Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

Agencia Española de Protección de Datos AEPD, Comisión Nacional de los Mercados y la Competencia CNMC, Ministerio de Consumo, Centro Criptológico Nacional del CNI,

Mercadona y AnyVision por solicitud publicada en www.cita.es/apedanica-reconocimiento-facial.pdf
https://twitter.com/miguelgallardo/status/1279442951471599616

La **Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA**, por su representante legal Dr. Miguel Gallardo, ha tenido conocimiento de que la cadena de supermercados MERCADONA ya está utilizando tecnología de reconocimiento fisonómico ANYVISION sin que exista una normativa, ni una autoridad que garantice efectivamente, al menos, la seguridad jurídica e interdicción de la arbitrariedad para:
1º Empresas especializadas en tecnologías de reconocimiento facial que compiten con AnyVision, como es el caso de Cognitec, Gemalto, Hikvision, Idemia, Microsoft o NEC y, en España, “La Tienda del Espía”.
2º Ciudadanos afectados por cualquier uso de las tecnologías de reconocimiento facial, tanto por entidades privadas, como por cuerpos y fuerzas de la Seguridad del Estado que se relacionen con ellas.
3º Supermercados y comercios que compiten con MERCADONA sin que se hayan atrevido a instalar nada parecido a ANYVISION, todavía.

APEDANICA está recomendando, a la vista de las recientes noticias, que todos los afectados, particulares y empresas, inicien procedimientos de **reclamación patrimonial contra las Administraciones Públicas** que resulten responsables de la seguridad jurídica y la interdicción de la arbitrariedad por la que pudieran resultar perjudicados no solamente por cualquier uso indebido de datos personales, sino también por el coste de oportunidad de quienes son más prudentes y no experimentan con tecnologías intrusivas sin garantizar previamente su privacidad y su seguridad. En principio, entendemos que el Delegado de Protección de Datos de MERCADONA es responsable de cuanto actualmente esté identificando rostros mediante tecnología de AnyVision, o cualquier otra.

Por lo expuesto, como mejor proceda solicitamos información sobre las responsabilidades según la normativa aplicable a la identificación facial en comercios y grandes superficies, con precisa identificación de sus autoridades responsables, que deben estar personalmente expuestos a las mismas tecnologías que utilizan, y solicitamos un interlocutor al que poder ofrecer más precisiones, y solicitar confirmaciones o desmentidos, a la mayor brevedad posible, a su disposición en el teléfono 902998352.

NOTICIAS RELEVANTES para que las autoridades actúen de oficio considerando que la Agencia EFE ya ha informado del uso, al menos, en Mercadona de Mallorca, Valencia y Zaragoza. Nos hemos dirigido a EFE por mensaje publicado en http://cita.es/efe-mercadona-apedanica/

Mercadona instala un sistema que detecta a personas con ...

EL INDEPENDIENTE-1 jul. 2020 **Mercadona instala un sistema que detecta a personas** con orden de alejamiento ... la seguridad del cliente y de los trabajadores, según informa **EFE**. ... este miércoles en unas **40 tiendas de Mallorca**, **Zaragoza y Valencia**,

Mercadona comienza a usar un sistema de reconocimiento ...

Hipertextual-2 jul. 2020 ... la tecnológica "todos los clientes tienen prohibido usar la tecnología para **fines inapropiados**, **impropios o ilegales**". **Anyvision** y su fundador, ...

Mercadona usará tecnología de la israelí **AnyVision** para ...

valenciaplaza.com-1 jul. 2020 **Mercadona** usará tecnología de la israelí **AnyVision** para detectar a personas con orden de alejamiento de sus locales.

La tecnológica israelí con un asesor exMossad que 'caza ...
El Confidencial-1 jul. 2020

Mercadona instala un sistema de reconocimiento facial en sus ...
Xataka-3 jul. 2020

Mercadona usa reconocimiento facial para detectar a quien ...
El Español-2 jul. 2020

El revolucionario sistema para evitar robos que **Mercadona** ...
ComputerHoy-2 jul. 2020

Mercadona implanta el reconocimiento facial para detectar a ...
Completo-ABC.es-2 jul. 2020

Certezas y dudas sobre el sistema de **reconocimiento facial** ...
Genbeta-3 jul. 2020

Espionaje israelí, “uno de los más grandes de su tipo en el ...

CubaDebate-18 nov. 2019 Las conexiones entre **AnyVision** y los servicios de seguridad israelíes apenas están ocultas. Su consejo asesor incluye a Tamir Pardo, ex jefe ...

Compañías de **espionaje** de alto perfil están dañando la ...

Noticias de Israel-21 nov. 2019 **AnyVision** negó las afirmaciones, afirmando que la tecnología sólo se está utilizando en los puntos de control de Cisjordania, pero parece que ...

Microsoft retira su inversión en **AnyVision** y deja de invertir en ...

MCPRO-30 mar. 2020 Microsoft ha decidido retirar la inversión que había hecho en la startup israelí de **reconocimiento facial AnyVision**, además de manifestar que ...

Microsoft dejará de invertir en compañías de **reconocimiento** ...
Europa Press-30 mar. 2020

IBM abandona el desarrollo y utilización de una polémica ...

iProUp-9 jun. 2020 La tecnología de **reconocimiento facial** se usa comúnmente para ... de una controversia sobre su financiación de la startup israelí **AnyVision**, ...

IBM se aleja del **reconocimiento facial**
ENTER.CO-9 jun. 2020

Mercado **Reconocimiento facial** 2020-2026: Norteamérica ...

La Nota De Tapa-9 jun. 2020 Gemalto, **Anyvision**, Synectics plc, Amazon Web Services, Sistemas Cognitec, IBM, Aware, IDEMIA, Ayonix cara Tecnologías y Seguridad Herta.

Reconocimiento facial Análisis de mercado por nueva ...

Radio Petrer 107,2 fm-27 may. 2020 El análisis de la cuota de mercado global de **Reconocimiento facial** se ... Gemalto, **Anyvision**, Synectics plc, Amazon Web Services, Sistemas …

NOTA: Desde 1989 Miguel Gallardo ha peritado y defendido informes y dictámenes en juzgados y tribunales, como "**perito fisonomista**". Desde su constitución en 1992, la asociación **APEDANICA** ha conocido bien, y contribuido a desarrollar muy diversas tecnologías para la identificación de sujetos y objetos, así como las normas aplicables. El artículo 2 de la Ley de Enjuiciamiento Criminal junto al 9.3, 14, 18, 20, 24, 105 y 120 de la Constitución Española posibilitan la contradicción de **falsos positivos y falsos negativos en las identificaciones humanas erróneas**. Hemos vivido experiencias kafkianas, incluso con prisión preventiva, por falso positivo en identificaciones mediante sistemas de videovigilancia. No solamente **dictaminamos para exculpación de inocentes e imputación de culpables**, sino para exigir responsabilidad patrimonial a las Administraciones Públicas y la **extracontractual** del art. 1902 del Código Civil, a quien se ocasione algún **perjuicio por sus acciones u omisiones relacionadas con identificaciones criminalísticas falsas**.

REFERENCIAS

http://miguelgallardo.es/perito/fisonomista/
http://www.miguelgallardo.es/fisonomista.pdf
http://www.miguelgallardo.es/identificaciones/humanas/
http://www.miguelgallardo.es/habeas-video.pdf
http://www.miguelgallardo.es/preso-prueba-fisonomista.pdf
http://www.miguelgallardo.es/dictamen-videodeovigilancia-sin-video.pdf
http://www.miguelgallardo.es/denuncia-supermercado-dia.pdf
http://www.miguelgallardo.es/preventivo.pdf
http://www.cita.es/peritajes-conductuales.pdf
http://www.miguelgallardo.es/plagio-guardia-civil.pdf
http://www.cita.es/asuntos-internos-guardia-civil-udima-cef.pdf
http://www.cita.es/interior-udima-reintegro.pdf
http://www.miguelgallardo.es/verint.pdf
http://www.miguelgallardo.es/reverint.pdf
http://www.miguelgallardo.es/cisen.pdf
http://www.cita.es/nieto-ballesteros.pdf
http://www.miguelgallardo.es/informe-boozallen.pdf
http://www.miguelgallardo.es/aepd-booz.pdf
http://www.miguelgallardo.es/recurso-booz.pdf
http://www.miguelgallardo.es/querella-nsa.pdf
http://www.miguelgallardo.es/querella-nsa-reforma.pdf
http://www.miguelgallardo.es/querella-nsa-apela.pdf
http://www.miguelgallardo.es/policiologia.pdf
http://www.miguelgallardo.es/tesis.pdf

“Study on Face Identification Technology for its Implementation in the Schengen Information System Administrative Arrangement” JRC-34751, Galbally, J Ferrara, P Haraksim, R Psyllos, A Beslay, L 2019.

“A Survey on Deep Learning: Algorithms, Techniques, and Applications,” S. Pouyanfar, S. Sadiq, Y. Yan, H. Tian, Y. Tao, M. P. Reyes, M.-L. Shyu, S.-C. Chen and S. S. Iyengar, ACM Computing Surveys, vol. 51, 2019.

“Face recognition via collaborative representation: Its discriminant nature and superposed representation,” W. Deng, J. Hu and J. Guo, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 99, pp. 1-1, 2018.

“Arcface: Additive angular margin loss for deep face recognition,” J. Deng, J. Guo and S. Zafeiriou, arXiv preprint arXiv:1801.07698, 2018.

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/AEPD-informe-sistemas-reconocimiento-facial-empresas-seguridad-privada

***(Madrid, 28 de mayo de 2020)**. La Agencia Española de Protección de Datos (AEPD) ha publicado **un informe en el que analiza varias cuestiones que se le han planteado relacionadas con la seguridad privada**, entre las que se encuentra la licitud de **incorporar sistemas de reconocimiento facial en los servicios de videovigilancia proporcionados por empresas seguridad privada**.*

*El empleo de tecnologías de reconocimiento facial en los sistemas de videovigilancia implica el tratamiento de datos biométricos, a los que se aplica el Reglamento General de Protección de Datos (RGPD), que los cataloga como **categorías especiales** al tratarse de datos “dirigidos a identificar de manera unívoca a una persona física”. Esta tecnología supone un tratamiento que, en principio, se encuentra prohibido por el RGPD.*

*Para poder tratar esos datos, el informe analiza si es posible aplicar a dicha prohibición alguna de las excepciones recogidas en la normativa. La instalación de los sistemas de videovigilancia con fines de seguridad, que captan y graban imágenes y sonidos, podría ampararse en el interés público, tal y como se plantea en la consulta realizada a la Agencia. No obstante, si se tratan categorías especiales de datos, como en el caso de la utilización de tecnologías de reconocimiento facial, la normativa requiere que exista un **“interés público esencial”** para que pueda ser legítimo, profundizando así en la importancia y **necesidad de mayor protección** de los datos tratados.*

*La aplicación del interés público esencial como base de legitimación **requiere de una norma con rango de ley** que justifique en qué medida y en qué supuestos el empleo de la biometría respondería al mismo. La norma con rango de Ley que ampararía ese tratamiento de categorías especiales de datos no existe en el actual ordenamiento jurídico y, en el caso de tramitarse, tendría que justificar específicamente en qué medida y en qué supuestos la utilización de dichos sistemas respondería a un interés público esencial, así como incorporar garantías específicas como exige el Tribunal Constitucional. Asimismo, debería cumplir con el principio de proporcionalidad y superar el juicio de necesidad, en el sentido de que no exista **otra medida más moderada con la que se consiguiera el mismo***

***propósito con igual eficacia**. La existencia de otras medidas que permiten la protección de las personas, bienes e instalaciones con una menor intrusión en el derecho de los afectados, exigiría una especial justificación de la necesidad de optar por el reconocimiento facial respecto de dichas otras medidas, estableciendo asimismo garantías reforzadas.*

*La Agencia rechaza, tal y como se planteaba en la consulta, que la legitimación reconocida para los sistemas de videovigilancia que sólo captan y graban imágenes y sonidos pueda abarcar otras **tecnologías mucho más intrusivas** para la privacidad como el reconocimiento facial u otras medidas biométricas como el reconocimiento de la forma de andar o el reconocimiento de voz. La regulación actual es insuficiente para permitir la utilización de técnicas de reconocimiento facial en sistemas de videovigilancia empleados por la seguridad privada, al no cumplir los requisitos anteriormente señalados.*

Por último, la Agencia considera que existen supuestos excepcionales en los que podría quedar justificado el empleo de sistemas de reconocimiento facial siempre que la legislación lo prevea, como se ha mencionado con anterioridad, como en el caso de infraestructuras críticas. Sin embargo, la autorización, con carácter general, del empleo de sistemas de reconocimiento facial en los sistemas de videovigilancia empleados por la seguridad privada carece de base jurídica y sería desproporcionada, dada la intrusión y los riesgos que supone para los derechos fundamentales de los ciudadanos.

El informe de la AEPD al que hace referencia esa nota puede verse en
https://www.aepd.es/es/documento/2019-0031.pdf
y concluye así:

Por consiguiente, no puede admitirse, tal y como pretende la consulta, que la legitimación reconocida para los sistemas de videovigilancia, dirigida solo a la captación y grabación de la imagen y el sonido, abarque otras tecnologías mucho más intrusivas para la privacidad como pueda ser el reconocimiento facial u otras medidas biométricas como el reconocimiento de la forma de andar o el reconocimiento de voz. Por el contrario, la regulación actual se considera insuficiente para permitir la utilización de técnicas de reconocimiento facial en sistemas de videovigilancia empleados por la seguridad privada, al no cumplir los requisitos anteriormente señalados, siendo necesario que se aprobara una norma con rango de ley que justificara específicamente en qué medida y en qué supuestos, la utilización de dichos sistemas respondería a un interés público esencial, definiendo dicha norma legal, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías técnicas, organizativas y procedimentales adecuadas, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos. Dicha norma, en el caso de tramitarse, deberá ser preceptivamente informada por esta Agencia, momento en el cual podría valorarse si la misma se ajusta a los criterios señalados, sin que, apriorísticamente, se puede establecer un criterio taxativo por nuestra parte. No obstante, si puede adelantarse que, atendiendo al principio de proporcionalidad y al juicio de necesidad, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia, la existencia de otras medidas que permiten la protección de las personas, bienes e instalaciones con una menor intrusión en el derecho de los afectados, exigiría una especial justificación de la necesidad de optar por el reconocimiento facial respecto de dichas otras medidas. Así, esta Agencia considera que existen supuestos excepcionales en

los que podría quedar justificado el empleo de sistemas de reconocimiento facial siempre que la legislación, en los términos anteriormente señalados, así lo prevea, como podría ser el caso de las infraestructuras críticas, entendiendo por tales, conforme a la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, aquéllas cuyo "funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales". En este caso, la adecuada protección de las mismas tiene por finalidad garantizar la seguridad de los ciudadanos y el correcto funcionamiento de los servicios esenciales, por lo que la autorización por el legislador del empleo de técnicas de reconocimiento facial, estableciendo las garantías adecuadas, podría considerarse proporcional. Sin embargo, la autorización, con carácter general, del empleo de sistemas de reconocimiento facial en los sistemas de videovigilancia empleados por la seguridad privada, tal y como se plantea en la consulta, sería considerada, por esta Agencia, como desproporcionada, dada la intrusión y los riesgos que supone para los derechos fundamentales de los ciudadanos.

Guía práctica de seguridad de servicios de ... - CCN-CERT

www.ccn-cert.cni.es › guias › 400-guias-generales › file

18 mar. 2020 - puede ser deshabilitada, aunque Apple afirma que el **reconocimiento facial** se realiza de forma local en el dispositivo y nunca se carga en los …

(ccn-stic-804) esquema nacional de seguridad ... - CCN-CERT

www.ccn-cert.cni.es › publico › seriesCCN-STIC › series

PDF

26 oct. 2011 - **reconocimiento facial**. 329. En el acceso a locales o áreas: ▫ reconocimiento de la mano. ▫ reconocimiento del iris o del fondo del ojo. 330.

Los dispositivos móviles, gran objetivo de las ciberamenazas ...

www.ccn-cert.cni.es › articulos-y-reportajes › file

11 may. 2018 - **reconocimiento facial** Mac. EMPRESAS. Microsoft no venderá tecnología de **reconocimiento facial** hasta que haya una ley que la regule.

Pregunta escrita - Acceso al reconocimiento facial automático y ...
www.europarl.europa.eu › sides › getDoc › TEXT+WQ+...
INDECT piensa capturar y vincular asimismo en tiempo real datos biométricos de personas y utilizar para ello igualmente un software de reconocimiento facial.

Reconocimiento facial e identificación en espacios accesibles ...
www.europarl.europa.eu › O-9-2020-000018_ES
4 mar. 2020 - Pregunta con solicitud de respuesta oral a la Comisión Artículo 136 del Reglamento interno. Manon Aubry, Anne-Sophie Pelletier, Philippe ...

Preguntas parlamentarias

46k 10 k

1 de marzo de 2020

O-000018/2020

Pregunta con solicitud de respuesta oral
a la Comisión
Artículo 136 del Reglamento interno

Manon Aubry, Anne-Sophie Pelletier, Philippe Lamberts, Manuel Bompard, Leila Chaibi, Clara Ponsatí Obiols, Mick Wallace, Idoia Villanueva Ruiz, Konstantinos Arvanitis, Cornelia Ernst, Emmanuel Maurel, David Cormand, Younous Omarjee, Alexandra Geese, Saskia Bricmont, Viktor Uspaskich, Patrick Breyer, Rosa D'Amato, Markéta Gregorová, Aurore Lalucq, Helmut Scholz, Isabella Adinolfi, Marie Toussaint, Henrike Hahn, Martina Michels, Niyazi Kizilyürek, Fabio Massimo Castaldo, Hilde Vautmans, Pierre Larrouturou, Yannick Jadot, Raphaël Glucksmann, Paul Tang, Nora Mebarek, Stelios Kouloglou, Miguel Urbán Crespo, Alexis Georgoulis, Malin Björk, Petra De Sutter, Ernest Urtasun, Anna Cavazzini, Özlem Demirel, Petros Kokkalis, José Gusmão, Marc Botenga, Maite Pagazaurtundúa, Eugenia Rodríguez Palop, Marisa Matias, Helmut Geuking, Benoît Biteau, Gwendoline Delbos-Corfield, Claude Gruffat, Michèle Rivasi, Caroline Roose

Asunto: Reconocimiento facial e identificación en espacios accesibles al público

1. En el contexto de la preparación del Libro Blanco sobre la inteligencia artificial y la Estrategia para una Europa adaptada a la era digital, ¿considera la Comisión que el despliegue de sistemas de reconocimiento facial o identificación facial en espacios accesibles al público por parte de Estados miembros es incoherente en relación con el artículo 9, apartado 1, y el artículo 9, apartado 2, letra g), del Reglamento General de Protección de Datos (RGPD), dado que no cumple los requisitos de ser «necesario por razones de un interés público esencial», y el artículo 4, apartado 1, el artículo 8, apartado 1, y el artículo 10 de la Directiva sobre protección de datos en el ámbito penal?

2. ¿Detecta la Comisión riesgos de violación de derechos fundamentales generados por el despliegue de sistemas de reconocimiento facial o identificación facial en espacios accesibles al público por parte de los Estados miembros?

3. En tal caso, ¿está estudiando la Comisión, en su calidad de guardiana de los Tratados, la prohibición de dichas prácticas o la apertura de procedimientos de infracción contra Estados miembros?

Presentación: 01/03/2020

Plazo límite: 02/06/2020

Agencia Española de Protección de Datos AEPD, Comisión Nacional de los Mercados y la Competencia CNMC, Ministerio de Consumo, Centro Criptológico Nacional del CNI, Mercadona y Anyvision por solicitud publicada en www.cita.es/apedanica-reconocimiento-facial.pdf

Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf