…", cit., p. 100. En estas ciudades el sistema era utilizado en un principio por la policía para la labor de vigilancia rutinaria. Posteriormente se amplió su uso para localizar a niños perdidos y personas desaparecidas y, también se vio como una herramienta muy útil en la lucha contra el terrorismo tras los atentados del 11 de septiembre.

[15] CONGER, K., FAUSSET, R., y KOVALENSKI, S.F. (2019). "San Francisco Bans Facial Recognition Technology", *New York Times*, 14 de mayo, recurso electrónico obtenido a través de la Web: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html, (consultado por última vez el día 15 de agosto de 2020); y LEE, D. (2019). "San Francisco is first US city to ban facial recognition", *BBC News*, 15 de mayo, recurso electrónico obtenido a través de la Web: https://www.bbc.com/news/technology-48276660, (consultado por última vez el día 30 de agosto de 2020). Las organizaciones de derechos civiles han dado la voz de alarma contra la misma, así como la necesidad de llevar a cabo una acción normativa y reglamentaria urgente para restringir su uso. Así, otros muchos Estados y ciudades estadounidenses ya están tomando la iniciativa en la regulación y prohibición de esta tecnología: INIOLUWA, D.R., y otros (2020). "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing". *Actas de la Conferencia AAAI/ACM sobre IA, ética y sociedad*, p. 145.

En línea con lo señalado, la utilización que de la misma viene realizando China genera enormes controversias, pues uno de los objetivos es controlar a millones de ciudadanos musulmanes y pertenecientes a minorías étnicas. El gobierno chino justifica esta aplicación como medio para actuar contra la radicalización islámica y evitar el terrorismo, de modo que unos 2,5 millones de personas en la región de Xinjiang (en la cual existen incluso campos de reeducación para controlar a estas personas) están vigilados dondequiera que vayan por este sistema biométrico. Los datos (entre los que se encuentran el nombre, domicilio, fecha de nacimiento, documento de identidad y empresa en la que trabajan) están incluidos en una gran base de datos que contiene una lista de los lugares que frecuentan y acumula en tiempo real los movimientos de las personas insertas en la misma. Para profundizar más en la cuestión, véase VIDAL LIY, M. (2019). "2,5 millones de personas en China, bajo el control de una empresa de vigilancia facial", *El País*, 18 de febrero, recurso electrónico obtenido a través de la Web: https://elpais.com/internacional/2019/02/17/actualidad/1550422679_515333.html, (consultado por última vez el día 10 de agosto de 2020); y COLLINS, J. (2019). "China is using facial recognition to track millions of Muslim citizens wherever they go", *Quartz*, 17 de febrero, recurso electrónico obtenido a través de la Web: https://qz.com/1552708/china-is-using-facial-recognition-to-track-millions-of-muslim-citizens-wherever-they-go/, (consultado por última vez el día 1 de septiembre de 2020). El país asiático no solo hace uso del reconocimiento facial para estos fines, dado que, recientemente, lo ha utilizado para luchar contra la pandemia provocada por la COVID-19. Para ello, se ha implementado en lugares públicos como estaciones de metro subterráneas de distintas ciudades para escanear multitudes en busca de personas con fiebre o identificar a aquellas que no usan mascarillas. Sobre esto último, *vid.*, JAKHAR, P. (2020). "Coronavirus: las innovadoras tecnologías que está utilizando China para combatir la COVID-19 (y las preocupaciones que plantean), *BBC*, 4 de marzo, recurso electrónico obtenido a través de la Web: https://www.bbc.com/mundo/noticias-51736635, (consultado por última vez el día 20 de agosto de 2020). El uso de esta y otras técnicas plantean problemas de privacidad. Además, el gobierno podría aprovechar la crisis sanitaria para justificar la expansión de su sistema de vigilancia.

[16] Sobre las distintas funciones que en España se da al reconocimiento facial, véase ORTEGA, E. (2020). "En España ya se está utilizando el reconocimiento facial, ¿sabes dónde?", *Computer hoy*, 6 de julio, recurso electrónico obtenido a través de la Web: https://computerhoy.com/reportajes/tecnologia/lugares-espana-ya-utilizan-reconocimiento-facial-547573, (consultado por última vez el día 10 de agosto de 2020).

[17] Concepto utilizado por CUERDA ARNAU para referirse al conjunto de medidas de investigación que suponen la intervención y registro de comunicaciones de cualquier clase, así como aquellas investigaciones que se valen de dispositivos técnicos para el seguimiento y/o geolocalización, para la captación, en espacios abiertos o cerrados, de la imagen y/o sonido o, por último, persiguen acceder al contenido de dispositivos de almacenamiento masivo o al registro remoto de un ordenador. Se trata, en definitiva, de un conjunto de diligencias que suponen una grave afectación de los derechos fundamentales y del secreto de las comunicaciones, a la intimidad y el derecho a la protección del propio entorno virtual, en "La reforma de Ley de Enjuiciamiento Criminal en materia de tecnovigilancia. Visión de conjunto". En Alonso Rimo, A., Cuerda Arnau, M.L., y Fernández Hernández, A., (Dirs.). (2018). *Terrorismo, sistema penal y derechos fundamentales*. Valencia: Tirant lo Blanch, pp. 514 y 515. Previamente, GÓMEZ NAVAJAS, J. *La protección de los datos personales…*, cit., pp. 39 y 40, había mostrado su preocupación por el hecho de que el control informático, omnipresente, derivara en una sociedad como la que planteara Orwell en 1984.

[18] Sobre el peligro de una utilización amplia y sin control de la biometría desde el punto de vista de la protección de los derechos y libertades fundamentales de las personas, se pronunció el día 1 de agosto de 2003 el Grupo del 29 en el *Documento de Trabajo sobre Biometría*. En dicho documento, concretamente

otras como las basadas en la recopilación de huellas dactilares y muestras de ADN, pues se realiza a distancia y se integra en los sistemas de vigilancia existentes, es una fuente abierta de imágenes que pueden recogerse de redes sociales sin conocimiento o consentimiento del titular[19]. De este modo, junto a la función preventiva llevada a cabo por la policía para identificar a personas consideradas de riesgo que pueden participar en futuros delitos, se encuentra la de análisis de imágenes tomadas desde Internet para obtener plantillas faciales para su inserción en bases de datos policiales.

Por lo tanto, nos encontramos ante una técnica que, si bien es de gran utilidad, pues coadyuva a preservar la seguridad ciudadana al contribuir a identificar de forma automática a individuos delincuentes y terroristas conocidos, así como otros a los que se les ha impuesto una medida de seguridad (aun de tipo administrativo), como podría ser el alejamiento y prohibición de acceso a determinados espacios[20], no son pocos los inconvenientes que su uso conlleva. Especialmente significativos son los problemas relacionados con la discriminación, la intimidad personal y la protección de datos personales. Todo ello es lo que legitima la intervención del Derecho Penal en la materia, pues es necesaria para salvaguardar los derechos a la intimidad personal y la protección de datos personales que recoge el art. 18 de la Constitución Española[21].

2.1. Discriminación

Uno de los problemas que presentan los sistemas de Inteligencia Artificial, en general y, el reconocimiento facial, en particular, es la discriminación por razón de sexo, raza u origen étnico. La no discriminación como derecho fundamental, viene recogido como aspecto fundamental de los derechos humanos en todos los tratados internacionales[22] y, en nuestro país, en el art. 14 del Texto Constitucional.

Los riesgos que sobre la discriminación puede acarrear el uso de técnicas de Inteligencia Artificial, como señala el *Libro Blanco sobre Inteligencia Artificial*, vienen como resultado de defectos en el diseño del sistema o el uso de datos sesgados sin corrección previa. De este modo, la discriminación por la utilización del reconocimiento facial se produce desde el momento en el que el sistema detecta más eficazmente los puntos de referencia más representados en la base de datos. Tiene sesgos cuando los datos introducidos por las personas en los modelos de aprendizaje automáticos, representan de modo dispar el género y la raza. Así, cuando se tiene menos diversidad demográfica inserta en la base de datos, en comparación con la de la población a la que se

en la p. 5, se sostiene que un problema que plantea este tipo de técnicas de identificación a distancia es el relativo a la recogida y tratamiento de datos que puede hacerse sin el conocimiento del interesado; otro inconveniente es que, independientemente de su fiabilidad, se prestan a la utilización generalizada por su "bajo nivel de intrusión". Por este motivo, es necesario establecer garantías específicas al respecto.

[19] MANN, M., y SMITH, M. "Automated Facial Recognition Technology…", cit., pp. 124 y 125. Como ejemplo, la red social Facebook tiene un sistema de reconocimiento facial que etiqueta automáticamente fotografías, uniendo las imágenes con los datos personales que los individuos comparten en su perfil. En Alemania, el Comisionado de Hamburgo para la Protección de Datos y la Libertad de Información, declaró que la red social ha violado el RGPD con la función del etiquetado automático de fotografías, por lo cual solicitó que la desactivara y eliminase todos los datos biométricos que habían sido almacenados sin consentimiento previo. Véase la p. 141 del citado estudio.

[20] Piénsese, por ejemplo, en la utilidad que podría tener el reconocimiento facial para garantizar el cumplimiento de la sanción de prohibición de acceso de hinchas violentos a los estadios deportivos (principalmente en el ámbito futbolístico) para evitar las manifestaciones de violencia y preservar la seguridad pública durante un encuentro o competición, establecida en los arts. 24.3 y 25 de la *Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte*. En este sentido, el apartado segundo del último precepto señala que "a efectos del cumplimiento de la sanción, podrán arbitrarse procedimientos de verificación de la identidad, que serán efectuados por miembros de las Fuerzas y Cuerpos de Seguridad". En la misma línea, los arts. 29 y 80.5 del *RD 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte*. Por lo tanto, para el efectivo cumplimiento de dicha sanción, podría implantarse el sistema de reconocimiento facial en las videocámaras del circuito cerrado de televisión (CCTV) de los recintos deportivos para evitar manifestaciones violentas durante un encuentro o competición y garantizar el cumplimiento de la medida de prohibición de acceso de individuos violentos conocidos.

[21] Acerca de la necesaria intervención del ordenamiento punitivo en aras a salvaguardar la intimidad recogida como derecho fundamental en el art. 18 CE, *vid.*, MUÑOZ CONDE, F. (2019). *Derecho Penal. Parte Especial*. Valencia: Tirant lo Blanch, p. 255; en esta línea, SÁINZ-CANTERO CAPARRÓS, sostiene que "el ser humano, por ser ante todo un animal social, precisa de ciertos ámbitos propios, reservados, privados, íntimos, en los que poder manifestar plenamente su forma de ser y desarrollar su personalidad sin injerencia o intervención de terceros". Así, por ser la intimidad un derecho fundamental, crea el derecho a ser protegido frente a las intromisiones o injerencias de otros en la vida privada y, por este motivo, es por el que el ordenamiento punitivo debe intervenir: "Capítulo 14. Delitos contra la intimidad…", cit., p. 339; en términos similares, DE LA MATA BARRANCO, N.J., y BARINAS UBIÑAS, D. (2014). "La protección penal de la vida privada en nuestro tiempo social: ¿necesidad de redefinir el objeto de tutela?". *Revista de Derecho Penal y Criminología*, 3ª Época, 11, p. 14, afirman "que el ser humano sigue teniendo entre sus necesidades jurídicas básicas, como siempre, la de que se le garantice un espacio de actuación propio, ajeno a interferencias, intromisiones o simplemente conocimiento de otros; pero el modo en el que empieza a entenderse hoy en día está muy condicionado por una diferente forma de desarrollo de las relaciones sociales desde la perspectiva de la realidad tecnológica virtual. Y a ello no puede ser ajeno ni el Derecho ni, mucho menos, el Derecho Penal".

[22] Concretamente, en el art. 2 de la Declaración Universal de Derechos Humanos, en el que expresamente se señala que "toda persona tiene todos los derechos y libertades proclamados en esta Declaración, sin distinción alguna de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición".

destina, los errores son mayores, puesto que los individuos de los grupos con menor representación no se detectan correctamente[23], produciendo fallos en la identificación.

En este sentido, la investigación ha demostrado que la técnica yerra más a la hora de localizar a personas con la piel oscura y mujeres. Mientras que el perfil del varón blanco es el que menos errores presenta, el de mujeres de color es el que más errores reporta[24]. Por ser un método que favorece el sesgo racista, algunas grandes multinacionales que vendían sus servicios de reconocimiento facial a las fuerzas del orden, entre las que se encuentran IBM y Amazon, retiran estos productos del mercado. Esto trae causa de las protestas extendidas por todo el mundo contra el racismo por la brutalidad policial hacia personas afroamericanas en EE.UU.[25], de lo que fuimos testigos durante los meses de junio y julio del año 2020 por la muerte de George Floyd a manos de un agente de policía.

Los errores en las identificaciones preocupan especialmente cuando van dirigidas a la detención de delincuentes y el sistema reconoce como sospechosos a personas inocentes. Como ejemplo, traemos a colación la reciente detención errónea en Detroit (EE.UU.), de un individuo afroamericano a través de una antigua fotografía de su licencia de conducir, por un delito que no había cometido[26].

Por tanto, nos encontramos ante una técnica que, si no se prepara adecuadamente, presenta graves sesgos, lo cual viene a favorecer la discriminación racial y de género. Para poder hacer un uso correcto de la misma en un determinado lugar, habría que entrenar el sistema con datos que representen a todos los grupos demográficos que habitan en el mismo, con lo cual se reducirían los problemas de error, garantizando además la no discriminación.

2.2. Intimidad personal

La protección de la vida privada supone el derecho que permite al individuo ocultar información sobre sí mismo, resaltando su inmunidad y la importancia de salvaguardar su integridad. Está íntimamente ligado a la dignidad y el libre desarrollo de la personalidad, sito en el art. 10.1 CE. Aquél, concede ciertas esferas al individuo, indispensables para el adecuado desenvolvimiento social por ser, a juicio de SÁINZ-CANTERO CAPARRÓS, un derecho de la personalidad que concede a todo individuo, la facultad de excluir a los demás de ciertos ámbitos de su vida privada o su vida y relaciones familiares, sobre los que no quiere injerencias o intromisiones de terceros, incluidos los poderes públicos[27]. Por tanto, siguiendo a MIRÓ LLINARES, podemos afirmar que la intimidad es la "parcela de la vida que se considera no sólo secreta sino absolutamente privada y reservada para uno mismo" y que lleva consigo la posibilidad de excluir a otros de la misma[28]. Así, supone la capacidad de decisión del individuo sobre determinados aspectos de su vida, reservados, personales, íntimos, los cuales pretende mantener en privado y alejados de extraños.

Así las cosas, el uso de esta técnica puede conllevar la injerencia en la privacidad o intimidad[29] por varios motivos. Por un lado, la codificación de una parte corporal hace que la misma adquiera un nuevo significado o

---

[23] LEARNED-MILLER, E., y otros. (2020). *Facial recognition technologies in the wild: a call for a federal office*. MacArthur Foundation, p. 9.

[24] Véase, más ampliamente, INIOLUWA D.R., y otros. "Saving Face…", cit., p. 146; y, más específicamente en relación al género, el interesante estudio de BUOLAMWINI, J., y GEBRU, T. (2018). "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification". *Proceedings of Machine Learning Research*, 81, pp. 1 y ss.

[25] NAVARRO, B. (2020). "IBM y Amazon abjuran de la tecnología de reconocimiento facial por su sesgo racista", *La Vanguardia*, 16 de junio, recurso electrónico obtenido a través de la Web: https://www.lavanguardia.com/internacional/20200611/481710398480/ibm-reconocimiento-facial-racismo-tecnologia-negros.html, (consultado por última vez el día 18 de agosto de 2020).

[26] Afortunadamente, el fiscal pidió su absolución por falta de pruebas: LABORDE, A. (2020). "Detenido injustamente un afroamericano en EE UU por un error en el sistema de reconocimiento facial", *El País*, 26 de junio, recurso electrónico obtenido a través de la Web: https://elpais.com/tecnologia/2020-06-26/un-afroamericano-es-detenido-injustamente-por-un-error-en-el-sistema-de-reconocimiento-facial.html, (consultado por última vez el día 24 de agosto de 2020).

[27] SÁINZ-CANTERO CAPARRÓS, J.E. "Capítulo 14. Delitos contra la intimidad…", cit., p. 339.

[28] MIRÓ LLINARES, F. "Inteligencia Artificial y justicia penal…", cit., p. 115.

[29] Aunque anteriormente, al abordar las cuestiones generales de la biometría, hacíamos referencia a la privacidad como un ámbito afectado especialmente por el uso de estas técnicas, procedemos a realizar un tratamiento unitario de aquella junto con el derecho a la intimidad personal, pues aun siendo conscientes de las diferencias entre ambos, adoptamos la posición del sector doctrinal que considera este último incluido en el concepto amplio de privacidad. En este sentido, seguimos la línea establecida en nuestra Constitución, que recoge en un mismo precepto, el art. 18 CE, la tutela de la vida privada de forma integral, protegiendo distintos bienes de la personalidad unidos bajo el mismo nexo común: la protección del uso de la información

función, suponiendo la creación de información de partes del cuerpo de una persona que son usadas y controladas por otras, lo cual deriva en un proceso de alienación[30]. Además, los datos del rostro pueden ser registrados sin el consentimiento del titular. Cuando el reconocimiento facial se utiliza con fines de vigilancia, puede derivar (como señalamos *supra*) en una vigilancia masiva, destinada a obtener datos relativos a las creencias religiosas de los sujetos o sus relaciones sociales, puesto que puede rastrearse dónde van las personas a rezar, con quienes se relacionan y si asisten a manifestaciones, pudiendo inhibirse de realizar estas actividades cotidianas por temor a sufrir represalias y estigma social[31]. Relacionado con esto último, una vez que los parámetros del rostro han sido registrados, pueden vincularse a información personal de todo tipo para realizar perfiles o patrones de comportamiento.

Incluso cuando se pretende localizar a una persona sobre la que recae una orden de detención, todas las caras detectadas por el sistema pueden ser buscadas algorítmicamente sin consentimiento y sin que medie proceso judicial contra ellas. Para evitar esto, se debería garantizar que el sistema detecte y conserve únicamente la imagen de aquellos individuos previamente registrados, no así la de los demás.

2.3. Protección de datos de carácter personal

Estrechamente vinculado a la intimidad, el derecho a la protección de datos personales. Este último, aun siendo una manifestación de la intimidad personal, es autónomo[32]. Se manifiesta como la voluntad de la persona de controlar qué datos e informaciones pueden conocerse o utilizarse. Supone controlar la propia información, estableciendo qué se puede conocer, quién puede conocerlo y para qué se puede conocer o utilizar lo que se conoce[33]. Si bien los datos personales no son solo de tipo privado, sino también públicos, ya que, como señalamos anteriormente, son todos los que identifican o permiten identificar a una persona. De modo que, cuando se hace referencia a la protección de la intimidad y la vida privada, aludimos a todos los datos de carácter personal, no solo a los privados. Esto cobra especial sentido para nuestro objeto de estudio, debido a que el reconocimiento facial se basa en la identificación de una persona a través de la imagen de su rostro (dato personal por antonomasia) la parte más visible y pública de los individuos, a través de la que es más fácil realizar su identificación.

Pues bien, aun siendo los anteriores dos derechos fundamentales independientes, un sector doctrinal considera que nos encontramos ante un único derecho fundamental, intimidad –y, por ende, un solo bien jurídico a tutelar en los delitos del Capítulo I del Título X del Texto punitivo– en una doble vertiente, negativa y positiva. Tal y como expone MUÑOZ CONDE, la primera se refiere a la intimidad en sentido estricto, haciendo referencia a una especie de derecho a la exclusión de los demás de ciertos aspectos de la vida privada que pueden

personal. Sobre esta cuestión, véase más ampliamente: NOAIN SÁNCHEZ, A. (2016). "La protección de la intimidad y vida privada en Internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)". *Premio de Protección de Datos Personales de Investigación 2015*. Madrid: Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del Estado, pp. 41 y ss. Según la autora, la privacidad, como derecho supraindividual, supone la salvaguarda de la dimensión propia del individuo, aquella que le es irrenunciable, por ser inherente a su esencia como persona. Por su parte, la intimidad es de índole inmaterial, relativa a la parte más interna de la persona, siendo, además de reservada, genuina. Recoge los aspectos individuales desconocidos por los demás, por lo que constituye una especie de "derecho al secreto" sobre lo que hacemos, decimos o pensamos. Es inherente a todas las personas y forma parte de la esencia de la personalidad. Por tanto, son términos afines pero no sinónimos. Comparten como característica en común la ausencia de difusión.

[30] BREY, P. "Ethical Aspects of Facial Recognition Systems in Public Places…", cit., p. 107. Y, en relación al primer problema, el autor plantea que mucha gente encuentra la biometría como una técnica deshumanizadora.

[31] LEARNED-MILLER, E., y otros. *Facial recognition technologies in the wild…*, cit., p. 12.

[32] Sobre la autonomía de la protección de datos personales respecto a la intimidad, se ha pronunciado el Tribunal Constitucional, entre otras, en las Sentencias 209/2000 de 30 de noviembre [RTC 2000/290]; 14/2003 de 28 de enero [2003/14]; 151/2014 de 25 de septiembre [RTC 2014/151]; y 58/2018 de 4 de junio [RTC 2018/58], pues considera que ambos tienen un contenido propio y específico. El primero entendido como "derecho fundamental a la protección de datos", "*habeas data*" o "derecho a la autodeterminación informativa". En la doctrina también encontramos planteamientos que siguen la línea establecida por el Tribunal Constitucional. Así, entre otros, GÓMEZ NAVAJAS, J. *La protección de los datos personales…*, cit., pp. 30 y 31.

[33] SÁINZ-CANTERO CAPARRÓS, J.E "Capítulo 14. Delitos contra la intimidad…", cit., p. 340. De forma parecida, ESQUINAS VALVERDE, P. (2010). *Protección de datos personales en la Policía Europea.* Valencia: Tirant lo Blanch, p. 18, cuando sostiene que este derecho se define "como la libertad para precisar quién y con qué ocasión puede conocer informaciones que conciernen a cada sujeto". A lo anterior añade también "el conjunto de medios jurídicos para que los individuos puedan gestionar el uso por parte de terceros de sus datos personales".

considerarse secretos. La segunda, sería el derecho de control sobre la información y los datos personales, incluso los ya conocidos, para que sólo puedan usarse conforme a la voluntad de su titular[34].

Así las cosas, hemos de concluir que, en torno al concepto de intimidad existen discrepancias doctrinales, pues nos encontramos, en palabras de CASTELLÓ NICÁS, ante "un objeto de protección con contornos difícilmente definibles"[35]. A pesar de ello, de lo que no cabe duda es que nos encontramos ante dos derechos fundamentales que constituyen el bien jurídico amplio intimidad en su doble vertiente negativa o derecho "a ser dejado en paz" y positiva[36], que permite al sujeto el desarrollo de su personalidad y la afirmación de su libertad individual, a través del control de la información personal.

Para concluir el análisis del presente apartado y a modo de recopilación, señalar que los derechos a la intimidad personal y a la protección de datos de carácter personal pueden verse gravemente vulnerados por el uso policial del reconocimiento facial. En vista de ello, inmediatamente se nos plantea el debate sobre qué ha de prevalecer en estos casos, si la seguridad pública o los citados derechos y libertades fundamentales.

3. Discusión en torno a la limitación de los derechos fundamentales y preservación de la seguridad ciudadana

La controversia existente entre la preservación de la seguridad ciudadana y la posible limitación del ejercicio de los derechos y libertades fundamentales es un problema real, especialmente cuando se utilizan técnicas muy intrusivas en estos últimos, como el reconocimiento facial inserto en los sistemas de videovigilancia[37]. Ello trae causa del hecho de que esta técnica –como se expuso ampliamente en líneas superiores– vulnera gravemente éstos, mientras que los beneficios de seguridad no son tan elevados como se pretende, al existir un elevado índice de identificaciones erróneas[38]. En este sentido, habría que decidir qué prevalece más con su uso, si la seguridad ciudadana o los derechos de los individuos.

La seguridad ciudadana se define en el Preámbulo de la *LO 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana* (en adelante, LOPSC) como la "actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad ciudadana"[39]. La misma, ha de ser preservada por las FCS, tal como queda

[34] Véase, MUÑOZ CONDE, F. *Derecho Penal. Parte Especial…*, cit., p. 256. La jurisprudencia, en la misma línea, entiende la intimidad como un derecho del sujeto a impedir que otros accedan a determinados aspectos de su vida, siendo así un derecho garantista o de defensa; y, la protección de datos personales, relacionada con la libertad de acción del individuo que tiene potestad para controlar la información relativa a él mismo y su familia: STS (Sala de lo Penal, Sección 1ª) 412/2020 de 20 de julio [JUR 2020/235172]. Años antes, el Tribunal Constitucional en Sentencia 292/2000 de 30 de noviembre [RTC 2000/292] planteó que el derecho a la intimidad "permite excluir ciertos datos de una persona del conocimiento ajeno" (aspecto negativo de la intimidad), mientras que el derecho a la protección de datos "garantiza a los individuos un poder de disposición sobre esos datos" (vertiente positiva del derecho general a la intimidad).

[35] CASTELLÓ NICÁS, N. (2015). "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio". En Morillas Cueva, L., (Dir.). *Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015)*. Madrid: Dykinson, p. 493. En términos similares, MUÑOZ CONDE, F. *Derecho Penal. Parte Especial…*, cit., p. 256, cuando afirma que es "difícil precisar con nitidez el concepto de intimidad como bien jurídico protegido".

[36] DE LA MATA BARRANCO, N.J., y BARINAS UBIÑAS, D. "La protección penal de la vida privada en nuestro entorno social…", cit., p. 31.

[37] Ya el uso de los sistemas de videovigilancia en lugares públicos con tales fines, plantea serios problemas sobre su licitud por trasgredir los derechos y libertades ciudadanas. Al no existir abundante materia de estudio sobre el reconocimiento facial, acudiremos mayoritariamente a la bibliografía existente sobre el uso de videocámaras y los CCTV.

[38] Acerca del debate existente en este punto entre los detractores y defensores de la implantación de la técnica, véase en mayor profundidad: BREY, P. "Ethical Aspects of Facial Recognition Systems in Public Places…", cit., pp. 101 y ss.

[39] En este punto, entendemos necesario distinguir entre la seguridad ciudadana y la personal, pues son conceptos distintos. La primera es muy difícil de definir, es un concepto polémico, dada la dificultad de establecer con precisión su contenido, pues no hay ningún texto normativo que lo concrete. El Tribunal Constitucional lo asemeja al "orden público" en Sentencia 325/1994 de 12 de diciembre [RTC 1994/325], como "la situación de normalidad en que se mantiene y vive un Estado, cuando se desarrollan las diversas actividades colectivas sin que se produzcan perturbaciones o conflictos". Dicha resolución, conceptualiza ambos términos como manifestaciones de "tranquilidad". En esta línea, se refiere a la seguridad personal como "la tranquilidad de espíritu producida por la eliminación del miedo" y, cuando alude a la seguridad pública lo hace como "tranquilidad en las calles". A pesar del esfuerzo del Tribunal Constitucional por precisar el contenido del término, no existe consenso. Para ampliar más sobre la controversia existente a nivel jurisprudencial, véase JIMÉNEZ DÍAZ, M.J. (2006). *Seguridad ciudadana y Derecho Penal*. Madrid: Dykinson, pp. 13 y ss. La autora en cita culmina señalando, con buen criterio que, nos encontramos ante dos expresiones "que reflejan contenidos netamente diferenciados". Y, en la misma línea GÁLVEZ JIMÉNEZ, plantea además que, la seguridad personal es individual y se materializa a través del libre ejercicio de los derechos, mientras que la pública, es resultado del libre ejercicio de los derechos de todos y de su protección por las fuerzas del orden. Sobre el concepto de seguridad pública la autora debate más ampliamente en "El derecho a la seguridad personal". En Monereo Atienza, C., Monereo Pérez, J.L., y Aguilar Calahorro, A., (Coords.). (2014). *El sistema universal de los derechos humanos. Estudio sistemático de la declaración universal de los derechos humanos, el pacto internacional*

reflejado en el art. 104.1 CE. La seguridad de los ciudadanos sobrepasa la seguridad del Estado, entendiéndose que si los ciudadanos están seguros, ese Estado es seguro[40].

Por su parte, el respeto a los derechos humanos significa que éstos no pueden ser violados por otros y el cumplimiento significa que se deben implantar medidas positivas para asegurar que los individuos disfrutan de los mismos[41]. Tal como se establece en el Preámbulo de la LOPSC, la seguridad es el instrumento al servicio de la garantía de los derechos y libertades y no constituye un fin en sí mismo. Por este motivo, el Tribunal Constitucional ha manifestado que cualquier limitación en el ejercicio de estos últimos por razones de seguridad debe ampararse en el principio de proporcionalidad. Así, en Sentencia de 22 de mayo de 2019[42] –entre otras– expone que, como cualquier otro derecho fundamental, la protección de datos personales (y, por ende, también la intimidad) no tiene carácter absoluto. Puede restringirse por ley, siempre que responda a un fin de interés general y, los requisitos y alcance de la restricción estén precisados legalmente y respeten el principio de proporcionalidad. Principio este que incluye tres dimensiones: a) idoneidad, si consigue el objetivo propuesto; b) necesidad, basado en la inexistencia de otra medida menos intensa; y c) proporcionalidad, si de ello se deriva un beneficio para el interés público que justifica cierto sacrificio de los derechos[43].

Pues bien, en vista de lo anterior, la limitación de derechos fundamentales que supone el reconocimiento facial, estaría amparada si con ello se previene la delincuencia, ya que, tal y como afirma HOWARD-HASSMAN, la seguridad personal de los individuos se encuentra efectivamente amenazada por el crimen. Los Estados son los principales responsables, a través de las fuerzas policiales, de proteger a los sujetos contra los delincuentes. En este sentido, los Estados tienen la obligación de garantizar la seguridad de los ciudadanos, utilizando para ello medidas que inciden en los derechos fundamentales[44]. De este modo, los Estados actualmente estarían más preocupados por garantizar la seguridad de los ciudadanos, entendiendo que dentro de la misma se incluye la protección de los demás derechos y libertades fundamentales, utilizando para ello cualquier técnica que se muestre idónea a tal fin.

Así las cosas, la utilización del reconocimiento facial con fines policiales puede justificarse por ser un instrumento eficaz para mejorar la seguridad ciudadana, tanto en lugares privados como públicos, con el objetivo de desalentar y detectar comportamientos perjudiciales, delincuencia y disturbios. Sin embargo, a nuestro juicio, no sería adecuada su implantación en nuestro país, puesto que los beneficios en seguridad son mucho menores que la grave vulneración que supone a los derechos y libertades fundamentales (tal como se expuso *supra*). En esta línea se pronuncia BARONA VILAR, para quien, aunque la técnica venga con la promesa de garantizar una mayor seguridad, se aproxima al escenario orwelliano de una sociedad basada en el sometimiento al control de no se sabe muy bien quién o qué. Por ser algoritmos, técnicas de análisis de datos y creación de bancos de imágenes de caras, entregan a las fuerzas de seguridad un instrumento que, a pesar de identificar a delincuentes y terroristas, limita o restringe los derechos y garantías ciudadanas[45]. Además, la seguridad puede preservarse con métodos menos intrusivos como la videovigilancia común. Y, si finalmente se optase por su implementación, los límites y condiciones de su uso deben estar debidamente recogidos en una

de derechos civiles y políticos, el pacto internacional de derechos económicos, sociales y culturales y textos internacionales concordantes. Granada: Comares, pp. 395 y ss.

[40] HOWARD-HASSMAN, R.E. (2012). "Human Security: Understanding Human Rights". *Human Rights Quarterly*, 34, p. 90.

[41] *Ibd.*, pp. 93 y 94; e ISHAY, M.R. (2014). *The History of Human Rights: from Ancient Times to the Globalization Era.* University of California Press, pp. 63-116.

[42] STC (Pleno) 76/2019 de 22 de mayo [RTC 2019776].

[43] *Vid.*, en esta línea además, GIL MEMBRADO, C. (2019). *Videovigilancia y protección de datos. Especial referencia a la grabación de la vía pública desde el espacio privado*. Madrid: Wolters Reuters, p. 212. Igualmente, la AEPD en el Informe Jurídico 0117/2007 sobre la prevalencia en el ejercicio de derechos, pp. 6 y 7, entiende que la seguridad pública es un bien constitucionalmente protegido y los derechos y libertades fundamentales pueden limitarse siempre que la limitación no se salga de lo razonable y se tengan en cuenta los principios establecidos por el TC.
Igualmente, el considerando 4 del RGPD entiende que el derecho a la protección de datos personales no es absoluto y debe mantener un equilibrio respecto a otros derechos fundamentales, con arreglo al principio de proporcionalidad.

[44] HOWARD-HASSMAN, R.E. "Human security…", cit., pp. 99-103; PIÑAR MAÑAS, J.L. (2009). *Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio*. *Documento de Trabajo 147/2009*, Laboratorio de Alternativas, 147, pp. 23 y ss.; BREY, P. "Ethical Aspects of Facial Recognition Systems in Public Places…", cit., pp. 104-107: se entiende que la seguridad implica, a su vez, la protección contra daños a los derechos más básicos, como el derecho a la vida, a la libertad y a la propiedad; y GIL MEMBRADO, C. *Videovigilancia y protección de datos…*, cit., p. 126.

[45] BARONA VILAR, S. (2019). "Inteligencia Artificial o la algoritmización de la vida y de la justicia: ¿Solución o problema?". *Revista Boliviana de Derecho*, 28, p. 26.

Ley[46], a fin de que se garantice una conculcación mínima de los derechos y libertades ciudadanas en aras a preservar la seguridad. Por todo ello, entendemos que un uso inadecuado del reconocimiento facial podría dar lugar a los delitos recogidos en el Capítulo I del Título X del CP. Cuestión que abordamos a continuación.

III. POSIBLE INTERVENCIÓN DEL DERECHO PENAL

Una vez analizada la intromisión que el uso del reconocimiento facial con fines de preservación de la seguridad supone en los derechos y libertades fundamentales, así como el debate existente entre la preeminencia de aquella sobre estos últimos, procede analizar la posible intervención del Derecho Penal por el uso del sistema de reconocimiento facial con fines de preservación de la seguridad, ya que puede conculcar de gravedad el bien jurídico intimidad (en su doble vertiente, positiva y negativa), lo cual deriva en la responsabilidad penal por la comisión de las conductas tipificadas en el Texto punitivo, concretamente en el Capítulo I del Título X del Libro II (arts. 197 a 201) "Del descubrimiento y revelación de secretos"[47].

Dicho Título fue ampliamente modificado por la reforma al Texto punitivo llevada a cabo por la *LO 1/2015, de 30 de marzo*, a fin de incluir en el mismo determinadas conductas relacionadas con las nuevas tecnologías que, hasta la fecha, no encontraban respaldo penal[48]. En base al principio de intervención mínima, el legislador únicamente ha tipificado aquellos delitos que ha considerado de mayor gravedad, los que conculcan gravemente los derechos a la intimidad personal y la protección de datos personales. Ello no significa que las demás conductas que no reúnan los requisitos establecidos en el Código Penal –por su escasa entidad lesiva– queden sin el oportuno reproche, puesto que, pueden ser sancionadas por la legislación civil o administrativa existente en la materia[49].

1. Responsabilidad de los sujetos encargados del sistema de reconocimiento facial

El injusto de los delitos de descubrimiento y revelación de secretos, está en el hecho de no respetar la voluntad del titular de la intimidad, siendo necesaria la constancia del consentimiento al tratamiento de datos personales y compartir con los demás aquellos aspectos reservados de su vida privada que considere oportunos[50]. En caso de no existir dicho consentimiento, se incurriría en responsabilidad penal. Esto supone un problema en el reconocimiento facial, porque se inserta en los sistemas de videovigilancia y no es posible obtener el consentimiento de toda la población a la grabación de sus imágenes, con lo cual, su uso podría ser delictivo en todo caso. A pesar de ello, este inconveniente puede salvarse con la obligatoriedad de informar a la población sobre su implementación, a través de carteles informativos en los lugares en los que se vaya a utilizar (arts. 12

[46] En este sentido se pronuncia la AEPD en el informe emitido sobre el uso de sistemas de reconocimiento facial por parte de las empresas de seguridad privada, pp. 23 y 31. La Agencia sostiene que cualquier tratamiento de datos biométricos requiere su previsión en una norma de Derecho europeo o nacional, debiendo tener rango de Ley. Dicho texto normativo debe especificar además el interés público esencial que justifica la restricción de los derechos que afecta y bajo qué circunstancias puede hacerse, estableciendo además las reglas precisas que hagan previsible al interesado la imposición de la limitación y sus consecuencias, sin que sea suficiente la invocación genérica a un interés público. En vista de lo anterior, culmina exponiendo que la regulación actual es insuficiente, por lo que en principio, no puede implantarse.

[47] Los diversos artículos que recoge este Capítulo tipifican varios delitos que tienen como característica común el proteger la voluntad de una persona de que no sean conocidos determinados hechos, siendo así, secretos; pero también el derecho del sujeto a controlar cualquier información que afecte a su vida privada y, por tanto, su intimidad: MUÑOZ CONDE, F. *Derecho Penal. Parte Especial…*, cit., p. 255.

[48] Sobre la citada Reforma, véase ampliamente, CASTELLÓ NICÁS, N. "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio…", cit., pp. 487 y ss.

[49] En este sentido, sería de aplicación lo dispuesto por la *LO 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen*, así como la legislación en materia de protección de datos de carácter personal (RGPD y LOPD, ya citadas anteriormente). Y, por insertarse en sistemas de videovigilancia, la *LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos* y la *Ley 5/2014, de 4 de abril, de Seguridad Privada*. De este modo, por el carácter fragmentario y la subsidiariedad del ordenamiento punitivo (que conforman el principio de intervención mínima), éste solamente intervendrá cuando los demás mecanismos de control social, menos lesivos, hayan fracasado, dada la especial entidad de la infracción. *Vid.*, SUÁREZ LÓPEZ, J.M. (2015). "Los principios limitadores del *ius puniendi* en un Estado social y democrático de Derecho y su incidencia en la represión penal del dopaje en el deporte". En Benítez Ortúzar, I.F., (Coord.). *Tratamiento jurídico penal y procesal del dopaje en el deporte*. Madrid: Dykinson, p. 113; y, en mayor profundidad, MORILLAS CUEVA, L. (2005). "El Derecho Penal mínimo o la expansión del Derecho Penal". *Revista Cubana de Derecho*, 25, pp. 93 y ss. EL MISMO. (2018). *Sistema de Derecho Penal. Parte General.* Madrid: Dykinson, pp. 134 y 135.

[50] SÁINZ-CANTERO CAPARRÓS, J.E. "Capítulo 14. Delitos contra la intimidad…", cit., p. 340. De este modo, el consentimiento se erige como causa de atipicidad de la conducta, dado que la intimidad (dentro de la cual como concepto amplio, incluimos la protección de datos de carácter personal) es un bien jurídico personal y, por tanto, disponible por su titular, de forma que si este se ha prestado libremente, deriva en la atipicidad de la conducta. De idéntica opinión, anteriormente, GÓMEZ NAVAJAS, J. *La protección de los datos personales…*, cit., p. 225.

RGPD y 22.4 LOPD), en los que se especifique que determinado espacio está siendo vigilado a través de videocámaras que tienen insertados dispositivos de reconocimiento facial.

El reconocimiento facial no suele utilizarse directamente por los agentes de las FCS, sino que depende de empresas del sector privado que prestan sus servicios a aquellos. En este sentido, podría ser responsable penalmente el encargado del tratamiento de los datos, cuando hace uso de estos sistemas de grabación en detrimento de la privacidad de los individuos, con fines alejados de la preservación de la seguridad (para lo que inicialmente se implantó). Es decir, puede utilizar el sistema para captar la imagen del rostro de los individuos y controlar sus patrones de movimiento, creando así perfiles conductuales[51]. En este sentido, sería de aplicación lo dispuesto en el art. 197.1 *in fine* CP, pudiendo imponerse las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. En caso de que dicha información sea facilitada a otras empresas o individuos con distintos fines, entre los que se pueden encontrar los de tipo comercial, se impondrá, según el párrafo primero del apartado tercero del art. 197 CP, la pena de prisión de dos a cinco años. Por su parte, puede incurrir igualmente en responsabilidad, el sujeto que no tomó parte en la captación de las imágenes pero, aun conociendo su origen ilícito, realiza la conducta anterior (párrafo segundo del art. 197.3 CP)[52]. Piénsese en este caso, en el empleado de la empresa al que se le encomienda puntualmente la tarea de controlar el fichero de datos, conociendo que de los mismos se está haciendo un uso fraudulento pero no tomó parte en su captación. A pesar de ello, los cede a terceras personas, en detrimento de la intimidad de los individuos cuyos datos se encuentran recogidos en el fichero. A nuestro juicio, lo normal en ambos supuestos es que la conducta sea ejecutada con ánimo de lucro, a fin de obtener una ganancia. En este caso, sería de aplicación lo establecido en el apartado sexto del precepto que venimos analizando, por lo que las penas señaladas se impondrán en su mitad superior. Igualmente, los responsables de los ficheros o, aquellos que, por cualquier motivo, tengan acceso a los mismos, si modifican o alteran las plantillas del rostro de delincuentes o terroristas conocidos, pudiendo con ello darse identificaciones erróneas, podrían estar realizando la acción típica recogida en el art. 197.2 CP.

Como en este caso que venimos analizando, el sujeto activo es principalmente el encargado del fichero, cabría aplicar la agravante prevista en la letra a) del apartado cuarto del mismo artículo[53], imponiéndose así una pena de prisión de tres a cinco años. Y, en caso de que los datos sean cedidos a terceros, dichas penas se impondrán en su mitad superior. Finalmente, si quien realizara las conductas anteriormente descritas fuera un agente de las FCS, será de aplicación el art. 198 CP, pudiéndose imponer las penas de los anteriores preceptos en su mitad superior, además de la inhabilitación absoluta de seis a doce años.

2. Excurso: violación del derecho a un proceso con todas las garantías

Relacionado con el ámbito penal por cuanto se vincula al proceso judicial, pero sin constituir ilícito, traemos a colación una cuestión muy interesante que supone un serio problema, especialmente en lo relativo al derecho a un proceso con todas las garantías, previsto en el art. 24.2 CE. Este derecho se ve cercenado cuando no se tiene acceso a la evidencia utilizada en el procedimiento. En tal sentido, cuando se abre un proceso judicial sobre una persona mediante una identificación automática efectuada por el sistema de reconocimiento facial utilizado de forma encubierta, aquel se ve vulnerado. Así las cosas, si no se revela que la detención ha tenido lugar con la utilización de la técnica, el debido proceso no está garantizado[54].

A ello añadimos las identificaciones erróneas y la veracidad que se otorga a la prueba del reconocimiento facial automático para identificar delincuentes peligrosos o conocidos terroristas. En este sentido, la técnica –como se expuso *supra*– no es completamente exacta porque en no pocas ocasiones, como todo instrumento

[51] Esto es así, por cuanto para la consumación delictiva, no es suficiente con la instalación de los artificios técnicos, sino que se requiere la captación, en este caso, de la imagen, para descubrir los secretos de otro o vulnerar su intimidad (lo cual efectivamente tiene lugar con la acción señalada en el texto principal): MUÑOZ CONDE, F. *Derecho Penal. Parte Especial…*, cit., p. 259.

[52] Para esta conducta se prevé una pena de prisión de uno a tres años y multa de doce a veinticuatro meses. Es distinta y complementaria de la establecida en el párrafo primero, siendo, según señala SÁINZ-CANTERO CAPARRÓS, autónoma: "Capítulo 14. Delitos contra la intimidad…", cit., pp. 349 y 350.

[53] El fundamento de la agravación está en la cualidad del autor. El responsable del fichero tiene una posición privilegiada para conculcar el bien jurídico protegido. De este modo, a juicio de GÓMEZ NAVAJAS y, en ello nos mostramos de acuerdo, estamos ante una situación análoga a la posición de garante de los delitos de comisión por omisión, pues quien custodia un fichero tiene la obligación específica de proteger la intimidad de los datos personales que tiene en su poder y cuyo conocimiento indiscreto se pretende evitar: *La protección de los datos personales*…, cit., p. 347.

[54] LEARNED-MILLER, E., y otros. *Facial recognition technologies in the wild…*, cit., p. 12.

informático, falla[55]. En vista de lo inmediatamente señalado, debemos tomar con cautela la utilización del reconocimiento facial con fines de investigación policial, pues no debería aplicarse como prueba decisiva para determinar el destino de un sujeto en el sistema de justicia penal, ya que no es eficaz en todo caso y habría de supervisarse las identificaciones automáticas personalmente, a fin de evitar este tipo de errores que derivan en la iniciación de un procedimiento judicial contra personas inocentes.

IV. CONCLUSIONES

El uso de las nuevas tecnologías se está extendiendo cada vez más y ampliando sus funciones en una sociedad digitalizada que reclama mayores niveles de seguridad. El reconocimiento facial, como todo sistema informático, no es ajeno a este expansionismo, pues se ha implementado ya en varios países con diversos propósitos, principalmente para preservar la seguridad, tanto pública como privada.

Nos encontramos ante una técnica revolucionaria, capaz de captar en cuestión de segundos y entre una gran multitud, el rostro de una persona, cuya identidad se encuentra inserta en una plantilla. Esto puede reportar grandes beneficios de seguridad, pues agiliza a los agentes de las FCS la labor de detección y detención de peligrosos delincuentes, así como la localización de personas desaparecidas. Aun así, los perjuicios que suponen a los derechos y libertades fundamentales son muchos y no se pueden obviar.

Especialmente significativas, las injerencias que conllevan en la intimidad personal, a lo que se añaden otros problemas como los relacionados con el derecho a la no discriminación. De este modo, el ejercicio legítimo de tales derechos entra en colisión con la seguridad ciudadana, ante lo cual nos planteamos qué debe prevalecer en semejante caso. A nuestro juicio, aunque los derechos pueden limitarse bajo determinadas condiciones relacionadas con el principio de proporcionalidad, el reconocimiento facial sobrepasa en mucho dichas condiciones, por lo que no estaría legitimada su implantación en nuestro país, ya que hay otras técnicas menos intrusivas en aquellos para garantizar la seguridad. A lo que hemos de añadir que, en caso de aplicarse, puede utilizarse de forma fraudulenta por las personas encargadas del tratamiento de los datos personales recogidos por este sistema (principalmente empleados del sector privado aunque también los agentes policiales), pudiendo incurrir en los ilícitos de descubrimiento y revelación de secretos, tipificados en el Capítulo I del Título X del Código Penal.

En vista de todo lo señalado hasta el momento, debemos concluir que el sistema de reconocimiento facial con fines de preservación de la seguridad en lugares públicos, no debe ser asumido, al menos hasta que exista una Ley que recoja expresamente los objetivos, límites y condiciones de su utilización, respetando en lo esencial el derecho a la intimidad personal –y demás derechos fundamentales que su uso puede conculcar–. De lo contrario, una utilización inadecuada del mismo puede derivar en serias vulneraciones de aquella que, como bien jurídico tutelado por el Derecho Penal, legitima la intromisión de este último en aras a su protección, cuando sea lesionado de gravedad.

BIBLIOGRAFÍA

BARONA VILAR, S. (2019). "Inteligencia Artificial o la algoritmización de la vida y de la justicia: ¿Solución o problema?". *Revista Boliviana de Derecho*, 28, 18-49.

[55] Igualmente, el programa es fácil de "*hackear*" o alterar para evitar una identificación. Se ha demostrado que ciertos accesorios como sombreros, máscaras y bufandas pueden bloquear o emitir sombras en zonas clave de la cara, haciendo que las identificaciones sean menos fiables: LEARNED-MILLER, E., y otros. *Facial recognition technologies in the wild…*, cit., p. 10. Las identificaciones erróneas no solo se producen por la manipulación del sistema, ya que el mismo tiene un índice de error elevado. De este modo, se ha demostrado que cuatro de cada cinco personas identificadas como sospechosas en Londres, resultan ser inocentes, tal como se extrae del extenso estudio llevado a cabo por el Proyecto sobre Derechos Humanos, *Big Data* y Tecnología de la Universidad de Essex. Véase, en mayor amplitud: FUSSEY, P., y MURRAY, D. (2019). *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. Universidad de Essex.

BREY, P. (2004). "Ethical Aspects of Facial Recognition Systems in Public Places". *Journal of Information, Communication and Ethics in Society*, 2, 97-109.

BUOLAMWINI, J., y GEBRU, T. (2018). "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification". *Proceedings of Machine Learning Research*, 81, 1-15.

CASTELLÓ NICÁS, N. (2015). "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio". En Morillas Cueva, L., (Dir.). *Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015)*. Madrid: Dykinson, 487-514.

COFFIN, J.S., e INGRAM, D. (1999). *Facial recognition system for security Access and identification.* Patente de Estados Unidos, nº 5.991.429. Washington DC: Oficina de Patentes y Marcas de los Estados Unidos.

COTINO HUESO, L. (2017). "Big Data e Inteligencia Artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales". *Dilemata*, 24, 131-150.

CUERDA ARNAU, M.L. (2018). "La reforma de Ley de Enjuiciamiento Criminal en materia de tecnovigilancia. Visión de conjunto". En Alonso Rimo, A., Cuerda Arnau, M.L., y Fernández Hernández, A., (Dirs.). *Terrorismo, sistema penal y derechos fundamentales.* Valencia: Tirant lo Blanch, 507-538.

DE LA MATA BARRANCO, N.J., y BARINAS UBIÑAS, D. (2014). "La protección penal de la vida privada en nuestro tiempo social: ¿necesidad de redefinir el objeto de tutela?". *Revista de Derecho Penal y Criminología*, 3ª Época, 11, 13-92.

DE MIGUEL BERIAIN, I., y PÉREZ ESTRADA, M.J. (2019). "La Inteligencia Artificial en el proceso penal español: un análisis a su admisibilidad sobre la base de los derechos fundamentales implicados". *Revista de Derecho. UNED*, 25, 531-561.

DÍAZ RODRÍGUEZ, V. (2013). "Sistemas biométricos en materia criminal: un estudio comparado". *Revista del Instituto de Ciencias Jurídicas de Puebla*, 31, 28-47.

ESQUINAS VALVERDE, P. (2010). *Protección de datos personales en la Policía Europea.* Valencia: Tirant lo Blanch.

FUSSEY, P., y MURRAY, D., *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, Universidad de Essex, 2019.

GÁLVEZ JIMÉNEZ, A. (2014). "El derecho a la seguridad personal". En Monereo Atienza, C., Monereo Pérez, J.L., y Aguilar Calahorro, A., (Coords.). *El sistema universal de los derechos humanos. Estudio sistemático de la declaración universal de los derechos humanos, el pacto internacional de derechos civiles y políticos, el pacto internacional de derechos económicos, sociales y culturales y textos internacionales concordantes*. Granada: Comares, 393-404.

GIL MEMBRADO, C. (2019). *Videovigilancia y protección de datos. Especial referencia a la grabación de la vía pública desde el espacio privado*. Madrid: Wolters Reuters.

GÓMEZ NAVAJAS, J. (2005). *La protección de los datos personales. Un análisis desde la perspectiva del Derecho Penal*. Navarra: Aranzadi.

HOWARD-HASSMAN, R.E. (2012). "Human Security: Understanding Human Rights". *Human Rights Quarterly*, 34, 88-112.

INIOLUWA, D.R., y otros (2020). "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing". *Actas de la Conferencia AAAI/ACM sobre IA, ética y sociedad*, 145-151.

Instituto Nacional de Ciberseguridad (INCIBE). (2016). *Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario.*

ISHAY, M.R. (2014). *The History of Human Rights: from Ancient Times to the Globalization Era.* University of California Press.

JIMÉNEZ DÍAZ, M.J. (2006). *Seguridad ciudadana y Derecho Penal*. Madrid: Dykinson.

LEARNED-MILLER, E., y otros (2020). *Facial recognition technologies in the wild: a call for a federal office*. MacArthur Foundation.

MANN, M., y SMITH, M. (2017). "Automated Facial Recognition technology: recent developments and approaches to oversight". *University of New South Wales Law Journal*, 40 (1), 121-145.

MIRÓ LLINARES, F. (2018). "Inteligencia Artificial y justicia penal, más allá de los resultados lesivos causados por robots". *Revista de Derecho Penal y Criminología. UNED*, 3ª época, 20, 87-130.

MORILLAS CUEVA, L. (2005). "El Derecho Penal mínimo o la expansión del Derecho Penal". *Revista Cubana de Derecho*, 25, 93-118.

MORILLAS CUEVA, L. (2018). *Sistema de Derecho Penal. Parte General*. Madrid: Dykinson.

MUÑOZ CONDE, F. (2019). *Derecho Penal. Parte Especial*. Valencia: Tirant lo Blanch.

NOAIN SÁNCHEZ, A. (2016). "La protección de la intimidad y vida privada en Internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)". *Premio de Protección de Datos Personales de Investigación 2015*. Madrid: Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del Estado.

Observatorio de la Seguridad de la Información. (2011). *Estudio sobre las tecnologías biométricas aplicadas a la seguridad*. Ministerio de Industria, Turismo y Comercio.

PIÑAR MAÑAS, J.L. (2009). *Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio*. *Documento de Trabajo 147/2009*, Laboratorio de Alternativas, 147.

RIGANO, C. (2019). "Using Artificial Intelligence to address criminal justice needs". *National Institute of Justice*, 208, 1-10.

SÁINZ-CANTERO CAPARRÓS, J.E. (2020). "Capítulo 14. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I)". En Morillas Cueva, L., (Dir.). *Sistema de Derecho Penal. Parte Especial*. Madrid: Dykinson, 337-367.

SUÁREZ LÓPEZ, J.M. (2015). "Los principios limitadores del *ius puniendi* en un Estado social y democrático de Derecho y su incidencia en la represión penal del dopaje en el deporte". En Benítez Ortúzar, I.F., (Coord.). *Tratamiento jurídico penal y procesal del dopaje en el deporte*. Madrid: Dykinson, Madrid, 101-129.

YANG, W., WANG, S., HU, J., ZHENG, G., y VALLI, C. (2019). "Security and Accuracy of Fingerprint-Based Biometrics: A Review". *Symmetry*, 11 (141), 1-19.

WEBGRAFÍA

CAIXA BANK. (2020). *CaixaBank inicia el despliegue de los cajeros con tecnología de reconocimiento facial por toda España*, 6 de junio, recurso electrónico obtenido a través de la Web: https://www.caixabank.com/comunicacion/noticia/caixabank-inicia-el-despliegue-de-los-cajeros-con-tecnologia-de-reconocimiento-facial-por-toda-espana_es.html?id=42302#, (consultado por última vez el día 6 de agosto de 2020).

COLLINS, J. (2019). "China is using facial recognition to track millions of Muslim citizens wherever they go". *Quartz*, 17 de febrero, recurso electrónico obtenido a través de la Web: https://qz.com/1552708/china-

is-using-facial-recognition-to-track-millions-of-muslim-citizens-wherever-they-go/, (consultado por última vez el día 1 de septiembre de 2020).

CONGER, K., FAUSSET, R., y KOVALENSKI, S.F. (2019). "San Francisco Bans Facial Recognition Technology". *New York Times*, 14 de mayo, recurso electrónico obtenido a través de la Web: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html, (consultado por última vez el día 15 de agosto de 2020).

DEB, S., y SINGER, N. (2018). "Taylor Swift Said to Use Facial Recognition to Identify Stalkers". *New York Times,* 13 de diciembre, recurso electrónico obtenido a través de la Web: https://www.nytimes.com/2018/12/13/arts/music/taylor-swift-facial-recognition.html, (consultado por última vez el día 24 de agosto de 2020).

JAKHAR, P. (2020). "Coronavirus: las innovadoras tecnologías que está utilizando China para combatir el COVID-19 (y las preocupaciones que plantean). *BBC*, 4 de marzo, recurso electrónico obtenido a través de la Web: https://www.bbc.com/mundo/noticias-51736635, (consultado por última vez el día 20 de agosto de 2020).

LABORDE, A. (2020). "Detenido injustamente un afroamericano en EE UU por un error en el sistema de reconocimiento facial". *El País*, 26 de junio, recurso electrónico obtenido a través de la Web: https://elpais.com/tecnologia/2020-06-26/un-afroamericano-es-detenido-injustamente-por-un-error-en-el-sistema-de-reconocimiento-facial.html, (consultado por última vez el día 24 de agosto de 2020).

LEE, D. (2019). "San Francisco is first US city to ban facial recognition". *BBC News*, 15 de mayo, recurso electrónico obtenido a través de la Web: https://www.bbc.com/news/technology-48276660, (consultado por última vez el día 30 de agosto de 2020).

NAVARRO, B. (2020). "IBM y Amazon abjuran de la tecnología de reconocimiento facial por su sesgo racista", *La Vanguardia,* 16 de junio, recurso electrónico obtenido a través de la Web: https://www.lavanguardia.com/internacional/20200611/481710398480/ibm-reconocimiento-facial-racismo-tecnologia-negros.html, (consultado por última vez el día 18 de agosto de 2020).

ORTEGA, E. (2020). "En España ya se está utilizando el reconocimiento facial, ¿sabes dónde?". *Computer hoy*, 6 de julio, recurso electrónico obtenido a través de la Web: https://computerhoy.com/reportajes/tecnologia/lugares-espana-ya-utilizan-reconocimiento-facial-547573, (consultado por última vez el día 10 de agosto de 2020).

RUBIO, I. (2020). "Protección de Datos abre una investigación sobre las cámaras de vigilancia facial de Mercadona". *El País*, 6 de julio, recurso electrónico obtenido a través de la Web: https://elpais.com/tecnologia/2020-07-06/proteccion-de-datos-abre-una-investigacion-sobre-las-camaras-de-vigilancia-facial-de-mercadona.html, (consultado por última vez el día 6 de agosto de 2020).

VIDAL LIY, M. (2019). "2,5 millones de personas en China, bajo el control de una empresa de vigilancia facial". *El País*, 18 de febrero, recurso electrónico obtenido a través de la Web: https://elpais.com/internacional/2019/02/17/actualidad/1550422679_515333.html, (consultado por última vez el día 10 de agosto de 2020).

LEGISLACIÓN

Declaración Universal de Derechos Humanos, adoptada y proclamada por la Asamblea General de las Naciones Unidas en su resolución 217 A (III), de 10 de diciembre de 1948.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Libro Blanco sobre la Inteligencia Artificial: un enfoque europeo orientado a la excelencia y la confianza, de la Comisión Europea, COM(2020) 65 final.

Constitución Española, BOE núm. 311, de 29 de diciembre de 1978.

Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.

Ley 5/2014, de 4 de abril, de Seguridad Privada.

RD 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte.

INFORMES

Grupo del 29, *Documento de Trabajo sobre Biometría*, adoptado el 1 de agosto de 2003.

AEPD: *Prevalencia en el ejercicio de derechos. Informe Jurídico 0117/2007.*

Informe 36/2020, de 8 de mayo de 2020, sobre la utilización de técnicas de reconocimiento facial en la realización de pruebas de evaluación online.

Informe 10308/2019, de 28 de mayo de 2020, sobre el uso de sistemas de reconocimiento facial por parte de las empresas de seguridad privada.

Guía sobre el uso de videocámaras para seguridad y otras finalidades, última modificación del día 18 de junio de 2020.

APÉNDICE JURISPRUDENCIAL

Tribunal Constitucional

ATC (Sala Segunda) 57/2007 de 26 de febrero [RTC 2007/57].

STC (Sala Primera) 325/1994 de 12 de diciembre [RTC 1994/325],

STC (Pleno) 209/2000 de 30 de noviembre [RTC 2000/290].

STC (Pleno) 292/2000 de 30 de noviembre [RTC 2000/292].

STC 14/2003 de 28 de enero [2003/14].

STC (Pleno) 151/2014 de 25 de septiembre [RTC 2014/151]

STC (Pleno) 58/2018 de 4 de junio [RTC 2018/58].

STC (Pleno) 76/2019 de 22 de mayo [RTC 2019776].

Tribunal Supremo

STS (Sala de lo Contencioso-Administrativo, Sección 7ª) de 2 de julio de 2007 [RJ/2007/6598].

STS (Sala de lo Social) 96/2017 de 2 de febrero [RJ/2017/1628].

STS (Sala de lo Penal, Sección 1ª) 412/2020 de 20 de julio [JUR 2020/235172].

Tribunal Superior de Justicia

STSJ de Murcia (Sala de lo Social, Sección 1ª) de 25 de enero [AS/2010/165].