

Luces, cámara y persecución

DIARIO DE VURGOS :: 19/09/2020

Hace años que nos amenaza el software de reconocimiento facial pero parece que nos da igual.

Aún recuerdo la primera vez que vi apuntar una cámara contra la población, fue hace muchos años. La Falange se paseaba por Burgos y había convocadas acciones de protesta. El objetivo de la policía era contener, coaccionar y posteriormente perseguir e identificar a los que protestaban ante ese paseo.

Recuerdo al madero de turno portar una cámara, de aquellas vetustas VHS, con la que immortalizó a todas las personas allí presentes. Aquello me marcó tanto que lo recuerdo como si fuese ayer. Probablemente aquel madero hoy este jubilado y la juventud que tratábamos de frenar al fascismo en las calles hoy peinemos canas, pero el hedor de aquella idea hoy se ha extendido por todos los lugares de nuestra geografía y ya nadie lo huele. Da igual el tipo de régimen en el que te haya tocado vivir, hoy nuestra sociedad es retratada segundo a segundo por cámaras.

En plena era de la información, los policías no portan cámaras en sus manos, no son tan voluminosas como aquellas VHS, sus cámaras no se ven, están en los coches y las lecheras, en los paragolpes o tras los cristales tintados, pueden estar en sus ropas o incluso ser cámaras públicas o privadas. En ocasiones incluso medios de información o personas anónimas han facilitado que se obtengan vídeos y fotos haciéndolos públicos en internet. El Ministerio de Interior se reserva el derecho a acceder a todos los vídeos y custodiarlos a su antojo. Llevamos años de recopilaciones de vídeos e imágenes, a través de cámaras e internet se han podido recoger una cantidad ingente de datos que muy probablemente estén almacenados. Almacenar datos hoy en día es barato y si eres el Ministerio del Interior mucho más barato.

Pese a esta situación en estas tierras pocos grupos políticos hacen campaña contra la videovigilancia, son pocos los que denuncian o han denunciado esta situación. Además en muchos movimientos sociales se ve como algo malo taparse el rostro. Sin embargo es algo que deberíamos recomendar, enseñar, fomentar y normalizar. Hace años que nos amenaza el software de reconocimiento facial pero parece que nos da igual.

Antes de al menos el año 2014 procesar los vídeos de, por ejemplo, una numerosa manifestación para segmentar, clasificar e identificar a los participantes no solo no era ético sino que también era caro, muy caro. Nadie se planteaba una cosa así, se necesitaban muchas personas y muchas horas para poder llevar a cabo esa ardua tarea. Hoy, sigue siendo caro, pero es un gasto más que asumible para los que nos gobiernan. Es probable que todos esos años de recolección de vídeos comiencen a dar sus frutos, tal vez seas un número al que no se ha puesto nombre pero que ha sido reconocido en varios eventos públicos, tal vez tu cara ya ha sido vinculada a tu nombre y también hayas sido reconocido en varios eventos públicos o tengas suerte y tus rasgos faciales confundan a la inteligencia

artificial (en adelante IA) que los escanea. Conforme haya más vídeos, haya más datos, las inteligencias artificiales se mejoren y las capacidades de cálculo aumenten tendrás más posibilidades de ser identificado.

No todo son malas noticias

Antes de nada deberías saber que hablar de IA en muchas ocasiones es hablar de humo, mucha pretensión y pocos hechos. Las IAs se han perfeccionado mucho en los últimos años y son increíblemente eficientes en algunos aspectos. Pero en muchos otros siguen siendo ineficientes o poco resolutivas, el reconocimiento facial puede que sea una de esas cosas. Aún no existe, o al menos no se ha demostrado, que una IA sea más precisa identificando rostros que las personas. El sistema de reconocimiento facial del FBI tiene una tasa de acierto del 85%. DeepFace, una IA creada por Facebook para el reconocimiento facial, tiene un porcentaje de acierto del 97.35% algo ligeramente menor que el de un humano que se sitúa en un 97.53%. Aunque es un excelente resultado no es algo definitivo y arañar una centésima a este record puede suponer años de investigación. Si de cada 100 registros entre 15 y 4 son erróneos tal vez el remedio sea peor que la enfermedad y no compense por el momento para según que tareas el reconocimiento facial por parte de una IA. Además todo parece indicar que este trabajo aún tenga que estar supervisado por personas. Pero el reconocimiento facial va mucho más allá de la tarea de comparar rostros hay infinidad de peculiaridades que hacen de esto algo mucho más complejo. Es necesario analizar rasgos, gestos, tratar la calidad de la imagen, calcular el envejecimiento, detectar complementos, épocas del año, tipos de actividades... algo donde las IAs son aún mucho peores que los humanos.

Esto no es para identificar malhechores

Londres es uno de los pioneros del reconocimiento facial, algunos distritos llevan vigilando a sus habitantes desde 2004 con el pretexto de perseguir a los malhechores. Sin embargo, el sistema de videovigilancia londinense apenas ha identificado malhechores en los 16 años de funcionamiento. Esto puede deberse a que efectivamente el reconocimiento facial, como hemos dicho antes, no es tan efectivo. Pero lo más probable es que la inversión en reconocimiento facial no se enfoque o no sea útil frente a malhechores si no a investigar a la población y usarlo como sistema de inteligencia. Imagina que vives en Londres y quieres robar a alguien la cartera, elegirás una zona donde sabes que no hay cámaras y poder realizar la acción fuera de la vídeo vigilancia, además lo lógico sería operar en distintas ubicaciones y nunca donde vives o te conocen. Sin embargo si quieres ir al trabajo, reunirte con un amigo o ver a tu familia lo tienes mucho más difícil para escapar del control de las cámaras.

Las redes sociales son un enemigo de la privacidad

Muchos expertos en el estado del arte de la IA afirman que China es el país que actualmente está ganando la carrera mundial de la IA. En Agosto del 2020 un ciudadano chino fue encarcelado por mandar un vídeo a través de la red social WeChat donde se le podía reconocer junto a otro activista chino exiliado y perseguido por la justicia china, la teoría tras esta detención es que el gobierno chino procesa y analiza los vídeos compartidos a traves de WeChat. Los estados tienen acuerdos o controlan los contenidos de muchas redes

sociales, vídeos e imágenes son procesados a diario por los gobiernos para perseguir, ajusticiar, investigar o simplemente documentar a cualquier disidente. Además es probable que los estados, como pasa con el armamento militar, vendan servicios a otros estados. Hace años que Edward Snowden desveló que el gobierno español cedía datos a EEUU para su posterior tratamiento.

Las redes GSM

Si a un sistema de reconocimiento facial le añades otro de geolocalización, la identificación se vuelve mucho más efectiva. Las redes GSM más conocidas por sus nombres comerciales, 3G, 4G, 5G... son las redes inalámbricas con las que operan las compañías telefónicas. Unos datos con patente nacional mucho más accesibles para los gobiernos que tener que traspasar las fronteras donde operan las redes sociales. Las primeras generaciones de la telefonía GSM no ponían el foco en la geolocalización las mentes que diseñaron estas redes se preocuparon única y exclusivamente en comunicar, que debería ser el único cometido de estas redes. Pero poco a poco según fueron avanzando fueron incorporando sistemas para localizar geográficamente a sus usuarios, al principio eran poco precisos pero para la llegada del 3G ya podían incorporar una capacidad de geolocalización bastante precisa. Conforme las redes GSM han avanzado han ido necesitando más antenas, la llegada del 5G no supondrá un avance en la geolocalización, sin embargo el número de antenas por kilómetros aumentará mucho y esto hará que tengan aún más precisión por el simple hecho de tener menos radio de acción. En el momento en que el resultado de un análisis de la IA no sea claro, puede ser resuelto recurriendo a los datos de la compañía móvil, incluso si la persona a identificar no lleva móvil tal vez los datos de las llamadas realizadas puedan ayudar a identificar a la persona por los que le rodean.

A ciencia cierta nadie sabe si los vídeos, imágenes y demás material en el Estado español ha sido, es o será analizado, pero si no se está haciendo dar por seguro que en un futuro cercano se hará. Acostumbraros a la mascarilla, no deberíamos abandonarla, incluso cuando ya no nos amenace un virus. El Ministro de interior te vigila.

<https://diariodevurgos.com/dvwps/luces-camara-y-persecucion.php>

https://www.lahaine.org/est_espanol.php/luces-camara-y-persecucion