Reconocimiento facial, una distopía para vender humo

ÁLVARO LORITE :: 14/10/2020

A pesar de los medios, nos encontramos ante una tecnología incipiente que está muy lejos de llegar a ser el panóptico digital que imaginamos

Si el 11 de septiembre de 2001 marcó un punto de inflexión y Estados Unidos se ocupó de escorar el debate público de los países de su órbita hacia el mantra de la seguridad, poblando las grandes ciudades de cámaras de vigilancia, el año 2020 y su covid-19 han marcado el siguiente hito en la videovigilancia: el reconocimiento facial. A pesar de que los primeros sistemas se instalaron en EE UU a principios de los años 10, la prensa nos ha hecho testigos en los últimos meses de la cantidad de proyectos que se han implementado en hasta 75 países. Según un estudio realizado por la empresa Técnicas en Cámaras y Seguridad, contando las instalaciones dadas de alta en la Agencia Española de Protección de Datos (AEPD) y los informes de ventas anuales de empresas del sector, se calcula que hay más de 900.000 cámaras de seguridad en España.

En el Estado español, el reconocimiento facial opera desde 2016 en la estación de autobuses de Méndez Álvaro en Madrid. Funciona en aeropuertos de diversas ciudades, centros comerciales, casinos y salas de juego. El BBVA, a través de Véridas, una empresa de biometría creada por el propio banco, y Bankia han sacado sus propios sistemas de pago por reconocimiento facial en 2020. Caixabank lanzó en Canarias sus primeros cajeros que identifican las caras de sus clientes para operar sin meter el identificador PIN. Este mismo año, la compañía PwC Tax and Legal Services ha comercializado un sistema para procesar ayudas al alquiler. Uber implanta tecnología de reconocimiento de objetos en sus vehículos para certificar el uso de mascarilla en empleados y clientes. En mayo, la cadena de hoteles Meliá anunció que integraría el sistema Rekognition de Amazon para registrar clientes.

El 6 de julio, Protección de Datos abrió una investigación contra Mercadona, ya que había instalado estos sistemas en 40 de sus sucursales en Mallorca, Zaragoza y Valencia. Según la normativa vigente, “la utilización de dichos sistemas está prohibida en el ámbito privado a menos que responda a un interés público esencial”. Mercadona declaró tener bases con datos biométricos de sus propios ficheros. La empresa responsable es AnyVision, que estuvo implicada en una polémica cuando Microsoft, IBM y Amazon retiraron sus inversiones al publicarse que usaba su tecnología para vigilar población palestina en Cisjordania.

En septiembre de 2019 un instituto de Badalona fue multado con 19.000 euros por utilizar el reconocimiento facial para confirmar la asistencia de los alumnos. El debate en el ámbito docente se ha reabierto en los últimos meses a raíz de los exámenes y clases telemáticas en la universidad. El IE Business School, CEU San Pablo o la Universidad Rey Juan Carlos han aplicado estos programas. El *software* se activa durante el examen para fotografiar al alumnado, identificarlo e incluso detectar movimientos o gestos sospechosos, siempre según las empresas desarrolladoras. De nuevo la AEPD publicó un comunicado en el que señalaba que esto solo podía hacerse con el consentimiento expreso de los alumnos.

Otro de los campos donde se han desarrollado y aplicado este tipo de algoritmos en el Estado es el de las entrevistas laborales. La empresa Eyesecure dice haber desarrollado un algoritmo que analiza la expresión gestual, entre otros parámetros, para sugerir candidatos a partir de videoentrevistas. Telepizza, Porcelanosa, Prosegur, Securitas Direct, Five Guys, Econocon o Sprinter ya lo usan.

En septiembre de 2020, un conglomerado de seis empresas, tres universidades y el Instituto Tecnológico de Castilla y Leon, supervisados por el Ministerio del Interior, han anunciado estar diseñando AI MARS, un sistema que, según sus promotores, "permitirá rastrear millones de caras por segundo en grandes concentraciones como manifestaciones, campos de fútbol o festivales". Aseguran, además, que el uso de la mascarilla no supondrá ningún obstáculo para el reconocimiento. Cuenta con un presupuesto de más de cinco millones de euros.

"No es fácil listar todos los lugares de tránsito público donde se usa esta tecnología", señala Ekaitz Ortega, periodista que investiga el tema desde hace varios años y ha tratado de buscar, una a una, estas localizaciones en enclaves destacados de las grandes ciudades. "No existe ningún registro que liste todos los lugares donde se aplica. Yo tuve que armarme de paciencia y encontré muchos a través de la prensa. En el caso de Ifema —en Madrid— encontré la licitación y eran casi dos millones de euros", añade. En un reciente reportaje publicado en el AlgorithmWatch, la periodista Naiara Bellio escrutaba el sistema de la Estación Sur de Autobuses de Madrid. Allí, las empleadas de los comercios de la estación contaban que desconocían que el sistema estaba siendo usado desde 2016 en la estación donde trabajaban.

TEORÍA Y PRÁCTICA EN EL RECONOCIMIENTO FACIAL

Los sistemas mencionados utilizan algoritmos de reconocimiento facial, pero no todos son iguales. Se pueden agrupar básicamente en dos grupos. Por un lado, los sistemas que funcionan 'de uno a uno', que verifican que eres quien dices ser. Son los sistemas de pago en bancos. El sistema te fotografía y compara esa imagen con una foto tuya que tiene en sus bases de datos. Por otro lado, estarían los algoritmos 'de uno a n', que son los que se utilizarían para procesos de securitización de espacios públicos. Estos sistemas cuentan con una base de datos previa de varias personas registradas. La cámara hace fotos de quienes transitan el espacio para ver si alguna coincide con las que componen esas bases.

Gemma Galdón, investigadora española de políticas públicas especializada en vigilancia y directora de la Fundación Éticas, donde se auditan algoritmos e inteligencias artificiales desde una perspectiva ética, se muestra escéptica ante los logros en temas de securitización que venden los CEO de estas compañías. "Esto ya nos pasó con la videovigilancia normal. Decir que una cámara de reconocimiento facial ha disminuido la delincuencia es inexacto. Tienes que explicarme cómo has llegado exactamente a ese cálculo o tu explicación tiene cero credibilidad, aunque digas que la criminalidad se ha reducido un tanto por ciento gracias a tus sistemas", desarrolla. Bellio coincide: "En mi caso se escudaron en que el sistema de la estación está catalogado como 'infraestructura crítica' para no darme ningún tipo de información, ni de la tecnología ni del supuesto descenso de la delincuencia asociado a la misma".

En el Estado español, Herta Security, empresa con sede en Barcelona y responsable del sistema que se aplica en la Estación Sur madrileña, que participa en el macroproyecto AI MARS con Interior, lanzó un comunicado afirmando que sus sistemas pueden identificar incluso cuando el o la transeunte lleva mascarilla. Jorge Félix, director del Departamento de calidad de FacePhi, otra de las líderes en reconocimiento biométrico cuyos productos se usan en Caixabank, afirmaba en una entrevista en Onda Cero que el reconocimento facial ahora mismo es el más fiable de los sistemas de reconocimiento biométrico desarrollados. También declaró haber resuelto el problema de las mascarillas. “Es una estrategia comunicativa basada en la publicidad comercial, pero si tratas de indagar más allá, silencio absoluto. Yo hablé en repetidas ocasiones con la administración de la estación y me dijeron que no intentara obtener más información porque no me la iban a dar”, expone Bellio.

“Es imposible reconocer a la gente con mascarilla, da igual lo que digan las empresas que venden estos productos. Esta tecnología establece varios puntos en la cara para comparar y la mayoría están alrededor de boca, nariz y ojos. Nos están tomando el pelo y vendiendo humo. En la inteligencia artificial no se ha establecido un control de calidad como en otros productos”, sentencia Galdón.

El Instituto Nacional de Estándares y Tecnología de EE UU ha publicado un informe reciente en el que señala que los fallos de reconocimiento con mascarilla llegan en ocasiones al 50% de los casos en el emparejamiento de ‘uno a uno’, el más fiable y sencillo de ambos. En la ciudad de Madrid el desarrollo de un sistema de pago para el transporte público (desarrollado por Mastercard y Saffe) se ha visto paralizado por el uso de las mascarillas.

El proyecto CV-Dazzle, financiado por la fundación NLnet, diseñó una serie de maquillajes basados en la idea de camuflaje disruptivo que lograban confundir a los algoritmos

San Francisco, cuna de Silicon Valley, prohibió el uso de esta tecnología por parte de la policía gracias a la presión por parte de grupos de activistas. Tras las protestas desencadenadas por el asesinato de George Floyd, Amazon anunció en junio de este año que prohibía el uso de su tecnología reconocimiento facial (Rekognition) durante un año, ya que se habían documentado un gran número de falsos positivos entre la población negra.

Sobre los falsos positivos y las discriminaciones raciales provocadas por sesgos en las bases de datos, Galdón reconoce: “En el nivel teórico me parece muy necesario el debate. Sin embargo, en el práctico no, sencillamente porque estos sistemas no funcionan, le hacemos un favor a quien está tratando de vender esta tecnología. Planteamos un escenario donde un algoritmo pueda discriminar a determinados grupos, cuando el problema es que dichos sistemas no funcionan. Operan relativamente bien, con errores superiores al 30%, en escenarios prácticamente estáticos, con una persona parada, sin nada en la cara”.

USOS ILEGALES Y RESISTENCIAS

Cuando los datos biométricos se usan como medio de identificación, el Reglamento General de Protección de Datos establece en su artículo 9 que se trata de categorías especiales de datos y prohíbe expresamente su tratamiento dirigido a identificar de manera unívoca a una persona física. “Es ilegal, lo que pasa es que no se aplica la ley. Recientemente la Agencia

de Protección de Datos británica se ha declarado incapaz de multar la cantidad de malas prácticas que existen. Hemos hecho leyes que nadie está cumpliendo. A veces son prácticas que emanan de la propia administración pública", señala Galdón al respecto.

Tanto en EE UU como en Europa, los modelos de resistencias surgen desde el activismo ciudadano. El proyecto CV-Dazzle, financiado por la fundación NLnet, diseñó una serie de maquillajes basados en la idea de camuflaje disruptivo que lograban confundir a los algoritmos mediante colores que contrasten con el color de piel y crear asimetrías en pelo y maquillaje. Este mismo año en la Universidad de Chicago se diseñó el sistema Fawkes, una herramienta digital que cambia ciertos píxeles en fotografías imperceptibles para el ojo humano, pero que eran capaces de confundir a los algoritmos. En Francia se ha diseñado el proyecto Technopolice, un detallado mapeo colaborativo de todos los sistemas de vigilancia digitales públicos y privados.

"La visión que tiene la gente de la tecnología está más influida por la ciencia ficción que por los hechos científicos. Esto ha sido creado y aupado por muchos sectores: las empresas que comercializan estos productos, pero también por los medios de comunicación, que reproducen sus comunicados sin cuestionarlos porque ganan clics. El problema es que es muy difícil tener un debate público sano cuando la gente no sabe de qué estamos hablando. Si nos lo explicaran, veríamos que nos están tomando el pelo", reflexiona Galdón. La investigadora finaliza recomendando la lectura de la socióloga y escritora turca Zeynep Tufekci, que lo resume así: "Estamos creando un escenario distópico solo para que la gente haga clic en un anuncio y vender lavadoras".

El Salto
