El reconocimiento facial, la tecnología biométrica del presente

La serie británica de ciencia ficción Black Mirror[1] cada vez se asemeja más a la realidad. Esta serie gira entorno a cómo la tecnología afecta a nuestras vidas, e ilustra sistemas de tratamiento de información que no sólo se utilizan ya actualmente, sino que su uso se ha visto incrementado de forma exponencial estos últimos años, como es el caso del reconocimiento facial. En los últimos meses se ha hablado mucho de la utilización del reconocimiento facial para distintos propósitos. No estamos hablando de que el reconocimiento facial sea tecnología nueva ya que su origen se remonta entorno al 1960. Lo realmente novedoso son las distintas finalidades e incluso los usos que se están explorando con esta tecnología. Tras años de maduración y perfeccionamiento de esta tecnología ha crecido la inquietud, no sólo de las organizaciones públicas, sino también de las privadas, para la utilización del reconocimiento facial con finalidades que van desde la seguridad, hasta la mejora de la experiencia del usuario de un servicio en sus distintas variantes, permitiendo, para citar algunos meros ejemplos, la realización de pagos a través de un smartphone mediante dicha tecnología, o posibilitando el etiquetado automático de fotografías en una red social, la mejora en la agilidad de algunos trámites, entre muchos otros.

¿Qué es el reconocimiento facial exactamente?

El reconocimiento facial es una técnica que posibilita la extracción de un dato biométrico que permite identificar de forma unívoca a los individuos. Los datos biométricos responden a rasgos físicos o comportamentales de los mismos. Existen distintos datos biométricos en nuestro cuerpo como la huella dactilar, el iris, la voz, la geometría de la mano, o incluso la forma de andar o teclear, entre otros. Un dato biométrico, como los mencionados anteriormente, es obtenido a través de la utilización de una tecnología denominada "tecnología biométrica" o "biometría", que mediante sensores es capaz de extraer y analizar parámetros de nuestro cuerpo. A modo de dato anecdótico, el Samsung Galaxy S9 llega a leer hasta 100 puntos distintos de nuestro rostro, combinando esta información con la de su lector de iris[2].

La tecnología biométrica es en definitiva un método que posibilita el reconocimiento de personas a través de sus características físicas, fisiológicas o de comportamiento a partir de la extracción y análisis de dato biométrico resultante, que permite identificar o confirmar la identidad única de una persona[3]. Con ello, en la medida en que el resultado de los datos obtenidos mediante tecnología biométrica permite la identificación inequívoca de un sujeto, es posible confirmar que se lleva a cabo un tratamiento de datos de carácter personal.

---

[1] *Black Mirror (2019, 5 de octubre) Wikipedia, La enciclopedia libre. Fecha de consulta: octubre 10, 2019 desde: https://es.wikipedia.org/wiki/Black_Mirror*

[2] *Tu cara me suena. Te contamos qué hay detrás del reconocimiento facial (2019, 5 de octubre). Fecha de consulta: octubre 10, 2019 desde: https://bloygo.yoigo.com/tecnologia/tu-cara-me-suena-te-contamos-que-hay-detras-del-reconocimiento-facial_29722795.html*

[3] *INCIBE (2016) Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario. Pág. 1*

Los datos biométricos, distintos al resto de datos personales

La gran particularidad de los datos biométricos en general es que son universales porque se extraen de rasgos físicos o biológicos presentes o latentes, generalmente, en todo individuo y a partir del mismo se extraen propiedades únicas de un individuo que en condiciones normales perduran con el paso del tiempo[4]. La tecnología biométrica nos permite captar dichos rasgos únicos de una persona y poder identificarla de forma directa.

Dependiendo de la tecnología biométrica utilizada, los parámetros a considerar son distintos: la voz, la imagen facial, los surcos de la huella dactilar, etc. De dichos rasgos se puede extraer un patrón único para cada persona[5].

La utilización de una u otra tecnología marcará si debemos hablar de datos biométricos dinámicos, estáticos o multimodales. Los primeros, son datos obtenidos a través de tecnologías de comportamiento que comparan acciones o movimientos, como por ejemplo los latidos del corazón.[6] Los segundos, cuando se utilizan tecnologías fisiológicas que miden y comparan rasgos físicos, como por ejemplo el reconocimiento del iris y los terceros cuando son la combinación de ambas tecnologías[7], como es el reconocimiento de la persona a partir de la voz y el reconocimiento facial.

Los avances tecnológicos en el campo de la biometría aumentan la fiabilidad de la utilización de tecnologías maduras como son la huella dactilar, la geometría de la mano, el reconocimiento del iris y el reconocimiento facial, en combinación con datos biométricos basados en la utilización de rasgos de comportamiento e incluso patrones psicológicos. A modo de ejemplo, podemos citar la tecnología utilizada en algunas clases en China que a partir del reconocimiento facial y las expresiones de la misma puede determinarse el estado de ánimo de una persona o su atención.

Diferencias entre el reconocimiento de huella dactilar y el reconocimiento facial

Podemos afirmar que la huella dactilar ha sido el dato biométrico más utilizado y extendido en los últimos años, tanto en organizaciones públicas como privadas, para finalidades no sólo de seguridad (control de acceso), sino también en muchos casos para el control laboral (control de ausencias y asistencia). El tratamiento de la huella dactilar ha llegado a gran cantidad de sectores, especialmente en las empresas tras la reforma laboral al incorporar la obligación del fichaje[8].

---

[4] *La información biométrica y los datos biométricos (2017) La base científica de los sistemas automatizados de identificación mediante Biometría. Aranzadi: Estudios Tecnologías biométricas, identidad y Derechos fundamentales. BIB 2017/4666*

[5] *INCIBE (2016) Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario. Pág. 5*

[6] *https://empresas.blogthinkbig.com/pulseid-los-latidos-del-corazon-la-proxima-contrasena/*

[7] *INCIBE (2016) Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario. Pág. 6*

[8] *Pascual Cortés, R. Así será la reforma para que todos los empleados fichen a diario en el trabajo (2018, 28 de noviembre) Fecha de consulta: octubre 1, 2019 desde: https://cincodias.elpais.com/cincodias/2018/11/27/midinero/1543333532_687470.html*

Pero las tecnologías también son víctimas de modas y tendencias. Actualmente el reconocimiento facial parece ser la tecnología biométrica favorita. El auge por el reconocimiento facial aumenta año a año y cabe preguntarnos si aún tratarse de datos biométricos ambos, son iguales los sistemas basados en el reconocimiento del rostro y los basados en el reconocimiento de huellas dactilares.

El reconocimiento a partir de la huella dactilar utiliza las crestas o surcos presentes en la superficie de los dedos que disponen de un diseño único. La utilización de esas minucias o el patrón global nos permite identificar a una persona con un gran grado de precisión[9]. Pero la huella dactilar, no permite analizar datos que van más allá de las características físicas de la propia huella.

En cambio, el reconocimiento facial permite identificar a una persona mediante una imagen, vídeo o fotografía utilizando programas de cálculo que analizan parámetros extraídos de los rostros humanos. Cabe diferenciar que las imágenes obtenidas a partir de un sistema de videovigilancia, si bien son datos personales, no conlleva necesariamente el tratamiento de datos biométricos salvo que la propia cámara incorpore una tecnología específica de reconocimiento facial, y ello no sucede la gran mayoría de ocasiones. Un sistema de videovigilancia sólo proporciona la imagen de una persona, pero no conlleva *per se* la extracción del patrón biométrico del rostro de un individuo. Si bien en ambos casos la imagen, en la medida en que identifique o pueda identificar a un individuo, conlleva el tratamiento de datos personales, sólo en el caso en que se lleve a cabo el reconocimiento facial aumentará la sensibilidad del dato y por ende las cautelas que debe asumir el responsable del tratamiento (empresa propietaria de las imágenes) deberán ser sustancialmente superiores. Únicamente hablaremos de que se trata de un reconocimiento facial si se combina la videovigilancia con tecnología de reconocimiento facial que permite la identificación de una persona a través de la utilización de programas de cálculo que analizan las imágenes de los rostros captados y permiten su identificación de manera automatizada[10].

Ciertamente, ambos sistemas se basan en la identificación mediante parámetros físicos únicos para comprobar la identidad de una persona. Parecería a simple vista, que la utilización de uno u otro para llevar a cabo la identificación de un individuo, para el desbloqueo de un móvil, el fichaje de trabajadores o el control de acceso, es una decisión de preferencia por parte del responsable del tratamiento.

Sin embargo, no es así. No es una cuestión baladí que nuestra imagen y la imagen de nuestro rostro se encuentra almacenada en múltiples lugares debido al amplio y extendido uso de videovigilancia, tanto en lugares públicos, como sucede en las calles más transitadas de ciudades como Barcelona o Londres, edificios públicos, museos etc. Así como también, en espacios privados como tiendas de ropa, aparcamientos o bancos. El uso combinado de ambas tecnologías, videovigilancia y reconocimiento facial abre muchas más puertas y supone una

---

[9] *INCIBE (2016) Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario. Pág. 7*

[10] *INCIBE (2016) Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario. Pág. 8*

información muy valiosa, ya que es posible analizar no sólo datos físicos del rostro como pasa con la videovigilancia, sino también comportamentales como las expresiones. ¿Has calculado alguna vez cuantas cámaras de videovigilancia captan tu imagen desde que te levantas hasta que te vas a dormir? Pues bien, por unos instantes trata de imaginar qué sucedería si estas cámaras de videovigilancia ya existentes en nuestras calles, dispusieran de tecnología de reconocimiento facial.

Una solución de inteligencia artificial podría saber todo nuestro día a día, organizaciones políticas, deportivas o religiosas a las que pertenecemos, las tiendas a las que hemos ido a comprar, las veces que hemos salido de casa durante el día, etc. Este nivel de detalle que da dicha información acerca de nuestra esfera privada sería de un valor mayúsculo para las empresas y gobiernos, pero sin duda supondría una gran intromisión en la vida privada de las personas, provocando inevitablemente un cambio importante en el significado de lo que se conoce hoy como intimidad o vida privada[11]. Esta situación, que parece de ciencia ficción, ya sucede en distintas ciudades de otros continentes[12].

¿Dónde se usa el reconocimiento facial?

El aumento en el uso de dicha tecnología, el grado de intrusión a la intimidad que supone la utilización de esta tecnología para determinados fines, y los errores conocidos derivados de esta tecnología, han llevado al reconocimiento facial al punto de mira de la regulación mundial.

Observando los últimos años, podemos ver que varias Administraciones Públicas han optado para poner en funcionamiento el reconocimiento facial en sus localidades. El sueño de todo municipio es conseguir detectar a sospechosos antes de cometer el delito, tal como mostraba la película de ciencia ficción “Minority Report” (2002) de Steven Spielberg.

Sin embargo, los resultados actuales no han sido demasiado esperanzadores. Veamos algunos ejemplos. La primera polémica estalló en 2015 cuando el algoritmo de una de las principales empresas tecnológicas, confundió a una pareja de tez oscura, con gorilas[13]. En el año 2017 el sistema de reconocimiento facial fue utilizado para el festival de Elvis en la ciudad de Porthcawl. En dicho evento se probó una tecnología de reconocimiento facial para realizar el seguimiento efectivo de delincuentes. Dichas cámaras detectaron 17 individuos como posibles sospechosos y de estos, diez eran correctos positivos y siete eran falsos positivos, según the Wired[14]. En 2018,

---

[11] *Reconocimiento facial, seguridad y derecho a la privacidad* *https://www.reglamentodatos.es/index.php/blog/170-reconocimiento-facial-seguridad-y-derecho-a-la-privacidad*

[12] *RECONOCIMIENTO FACIAL, SEGURIDAD Y DERECHO A LA PRIVACIDAD (2019, 24 de julio) Blog: Curso de Experto, Especialista y Máster en el Reglamento General de Protección de Datos de la UNED. Fecha de consulta: octubre 4, 2019 desde.* *https://www.lavanguardia.com/tecnologia/20190518/462270404745/reconocimiento-facial-china-derechos-humanos.html*

[13] *BBC (25 de julio de 2015).Google pide perdón por confundir a una pareja negra con gorilas* *https://www.bbc.com/mundo/noticias/2015/07/150702_tecnologia_google_perdon_confundir_afroamericanos_gorilas_lv*

[14] *Burgess, M. (2018, mayo 4) Facial recognition tech used by UK police is making a ton of mistakes. Fecha de consulta: octubre 4, 2019 desde: https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival*

el reconocimiento facial de Amazon confundió a 28 congresistas con sospechosos[15] y a ello debemos añadirle que un reciente estudio independiente realizado por los investigadores Pete Fussey y Daragh Murray de la Universidad de Essex, sobre el sistema de reconocimiento facial de la policía Metropolitana de Londres ha determinado que el mismo tiene una tasa de falsos positivos del 81%[16].

Debido a los fallos presentados por dicha tecnología y las distintas implicaciones en la privacidad, San Francisco fue en mayo de 2019 la primera ciudad de los Estados Unidos en prohibir el reconocimiento facial a través de cámaras, en ámbitos de su competencia como la policía local y las autoridades de transporte [17]. La prohibición del reconocimiento facial llego también, al cabo de pocos meses, a los municipios de Somerville en Massachussets y Oakland en California vetando el uso de dicha tecnología en espacios públicos[18].

Pero el afán de Estados Unidos para restringir la propagación del uso del reconocimiento facial no acaba aquí. El Tribunal de Apelaciones del Noveno circuito de San Francisco falló en agosto de 2019 en contra de la multinacional Facebook por la utilización de tecnología de reconocimiento facial sin el consentimiento de los interesados[19], considerando que dicho tratamiento invadía los asuntos privados y los intereses concretos del individuo.

Mas recientemente, en octubre de 2019, el mismo estado de California presentó un Proyecto de ley histórico en EEUU, en aras de impedir el uso del reconocimiento facial y otra vigilancia biométrica con fines policiales en dicho estado. Con este Proyecto de Ley se pretende "detener la expansión de un estado de vigilancia que presenta una amenaza sin precedentes" para los derechos y las libertades de las personas[20].

Sin embargo, no todos los países se muestran reticentes a la invasión de privacidad que puede ocasionar el reconocimiento facial. Al otro extremo, encontramos a China que ya dispone de una red de más de 170 millones de cámaras de seguridad con las que utiliza el reconocimiento

---

[15] Rubio, I. (2019, mayo 21) Reconocimiento Facial: La Tecnología Que Lo Sabe Todo. Fecha de consulta: octubre 4, 2019 desde https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html

[16] La Tecnología De Reconocimiento Facial De La Policía De Londres Se Equivoca Cuatro De Cada Cinco Veces - R3d: Red En Defensa De Los Derechos Digitales. Fecha de consulta: octubre 1, 2019 desde https://r3d.mx/2019/07/04/la-tecnologia-de-reconocimiento-facial-de-la-policia-de-londres-se-equivoca-cuatro-de-cada-cinco-veces/

[17] Miró, X. (2019, mayo 15), San Francisco prohibeix l'ús de la tecnología de reconexement facial a la policía. Fecha de consulta: octubre 4, 2019 desde: https://www.ccma.cat/324/san-francisco-prohibeix-lus-de-la-tecnologia-de-reconeixement-facial-a-la-policia/noticia/2922116/ i https://elpais.com/tecnologia/2019/05/15/actualidad/1557904606_766075.html

[18] Oakland Es La Tercera Ciudad En Ee.uu. En Prohibir El Reconocimiento Facial - R3d: Red En Defensa De Los Derechos Digitales. Fecha de consulta: octubre 4, 2019 desde https://r3d.mx/2019/07/17/oakland-es-la-tercera-ciudad-en-ee-uu-en-prohibir-el-reconocimiento-facial/

[19] Europa Press (9 de agosto de 2019). Un Tribunal Falla Contra El Reconocimiento Facial De Facebook, desde: https://www.lavanguardia.com/tecnologia/actualidad/20190809/463950823806/facebook-condena-reconocimiento-facial-patel.html

[20] EFE (10 de agosto de 2019). Aplauden veto a reconocimiento facial en las cámaras de la policía en Californa https://www.efe.com/efe/usa/politica/aplauden-veto-a-reconocimiento-facial-en-camaras-de-la-policia-california/50000105-4083420

facial para evaluar el comportamiento de sus ciudadanos y empresas, y así, puntuar dicho comportamiento para determinar qué crédito social merecen. Según la puntuación obtenida, las empresas y los ciudadanos pueden clasificarse como fiables o indignos de confianza que, en este último caso, supone desventajas, sanciones y trabas para acceder a cualquier tipo de ventaja ofrecida por la administración[21]. De forma más resciente, algunas ciudades chinas han empezado a utilizar el reconocimiento facial en farmacias, para luchar contra el abuso de drogas y sustancias[22]; o simplemente al tratar adquirir un terminal móvil [23]

No obstante, no debemos pensar que la tecnología del reconocimiento facial sólo es utilizada por China. En lo que respecta al sector privado la cosa es distinta. En Estados Unidos está siendo utilizada por algunas tiendas para evitar la entrada a individuos con antecedentes por hurto o también es usual su utilización en grandes eventos como es el caso del concierto de 18 de mayo de 2018 de la conocida cantante Taylor Swift en Los Angles, que utilizó reconocimiento facial para detectar acosadores sin que dicho extremo fuese conocido por sus fans[24]. Esta tecnología también es utilizada por otros países como Japón o Suecia a los que pronto parece que se les unirá Francia que pretende utilizar dicha tecnología para crear un ID digital llamado Alicem[25].

La visión de Europa respecto al reconocimiento facial

La Unión Europea tampoco queda inmune de la utilización de esta tecnología. En abril de 2019, el Parlamento de la Unión Europea aprobaó la creación de una base de datos biométricos, huella dactilar o reconocimiento facial, de los ciudadanos dentro de la Unión con la supuesta intención de aumentar la seguridad a través de la obtención de los datos biométricos de los ciudadanos de la Unión para su identificación, así como también la de los ciudadanos extranjeros que pretendan ingresar en el espacio Schengen para, según se describe, detectar posibles terroristas[26].

---

[21] *TV3 "ciutadans Per Punts", O Com La Xina Vigila Els Seus Habitants, a "30 Minuts"* https://www.ccma.cat/tv3/30-minuts/ciutadans-per-punts-a-30-minuts/noticia/2946594/

[22] *ElPaís.cr "Shanghái prueba terminales con reconocimiento facial en farmacias para luchar contra el abuso de drogas* https://www.elpais.cr/2020/01/17/shanghai-prueba-terminales-con-reconocimiento-facial-en-farmacias-para-luchar-contra-el-abuso-de-drogas/

[23] *BBC "La polémica en China por la imposición del reconocimiento facial a todos los compradores de teléfonos"* https://www.bbc.com/mundo/noticias-50622301

[24] *Zhou, M. (2018, diciembre 13). Taylor Swift utilizaría Reconocimiento Facial Para Identificar a Los Acosadores.* Fecha de consulta: octubre 2, 2019 desde *desde:* https://www.cnet.com/es/noticias/taylor-swift-reconocimiento-facial-acosadores/

[25] *Fernandez, M. (2019, octubre 3). Tu Cara Será Tu Dni: Francia Usará El Reconocimiento Facial Como Identificación*. Fecha de consulta: octubre 2, 2019 desde*:* https://www.elespanol.com/omicrono/20191003/cara-dni-francia-usara-reconocimiento-facial-identificacion/433956963_0.html

[26] *Arago, L. (2019, febrero 25). Europa Fortifica Sus Fronteras Digitales*. Fecha de consulta: octubre 1, 2019 desde *desde:* https://www.lavanguardia.com/internacional/20190225/46612119143/europa-fortifica-fronteras-base-datos-ciudadanos-extranjeros.html

De forma más particular, a principios de 2020, Londres anunció que comenzaría a implementar el sistema de reconocimiento facial "en vivo", en algunas calles de la ciudad con fines de seguridad.[27]

La utilización de la tecnología de reconocimiento facial no ha hecho más que empezar y avanza a gran velocidad moviendo un gran volumen de negocio que se prevé que ascienda a 1.200 millones de dólares este año[28].

La regulación del reconocimiento facial

A nivel europeo, la protección de datos viene de la mano de la regulación del Reglamento General de Protección de Datos que resultó de plena aplicación en mayo de 2018. El mismo, ante el auge de la utilización de la tecnología biométrica quiso proporcionar una mayor protección a estos datos y los calificó de categoría especial en su artículo 9. La especialidad de los datos biométricos junto con otros como son los datos de salud, filiación sindical, religión etc. reside en que, de buenas a primeras, el Reglamento en el apartado del artículo mencionado, establece la prohibición general para la utilización de estos.

Posteriormente, en su apartado segundo tipifica las excepciones que levantan dicha prohibición general. Entre las excepciones reguladas, cabe destacar el consentimiento explícito del interesado, el cumplimiento de obligaciones y ejercicio de derechos específicos del responsable o del interesado en el ámbito laboral y de la seguridad y protección social, así como también, por razones de interés público siempre y cuando sea proporcional al objetivo perseguido, entre otros. Sin embargo, el Reglamento ha dejado la puerta abierta, en el apartado cuarto para que los Estados puedan introducir condiciones adicionales o limitaciones a las existentes.

Cabe plantearnos si es suficiente que se dé una de las excepciones para el tratamiento de datos biométricos. Para la utilización de dichos datos no únicamente debe darse un supuesto que deshabilite la prohibición general, sino que también, deberá tratarse de un tratamiento que disponga de base legal suficiente y haya superado con creces el juicio de proporcionalidad, necesidad e idoneidad conforme al principio de minimización de los datos recogido en el propio Reglamento.

Así que, para valorar si los distintos usos y finalidades del reconocimiento facial son conformes a la legislación europea, deberá tenerse en cuenta, entre otros, qué riesgos supone, cuál puede ser su impacto para los derechos y libertades de los interesados, y qué beneficios supone su implementación y en qué circunstancias se implementa. En esta misma línea, Grupo de Trabajo del artículo 29 (Actualmente denominado Comité Europeo de Protección de Datos) en el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas ya trasladaba unas directrices para ponderar la proporcionalidad de una tecnología biométrica:

---

[27] *El País (24 de enero de 2020) La policía de Londres se dispone a usar las polémicas cámaras de reconocimiento facial* https://elpais.com/tecnologia/2020/01/24/actualidad/1579883409_559518.html

[28] *Reconocimiento Facial, Seguridad Y Derecho A La Privacidad*. Fecha de consulta: octubre 4, 2019 desde: https://www.reglamentodatos.es/index.php/blog/170-reconocimiento-facial-seguridad-y-derecho-a-la-privacidad

"*Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar. Un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado."*

Primeros posicionamientos administrativos y judiciales europeos sobre el reconocimiento facial

Es importante realizar dicho juicio de proporcionalidad de manera objetiva, en caso de quererse implementar dicha tecnología, ya que recientemente una escuela en Suecia ha sido multada con una sanción de alrededor 19.000 euros por utilizar tecnología de reconocimiento facial para controlar la asistencia de los estudiantes en clase por considerar que no era una medida proporcionada[29]. En lo que respecta a España, cabe apuntar que un centro educativo público de Badalona está utilizando este mismo sistema con dicha misma finalidad[30] y la Autoridad Catalana de Protección de Datos ha iniciado de oficio una investigación sobre el caso.

Ante la incertidumbre global acerca de la tecnología de reconocimiento facial, la Comisión Europea se está planteando la posibilidad de regular derechos explícitos para los ciudadanos sobre el uso de sus datos biométricos obtenidos a través de esta tecnología. El objetivo pasaría por limitar el uso indiscriminado de esta tecnología por parte de las empresas y autoridades públicas, según declaraciones de funcionarios realizadas en Financial Times[31].

En 2020, la Comisión Europea se plantea la posibilidad de prohibir el uso de a tecnología de reconocimiento facial durante un período de hasta cinco años en lugares públicos con el fin de avanzar en la regulación, la evaluación de impacto y en el desarrollo de soluciones que mitiguen los riesgos que puede suponer dicha tecnología. Esta idea se recoge en un borrador de un libro

---

[29] *Mu, M. (2019, agosto 28). Llega El Reconocimiento Facial a Las Escuelas... Y Las Multas Por 'espiar' a Estudiantes desde:* https://www.elconfidencial.com/tecnologia/2019-08-29/reconocimiento-facial-multa-gdpr-suecia_2197399/

[30] *Asenjo, A. (2019, setiembre 29). Un Instituto Catalán Está Usando Reconocimiento Facial Para Controlar La Asistencia a Clase, Algo Por Lo Que Ha Sido Multado Con 19.000 Euros Un Colegio Sueco. .* Fecha de consulta: octubre 4, 2019 desde*:* https://www.businessinsider.es/instituto-catalan-usa-reconocimiento-facial-asistencia84683?utm_source=Twitter&utm_medium=referral&utm_campaign=Botones_sociales

[31] *Khan, M. (2019, agosto 22). EU Plans Sweeping Regulation Of Facial Recognition*. Fecha de consulta: octubre 4, 2019 desde*:* https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9?segmentid=acee4131-99c2-09d3-a635-873e61754ec6

en blanco sobre inteligencia artificial que presentará su versión final el mes de febrero de 2020, como parte de una revisión más amplia de la regulación sobre inteligencia artificial.[32]

Conclusiones

No existe duda acerca del carácter imparable de esta tecnología y del amplio abanico de usos que proporciona. De hecho, los avances tecnológicos son buenos y positivos en una sociedad y como norma general no resulta oportuno pensar que hay que poner límites a la tecnología. Sin embargo, el uso extendido e ilimitado del reconocimiento facial puede acarrear consecuencias irreversibles en la sociedad atendiendo a la numerosa y sensible información que dicha tecnología permite recabar.

El reconocimiento facial ha vuelto a abrir, una vez más si cabe, el duelo entre la seguridad y la privacidad. Sin duda esta tecnología proporciona a los Gobiernos un nuevo sistema para la detección de criminales y terroristas, pero es importante realizar un correcto juicio de ponderación para determinar si una tecnología, aparte de ser eficaz, resulta adecuada. Más allá de los posibles errores técnicos y del grado de fiabilidad que actualmente ofrece, para determinar si el reconocimiento facial es una tecnología adecuada habrá analizar y concluir que no existen medios menos intrusivos para obtener la finalidad perseguida.

Si bien el uso de ésta tecnología con fines policiales resulta improbable de justificar en términos de proporcionalidad, no es descartable que existan situaciones que pudieran justificar una implementación parcial y temporal para un fin muy concreto.

Pero el uso del reconocimiento facial no se limita en el sector público. En el sector privado, hay empresas que desean utilizar dicha tecnología no sólo para fines de seguridad sino para conocer determinada información de sus clientes o usuarios, permitiendo esta tecnología conocer el grado de satisfacción o interés analizando las expresiones del rostro, grado de atención sobre los productos, el color de vestimenta predominante en una persona o incluso la talla aproximada de su ropa.

Todos estos usos, permiten a empresas y organizaciones acceder a grandes volúmenes de información relevante para su día a día. Pero el aspecto principal radica en cómo utilizar esta tecnología sin colisionar con la intimidad de las personas.

Existen tecnologías, como el reconocimiento facial, que parecen haber llegado en nuestra sociedad para quedarse. Los beneficios que otorgan esta y otras tecnologías son muchos, pero el gran reto de los legisladores, en particular el europeo, consistirá en poder regular esta tecnología, tratando de no sesgar el desarrollo natural de las sociedades, pero teniendo en cuenta los derechos y libertades de los ciudadanos, tanto los que pueden ser vistos vulnerados actualmente, como los que podrían serlo en un futuro tas la maduración de la tecnología.

---

[32] *El País "La UE plantea prohibir hasta cinco años el reconocimiento facial en lugares públicos"* https://elpais.com/tecnologia/2020/01/17/actualidad/1579243471_725904.html

Marta Suru, Abogada

Eduard Blasi, Abogado y Profesor en Univeridad Oberta de Catalunya (UOC)